Path Discovery Test Suite

Draft Version 0.1.1
June 3, 2005

Table of Contents

1 Introduction

1.1 Overview

A certification path is an ordered list of certificates starting with a certificate issued by the relying party's trust root, and ending with the target certificate that needs to be validated. Certification path processing verifies the binding between the subject distinguished name and/or subject alternative name and the subject public key defined in the target certificate. The binding is limited by constraints, which are specified in the certificates that comprise the path, and inputs that are specified by the relying party.

Certification path discovery is the process of creating the certification path needed to validate a target certificate. In order to validate a target certificate, a certification path starting with one of the relying parties trust anchors and ending with the target certificate must be constructed and all relevant revocation status information must be located. This document includes descriptions for certificates and CRLs for several sample PKI architectures. In each PKI architecture includes several end entity certificates that can be designated as target certificates. A set of tests are defined in which a target certificate and a trust anchor are defined. In some cases there is a valid certification path, which the relying party is expected to be able to build and validate and in some cases no valid certification path exists.

1.2 Background

In the fall of 2000, NIST worked in conjunction with CygnaCom Solutions and Getronics Government Solutions, LLC to develop a test suite for a subset of the features defined in the IETF PKIX Certificate and CRL Profile, RFC 2459. The resulting test suite, documented in *Conformance Testing of Relying Party Client Certificate Path Processing Logic* v. 1.07, has been widely used since its creation. Over the course of 2003 and 2004 the *Public Key Interoperability Test Suite (PKITS) Certification Path Validation* was developed. PKITS was designed to cover most of the features described in the successor to RFC 2549, RFC 3280, and was intended to be the successor to *Conformance Testing of Relying Party Client Certificate Path Processing Logic*. Both of these test suites were designed to enable the testing of the path validation capabilities of a path validation module (PVM), but not the path discovery capabilities of a PVM.

This document was developed to complement PKITS and it is intended for use with PVMs whose path validation capabilities have already been verified using PKITS. The tests in this test suite are subdivided based on the complexity of the PKI architecture in which the certification path must be built and based on the method by which certificates and CRLs must be located. At the Rudimentary level, all target certificates are issued by CAs that are hierarchically subordinate to the trust anchor and all certificates and CRLs in the certification paths are limited to the features that are included in the requirements for Enterprise PVMs in the *NIST Recommendation for X.509 Path Validation*. At the Basic level, the target certificates are issued by CAs that are not hierarchically subordinate to the trust anchor and certificates in the certification path include policy mappings, policy constraint extensions, and name constraints extensions. Some self-issued certificates assert the anyPolicy OID rather than asserting specific certificate policy OIDs.

For each level of testing, there are three nearly identical PKI architectures. In the first PKI architecture none of the certificates include authorityInfoAccess or subjectInfoAccess extensions. Some certificates include cRLDistributionPoints extensions that specify a distribution point as a

directoryName, but most certificates do not include a cRLDistributionPoints extension. In the other two PKI architectures, authorityInfoAccess, subjectInfoAccess, and cRLDistributionPoints extensions are included where appropriate. In one of the PKI architectures these extensions are populated with LDAP URIs and in the other PKI architecture these extensions are populated with HTTP URIs.

1.3 Getting the Test Data

Information about obtaining the data needed to run the tests in this test suite may be found at http://csrc.nist.gov/pki/testing/pathdiscovery.html. From this site it will be possible to download a copy of this document as well as all of the trust anchor certificates, end entity certificates, and S/MIME messages specified in this document. The Web site will also specify the location of an LDAP server from which the certificates and CRLs for the first PKI architecture may be obtained.

2 References

2.1 Documents

PKCS #12 PKCS 12 v1.0: Personal Information Exchange Syntax. RSA Laboratories, June 1999.

PKITS Public Key Interoperability Test Suite (PKITS) Certification Path Validation, version 1.0, September 2, 2004. http://csrc.nist.gov/pki/testing/PKITS.pdf.

PATHVAL NIST Recommendation for X.509 Path Validation, version 0.5, May 3, 2004. http://csrc.nist.gov/pki/testing/NIST_Recommendation_for_X509_PVMs.pdf.

RFC 822 Standard for the Format of ARPA Internet Text Messages, August 1982.

RFC 2253 IETF Request for Comments 2253, Lightweight Directory Access Protocol (v3): UTF-8 String Representation of Distinguished Names, December 1997.

RFC 2587 IETF Request for Comments 2587, Internet X.509 Public Key Infrastructure LDAP v2 Schema, June 1999.

RFC 3369 Cryptographic Message Syntax, August 2002.

RFC 3280 IETF Request for Comments 3280, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002.

X.509 ITU-T Recommendation X.509 (03/2000), Information Technology – Open Systems Interconnection – The Directory: Public-Key and Attribute Certificate Frameworks.

2.2 Acronyms

This section contains the definitions for some of the acronyms used in this document.

ARL Authority Revocation List

ASN.1 Abstract Syntax Notation One

CA Certification Authority

CRL Certificate Revocation List

DN	Distinguished Name
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
OID	Object Identifier
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PVM	Path Validation Module
RDN	Relative Distinguished Name
RFC	Request for Comments
S/MIME	Secure/Multipurpose Internet Mail Extensions
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector

2.3 Definitions

This section contains some of the definitions used in this document.

CA Certificate	A public key certificate whose subject is a CA.
Certification Path	A chain of certificates starting with a certificate issued by the trust anchor of the relying party and ending with the certificate issued to the subject of interest to the relying party. A Certification Path consists of zero or more **Intermediate Certificates** and one **End Certificate.** The first certificate in a Certification Path of length greater than one is also called an **Intermediate Certificate**. The first certificate in a Certification Path of length one is called an **End Certificate** since it is the last certificate in the Certification Path.
Distinguished Name	An unambiguous name that identifies an entity. A distinguished name is made up of one or more relative distinguished names (RDNs).
End Certificate	The last certificate in a **Certification Path.**
End Entity Certificate	A public key certificate whose subject is not a CA.
Intermediate Certificate	Any certificate in a **Certification Path** except for the **End Certificate**.

3 Initialization Procedures

This section contains the initialization parameters needed to be set when performing the test cases defined in this document.

All of the test cases are designed for processing with the following inputs:

- Trusted certificate to use (a.k.a. trust anchor) is either Basic Directory Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root Cert, or Basic HTTP URI Trust Anchor Root Cert;
- *initial-policy-set* is the special value *any-policy*[1];
- *initial-explicit-policy* indicator value is false;
- *initial-policy-mapping-inhibit* indicator value is false; and
- *initial-inhibit-any-policy* indicator value is false.

The inputs listed above are referred to as the *default settings*.

4 Certification Path Discovery Tests

4.1 Rudimentary

4.1.1 Rudimentary Directory-based Path Discovery

4.1.1.1 Rudimentary Directory Path Discovery Test1

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. All mandatory and optional information has been stored in the **cACertificate** and **crossCertificatePair** attributes of the directory entries of the CAs in the path.

Procedure: Validate Rudimentary Directory Path Discovery Test1 EE using the default settings[2] or open and verify Signed Test Message 5.3.2.1 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA1 Cert, Basic Directory Trust Anchor SubCA1 CRL
- Basic Directory Trust Anchor SubSubCA1 Cert, Basic Directory Trust Anchor SubSubCA1 CRL
- Rudimentary Directory Path Discovery Test1 EE

4.1.1.2 Rudimentary Directory Path Discovery Test2

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. Only the mandatory information has been stored in the **cACertificate** and **crossCertificatePair** attributes of the directory entries of the CAs in the path.

[1] In RFC 3280, the *initial-policy-set* is referred to as the user-initial-policy-set and *initial-inhibit-any-policy* is initial-any-policy-inhibit.

[2] The default settings are specified in Section 3.

Procedure: Validate Rudimentary Directory Path Discovery Test2 EE using the default settings or open and verify Signed Test Message 5.3.2.2 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA2 Cert, Basic Directory Trust Anchor SubCA2 CRL
- Basic Directory Trust Anchor SubSubCA2 Cert, Basic Directory Trust Anchor SubSubCA2 CRL
- Rudimentary Directory Path Discovery Test2 EE

4.1.1.3 Rudimentary Directory Path Discovery Test3

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The Trust Anchor Root CA has issued two certificates to the intermediate CA, one for each key.

Procedure: Validate Rudimentary Directory Path Discovery Test3 EE using the default settings or open and verify Signed Test Message 5.3.2.3 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA3 Cert, Basic Directory Trust Anchor SubCA3 Cert2, Basic Directory Trust Anchor SubCA3 CRL
- Rudimentary Directory Path Discovery Test3 EE

4.1.1.4 Rudimentary Directory Path Discovery Test4

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The Trust Anchor Root CA has issued two certificates to the intermediate CA, one for each key. The end entity certificate has been revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test4 EE using the default settings or open and verify Signed Test Message 5.3.2.4 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL

- Basic Directory Trust Anchor SubCA3 Cert, Basic Directory Trust Anchor SubCA3 Cert2, Basic Directory Trust Anchor SubCA3 CRL
- Rudimentary Directory Path Discovery Test4 EE

4.1.1.5 Rudimentary Directory Path Discovery Test5

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate.

Procedure: Validate Rudimentary Directory Path Discovery Test5 EE using the default settings or open and verify Signed Test Message 5.3.2.5 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA4 Cert, Basic Directory Trust Anchor SubCA4 CRL
- Basic Directory Trust Anchor SubCA4 Self-Issued Cert
- Rudimentary Directory Path Discovery Test5 EE

4.1.1.6 Rudimentary Directory Path Discovery Test6

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate. The end entity certificate has been revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test6 EE using the default settings or open and verify Signed Test Message 5.3.2.6 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA4 Cert, Basic Directory Trust Anchor SubCA4 CRL
- Basic Directory Trust Anchor SubCA4 Self-Issued Cert
- Rudimentary Directory Path Discovery Test6 EE

4.1.1.7 Rudimentary Directory Path Discovery Test7

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the end entity certificate. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the end entity certificate and certifies the key needed to verify the CRL.

Procedure: Validate Rudimentary Directory Path Discovery Test7 EE using the default settings or open and verify Signed Test Message 5.3.2.7 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA5 Cert, Basic Directory Trust Anchor SubCA5 Self-Issued Cert, Basic Directory Trust Anchor SubCA5 CRL
- Rudimentary Directory Path Discovery Test7 EE

4.1.1.8 Rudimentary Directory Path Discovery Test8

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the end entity certificate. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the end entity certificate and certifies the key needed to verify the CRL. The end entity certificate has been revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test8 EE using the default settings or open and verify Signed Test Message 5.3.2.8 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA5 Cert, Basic Directory Trust Anchor SubCA5 Self-Issued Cert, Basic Directory Trust Anchor SubCA5 CRL
- Rudimentary Directory Path Discovery Test8 EE

4.1.1.9 Rudimentary Directory Path Discovery Test9

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The first intermediate CA has issued an Authority Revocation List (ARL), which is stored in the CA's authorityRevocationList attribute, that lists the second intermediate CA's certificate as being revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test9 EE using the default settings or open and verify Signed Test Message 5.3.2.9 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA6 Cert, Basic Directory Trust Anchor SubCA6 CRL
- Basic Directory Trust Anchor SubSubCA6 Cert, Basic Directory Trust Anchor SubSubCA6 CRL
- Rudimentary Directory Path Discovery Test9 EE

4.1.1.10 Rudimentary Directory Path Discovery Test10

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has issued a CRL, which is not stored in the CA's directory entry, that lists the end entity certificate as being revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test10 EE using the default settings or open and verify Signed Test Message 5.3.2.10 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA7 Cert, Basic Directory Trust Anchor SubCA7 CRL
- Rudimentary Directory Path Discovery Test10 EE

4.1.1.11 Rudimentary Directory Path Discovery Test11

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has issued an ARL, which is not stored in the CA's directory entry, that lists the second intermediate CA's certificate as being revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test11 EE using the default settings or open and verify Signed Test Message 5.3.2.11 using the default settings.

Expected Result: The path should not validate successfully since the intermediate certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL

- Basic Directory Trust Anchor SubCA7 Cert, Basic Directory Trust Anchor SubCA7 CRL
- Basic Directory Trust Anchor SubSubCA7 Cert, Basic Directory Trust Anchor SubSubCA7 CRL
- Rudimentary Directory Path Discovery Test11 EE

4.1.1.12 Rudimentary Directory Path Discovery Test12

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The directory entries of the two intermediate CAs are not stored in the local directory, but the local directory provides a referral to the directory that holds these directory entries.

Procedure: Validate Rudimentary Directory Path Discovery Test12 EE using the default settings or open and verify Signed Test Message 5.3.2.12 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA8 Cert, Basic Directory Trust Anchor SubCA8 CRL
- Basic Directory Trust Anchor SubSubCA8 Cert, Basic Directory Trust Anchor SubSubCA8 CRL
- Rudimentary Directory Path Discovery Test12 EE

4.1.1.13 Rudimentary Directory Path Discovery Test13

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The directory entries of the two intermediate CAs are not stored in the local directory, but the local directory provides a referral to the directory that holds these directory entries. The end entity certificate has been revoked.

Procedure: Validate Rudimentary Directory Path Discovery Test13 EE using the default settings or open and verify Signed Test Message 5.3.2.13 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor SubCA8 Cert, Basic Directory Trust Anchor SubCA8 CRL
- Basic Directory Trust Anchor SubSubCA8 Cert, Basic Directory Trust Anchor SubSubCA8 CRL
- Rudimentary Directory Path Discovery Test13 EE

4.1.2 Rudimentary URI based Path Discovery

4.1.2.1 Rudimentary LDAP Path Discovery Test1

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. All mandatory and optional information has been stored in the **cACertificate** and **crossCertificatePair** attributes of the directory entries of the CAs in the path. All intermediate certificates include **subjectInfoAccess** extensions with LDAP URIs and all certificates include **authorityInfoAccess** extensions with LDAP URIs.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test1 EE using the default settings or open and verify Signed Test Message 5.3.2.14 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA1 Cert, Basic LDAP URI Trust Anchor SubCA1 CRL
- Basic LDAP URI Trust Anchor SubSubCA1 Cert, Basic LDAP URI Trust Anchor SubSubCA1 CRL
- Rudimentary LDAP URI Path Discovery Test1 EE

4.1.2.2 Rudimentary HTTP Path Discovery Test2

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. All intermediate certificates include **subjectInfoAccess** extensions with HTTP URIs and all certificates include **authorityInfoAccess** extensions with HTTP URIs.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test2 EE using the default settings or open and verify Signed Test Message 5.3.2.15 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA1 Cert, Basic HTTP URI Trust Anchor SubCA1 CRL
- Basic HTTP URI Trust Anchor SubSubCA1 Cert, Basic HTTP URI Trust Anchor SubSubCA1 CRL
- Rudimentary HTTP URI Path Discovery Test2 EE

4.1.2.3 Rudimentary LDAP Path Discovery Test3

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. Only the mandatory information has been stored in the **cACertificate** and **crossCertificatePair** attributes of the directory entries of the CAs in the path. All certificates include **authorityInfoAccess** extensions with LDAP URIs, but none of the intermediate certificates include **subjectInfoAccess** extensions.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test3 EE using the default settings or open and verify Signed Test Message 5.3.2.16 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA2 Cert, Basic LDAP URI Trust Anchor SubCA2 CRL
- Basic LDAP URI Trust Anchor SubSubCA2 Cert, Basic LDAP URI Trust Anchor SubSubCA2 CRL
- Rudimentary LDAP URI Path Discovery Test3 EE

4.1.2.4 Rudimentary HTTP Path Discovery Test4

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. All certificates include **authorityInfoAccess** extensions with HTTP URIs, but none of the intermediate certificates include **subjectInfoAccess** extensions.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test4 EE using the default settings or open and verify Signed Test Message 5.3.2.17 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA2 Cert, Basic HTTP URI Trust Anchor SubCA2 CRL
- Basic HTTP URI Trust Anchor SubSubCA2 Cert, Basic HTTP URI Trust Anchor SubSubCA2 CRL
- Rudimentary HTTP URI Path Discovery Test4 EE

4.1.2.5 Rudimentary LDAP Path Discovery Test5

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity

certificate. The Trust Anchor Root CA has issued two certificates to the intermediate CA, one for each key.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test5 EE using the default settings or open and verify Signed Test Message 5.3.2.18 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA3 Cert, Basic LDAP URI Trust Anchor SubCA3 Cert2, Basic LDAP URI Trust Anchor SubCA3 CRL
- Rudimentary LDAP URI Path Discovery Test5 EE

4.1.2.6 Rudimentary LDAP Path Discovery Test6

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The Trust Anchor Root CA has issued two certificates to the intermediate CA, one for each key. The end entity certificate has been revoked.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test6 EE using the default settings or open and verify Signed Test Message 5.3.2.19 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA3 Cert, Basic LDAP URI Trust Anchor SubCA3 Cert2, Basic LDAP URI Trust Anchor SubCA3 CRL
- Rudimentary LDAP URI Path Discovery Test6 EE

4.1.2.7 Rudimentary HTTP Path Discovery Test7

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The Trust Anchor Root CA has issued two certificates to the intermediate CA, one for each key.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test7 EE using the default settings or open and verify Signed Test Message 5.3.2.20 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA3 Cert, Basic HTTP URI Trust Anchor SubCA3 Cert2, Basic HTTP URI Trust Anchor SubCA3 CRL
- Rudimentary HTTP URI Path Discovery Test7 EE

4.1.2.8 Rudimentary HTTP Path Discovery Test8

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The Trust Anchor Root CA has issued two certificates to the intermediate CA, one for each key. The end entity certificate has been revoked.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test8 EE using the default settings or open and verify Signed Test Message 5.3.2.21 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA3 Cert, Basic HTTP URI Trust Anchor SubCA3 Cert2, Basic HTTP URI Trust Anchor SubCA3 CRL
- Rudimentary HTTP URI Path Discovery Test8 EE

4.1.2.9 Rudimentary LDAP Path Discovery Test9

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test9 EE using the default settings or open and verify Signed Test Message 5.3.2.22 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA4 Cert, Basic LDAP URI Trust Anchor SubCA4 CRL
- Basic LDAP URI Trust Anchor SubCA4 Self-Issued Cert

- Rudimentary LDAP URI Path Discovery Test9 EE

4.1.2.10 Rudimentary LDAP Path Discovery Test10

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate. The end entity certificate has been revoked.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test10 EE using the default settings or open and verify Signed Test Message 5.3.2.23 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA4 Cert, Basic LDAP URI Trust Anchor SubCA4 CRL
- Basic LDAP URI Trust Anchor SubCA4 Self-Issued Cert
- Rudimentary LDAP URI Path Discovery Test10 EE

4.1.2.11 Rudimentary LDAP Path Discovery Test11

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the end entity certificate. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the end entity certificate and certifies the key needed to verify the CRL.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test11 EE using the default settings or open and verify Signed Test Message 5.3.2.24 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA5 Cert, Basic LDAP URI Trust Anchor SubCA5 Self-Issued Cert, Basic LDAP URI Trust Anchor SubCA5 CRL
- Rudimentary LDAP URI Path Discovery Test11 EE

4.1.2.12 Rudimentary LDAP Path Discovery Test12

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the end entity certificate. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the end entity certificate and certifies the key needed to verify the CRL. The end entity certificate has been revoked.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test12 EE using the default settings or open and verify Signed Test Message 5.3.2.25 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA5 Cert, Basic LDAP URI Trust Anchor SubCA5 Self-Issued Cert, Basic LDAP URI Trust Anchor SubCA5 CRL
- Rudimentary LDAP URI Path Discovery Test12 EE

4.1.2.13 Rudimentary HTTP Path Discovery Test13

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test13 EE using the default settings or open and verify Signed Test Message 5.3.2.26 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA4 Cert, Basic HTTP URI Trust Anchor SubCA4 CRL
- Basic HTTP URI Trust Anchor SubCA4 Self-Issued Cert
- Rudimentary HTTP URI Path Discovery Test13 EE

4.1.2.14 Rudimentary HTTP Path Discovery Test14

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify

the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate. The end entity certificate has been revoked.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test14 EE using the default settings or open and verify Signed Test Message 5.3.2.27 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA4 Cert, Basic HTTP URI Trust Anchor SubCA4 CRL
- Basic HTTP URI Trust Anchor SubCA4 Self-Issued Cert
- Rudimentary HTTP URI Path Discovery Test14 EE

4.1.2.15 Rudimentary HTTP Path Discovery Test15

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test15 EE using the default settings or open and verify Signed Test Message 5.3.2.28 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA5 Cert, Basic HTTP URI Trust Anchor SubCA5 Self-Issued Cert, Basic HTTP URI Trust Anchor SubCA5 CRL
- Rudimentary HTTP URI Path Discovery Test15 EE

4.1.2.16 Rudimentary HTTP Path Discovery Test16

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The intermediate CA has used a different key to sign its CRL than the key used to sign the end entity certificate. The certificate issued by the Trust Anchor Root CA certifies the key needed to verify the CRL. The self-issued certificate issued by the intermediate CA is signed by the key used to sign the CRL and certifies the key needed to verify the end entity certificate. The end entity certificate has been revoked.

Procedure: Validate Rudimentary HTTP URI Path Discovery Test16 EE using the default settings or open and verify Signed Test Message 5.3.2.29 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic HTTP URI Trust Anchor SubCA5 Cert, Basic HTTP URI Trust Anchor SubCA5 Self-Issued Cert, Basic HTTP URI Trust Anchor SubCA5 CRL
- Rudimentary HTTP URI Path Discovery Test16 EE

4.1.2.17 Rudimentary LDAP Path Discovery Test17

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The first intermediate CA has issued an ARL that lists the second intermediate certificate as revoked.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test17 EE using the default settings or open and verify Signed Test Message 5.3.2.30 using the default settings.

Expected Result: The path should not validate successfully since the second intermediate certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA6 Cert, Basic LDAP URI Trust Anchor SubCA6 CRL
- Basic LDAP URI Trust Anchor SubSubCA6 Cert, Basic LDAP URI Trust Anchor SubSubCA6 CRL
- Rudimentary LDAP URI Path Discovery Test17 EE

4.1.2.18 Rudimentary LDAP Path Discovery Test18

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The directory information for the two intermediate CAs are not stored in the CAs' directory entries, but the LDAP URIs in the authorityInfoAccess, subjectInfoAccess, and cRLDistributionPoints extensions point to the directory entries that hold the information. These directory entries are not located on the LDAP server specified by the LDAP URIs, but the specified LDAP server provides a referral to the server that holds these entries.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test18 EE using the default settings or open and verify Signed Test Message 5.3.2.31 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA7 Cert, Basic LDAP URI Trust Anchor SubCA7 CRL
- Basic LDAP URI Trust Anchor SubSubCA7 Cert, Basic LDAP URI Trust Anchor SubSubCA7 CRL
- Rudimentary LDAP URI Path Discovery Test18 EE

4.1.2.19 Rudimentary LDAP Path Discovery Test19

In this test, the end entity certificate is hierarchically subordinate to the trust anchor CA. The directory information for the two intermediate CAs are not stored in the CAs' directory entries, but the LDAP URIs in the authorityInfoAccess, subjectInfoAccess, and cRLDistributionPoints extensions point to the directory entries that hold the information. These directory entries are not located on the LDAP server specified by the LDAP URIs, but the specified LDAP server provides a referral to the server that holds these entries. The end entity certificate has been revoked.

Procedure: Validate Rudimentary LDAP URI Path Discovery Test19 EE using the default settings or open and verify Signed Test Message 5.3.2.32 using the default settings.

Expected Result: The path should not validate successfully since the end entity certificate has been revoked.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic LDAP URI Trust Anchor SubCA7 Cert, Basic LDAP URI Trust Anchor SubCA7 CRL
- Basic LDAP URI Trust Anchor SubSubCA7 Cert, Basic LDAP URI Trust Anchor SubSubCA7 CRL
- Rudimentary LDAP URI Path Discovery Test19 EE

4.2 Basic Path Discovery

4.2.1 Basic Directory-based Path Discovery

4.2.1.1 Basic Directory Mesh Path Discovery Test1

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate.

Procedure: Validate Basic Directory Path Discovery Test1 EE using the default settings or open and verify Signed Test Message 5.3.2.33 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor to Basic Directory Peer 1 Cert, Basic Directory Peer 1 CRL
- Basic Directory Peer 1 to Basic Directory Peer 2 Cert, Basic Directory Peer 2 CRL
- Basic Directory Peer 2 SubCA Cert, Basic Directory Peer 2 SubCA CRL
- Basic Directory Path Discovery Test1 EE

4.2.1.2 Basic Directory Mesh Path Discovery Test2

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate.

Procedure: Validate Basic Directory Path Discovery Test2 EE using the default settings or open and verify Signed Test Message 5.3.2.34 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor to Basic Directory Peer 5 Cert, Basic Directory Peer 5 CRL
- Basic Directory Peer 5 to Basic Directory Peer 8 Cert, Basic Directory Peer 8 CRL
- Basic Directory Peer 8 to Basic Directory Peer 9 Cert, Basic Directory Peer 9 CRL
- Basic Directory Path Discovery Test2 EE

4.2.2 Basic URI based Path Discovery

4.2.2.1 Basic LDAP URI Mesh Path Discovery Test1

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate.

Procedure: Validate Basic LDAP URI Path Discovery Test1 EE using the default settings or open and verify Signed Test Message 5.3.2.47 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert, Basic LDAP URI Peer 1 CA CRL
- Basic LDAP URI Peer 1 to Basic LDAP URI Peer 2 Cert, Basic LDAP URI Peer 2 CA CRL

- Basic LDAP URI Peer 2 to Basic LDAP URI Peer 2 SubCA Cert, Basic LDAP URI Peer 2 SubCA CRL
- Basic LDAP URI Path Discovery Test1 EE

4.2.2.2 Basic HTTP URI Mesh Path Discovery Test2

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate.

Procedure: Validate Basic HTTP URI Path Discovery Test2 EE using the default settings or open and verify Signed Test Message 5.3.2.48 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic URI Trust Anchor to Basic HTTP URI Peer 1 Cert, Basic HTTP URI Peer 1 CA CRL
- Basic HTTP URI Peer 1 to Basic HTTP URI Peer 2 Cert, Basic HTTP URI Peer 2 CA CRL
- Basic HTTP URI Peer 2 to Basic HTTP URI Peer 2 SubCA Cert, Basic HTTP URI Peer 2 SubCA CRL
- Basic HTTP URI Path Discovery Test2 EE

4.2.2.3 Basic LDAP URI Mesh Path Discovery Test3

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate.

Procedure: Validate Basic LDAP URI Path Discovery Test3 EE using the default settings or open and verify Signed Test Message 5.3.2.49 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic LDAP URI Trust Anchor Root Cert, Basic LDAP URI Trust Anchor Root CRL
- Basic URI Trust Anchor to Basic LDAP URI Peer 5 Cert, Basic LDAP URI Peer 5 CA CRL
- Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert, Basic LDAP URI Peer 8 CA CRL
- Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert, Basic LDAP URI Peer 9 CA CRL
- Basic LDAP URI Path Discovery Test3 EE

4.2.2.4 Basic LDAP URI Mesh Path Discovery Test4

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate.

Procedure: Validate Basic HTTP URI Path Discovery Test4 EE using the default settings or open and verify Signed Test Message 5.3.2.50 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic HTTP URI Trust Anchor Root Cert, Basic HTTP URI Trust Anchor Root CRL
- Basic URI Trust Anchor to Basic HTTP URI Peer 5 Cert, Basic HTTP URI Peer 5 CA CRL
- Basic HTTP URI Peer 5 to Basic HTTP URI Peer 8 Cert, Basic HTTP URI Peer 8 CA CRL
- Basic HTTP URI Peer 8 to Basic HTTP URI Peer 9 Cert, Basic HTTP URI Peer 9 CA CRL
- Basic HTTP URI Path Discovery Test4 EE

4.2.3 Basic Combined Path Discovery

4.2.3.1 Basic Combined Mesh Path Discovery Test1

In this test, there is a non-hierarchical mesh between the trust anchor and the end entity certificate. The certificates and CRLs that are issued by CAs "closest" to the trust anchor do not include URIs. The end entity certificate includes LDAP URIs and the final intermediate certificate includes HTTP URIs.

Procedure: Validate Basic Combined Path Discovery OU4 EE1 using the default settings or open and verify Signed Test Message 5.3.2.75 using the default settings.

Expected Result: The path should validate successfully.

Certification Path: The certification path is composed of the following objects:

- Basic Directory Trust Anchor Root Cert, Basic Directory Trust Anchor Root CRL
- Basic Directory Trust Anchor to Bridge Directory Cert, Basic Directory Bridge CA ARL1
- Basic Directory Bridge to Combined OU4 CA Cert, Basic Combined OU4 CA CRL
- Basic Combined OU4 to OU4 subCA Cert, Basic Combined OU4 subCA CRL
- Basic Combined Path Discovery OU4 EE1

4.2.4 Additional Basic Bridge Path Discovery Tests

In each of the three basic level PKI architectures (Directory, LDAP URI, and HTTP URI), the trust anchor CA is cross-certified with a "bridge" CA which has in turn cross-certified several

"organizational" CAs. The certificates and CRLs of the bridge CA and the organizational CAs are nearly identical in all three architectures with the only significant differences lying in the methods by which the certificates and CRLs needed for path validation may be located. In each case, the trust anchor has issued two certificates to the bridge CA with each certificate containing different policy information. This section provides a brief description of each of the organizational PKIs that are cross-certified with the bridge along including information about the end entity certificates issued within each organization.

4.2.4.1 Organization 1

Organization 1 (OU1) operates a single CA that issues certificates under four different policies only three of which are mapped to policies at the bridge CA. The bridge CA has issued a cross-certificate to OU1 that includes the mapping information for these three policies and that includes a name constraints extension limiting OU1 to OU1's name space. The following end entity certificates have been issued by OU1:

Basic Directory Path Discovery OU1 EE1:
Basic LDAP URI Path Discovery OU1 EE1:
Basic HTTP URI Path Discovery OU1 EE1:

> These certificates assert certificate policy 2.16.840.1.101.3.2.1.48.37, which maps to 2.16.840.1.101.3.2.1.48.7 at the trust anchor.

Basic Directory Path Discovery OU1 EE2:
Basic LDAP URI Path Discovery OU1 EE2:
Basic HTTP URI Path Discovery OU1 EE2:

> These certificates assert certificate policy 2.16.840.1.101.3.2.1.48.38, which maps to 2.16.840.1.101.3.2.1.48.1 and 2.16.840.1.101.3.2.1.48.3 at the trust anchor.

Basic Directory Path Discovery OU1 EE3:
Basic LDAP URI Path Discovery OU1 EE3:
Basic HTTP URI Path Discovery OU1 EE3:

> These certificates assert certificate policy 2.16.840.1.101.3.2.1.48.39, which maps to 2.16.840.1.101.3.2.1.48.10 at the trust anchor.

Basic Directory Path Discovery OU1 EE4:
Basic LDAP URI Path Discovery OU1 EE4:
Basic HTTP URI Path Discovery OU1 EE4:

> These certificates assert certificate policy 2.16.840.1.101.3.2.1.48.40. Since cross-certificate from bridge CA to the OU1 CA does not include any mapping to 2.16.840.1.101.3.2.1.48.40 and since both cross-certificates from the trust anchor to the bridge CA include a policyConstraints extension with requireExplicitPolicy set to 0, there certificates are not valid.

Basic Directory Path Discovery OU1 EE5:
Basic LDAP URI Path Discovery OU1 EE5:
Basic HTTP URI Path Discovery OU1 EE5:

> The subject names in these certificates do not satisfy the name constraints extension in the cross-certificate from the bridge CA to the OU1 CA and so these certificates are not valid.

4.2.4.2 Organization 2

Organization 2 (Org2) operates a single CA that has maintains four key pairs as a result of having performed key rollover three times. After each key rollover two self-issued certificates were created, one containing the new public key signed by the previous private key and one containing the previous public key signed by the new private key. The CRLs are signed by the newest private key, but the bridge CA cross-certified with second newest key pair. All of the end entity certificates assert two certificate policies. One policy maps to 2.16.840.1.101.3.2.1.48.1 and 2.16.840.1.101.3.2.1.48.3 at the trust anchor while the other policy does not map to any other policies. In the Directory and LDAP URI architectures, LDAP referrals must be followed in order to obtain the information from Org2's directory entry. The end entity certificates differ by the key used to sign them and the CRL distribution point that they reference. Some of the certificates have been revoked.

Basic Directory Path Discovery Org2 EE1:
Basic LDAP URI Path Discovery Org2 EE1:
Basic HTTP URI Path Discovery Org2 EE1:

These certificates were signed by the private key corresponding to the public key that was certified by the bridge CA.

Basic Directory Path Discovery Org2 EE2:
Basic LDAP URI Path Discovery Org2 EE2:
Basic HTTP URI Path Discovery Org2 EE2:

These certificates were signed by the private key corresponding to the public key that was certified by the bridge CA and they have been revoked.

Basic Directory Path Discovery Org2 EE3:
Basic LDAP URI Path Discovery Org2 EE3:
Basic HTTP URI Path Discovery Org2 EE3:

These certificates were signed by the private key that was generated prior to the key pair that was certified by the bridge CA.

Basic Directory Path Discovery Org2 EE4:
Basic LDAP URI Path Discovery Org2 EE4:
Basic HTTP URI Path Discovery Org2 EE4:

These certificates were signed by the private key that was generated prior to the key pair that was certified by the bridge CA and they have been revoked.

Basic Directory Path Discovery Org2 EE5:
Basic LDAP URI Path Discovery Org2 EE5:
Basic HTTP URI Path Discovery Org2 EE5:

These certificates were signed by the oldest private key. The self-issued certificate with the oldest public key, signed by the second oldest private key, has been revoked and so these certificates cannot be validated.

4.2.4.3 Organization 3

Organization 3 (OU3) operates 3 CAs: a principal CA that is cross-certified with the bridge CA; a peer CA that is cross-certified with the principal CA; and a subordinate CA that has been issued a certificate by the principal CA. The cross-certificate from the bridge CA to the principal CA includes a name constraints extension that is not satisfied by the cross-certificate from the principal

CA to the peer CA. This cross-certificate asserts two certificate policies, one which is mapped to policies used by OU3 and one which is not mapped.

Basic Directory Path Discovery OU3 EE1:
Basic LDAP URI Path Discovery OU3 EE1:
Basic HTTP URI Path Discovery OU3 EE1:

These certificates were issued by the subordinate CA and each assert the four certificate policies including one that maps to 2.16.840.1.101.3.2.1.48.10 at the trust anchor.

Basic Directory Path Discovery OU3 EE2:
Basic LDAP URI Path Discovery OU3 EE2:
Basic HTTP URI Path Discovery OU3 EE2:

These certificates were issued by the subordinate CA and assert the certificate policy that was included in the cross-certificate from the bridge CA to the OU3 principal CA (2.16.840.1.101.3.2.1.48.2). This policy is also asserted in the cross-certificate from the trust anchor to the bridge CA that does not include a policy mappings extension. Thus, validating these certificates requires the use of a different cross-certificate from the trust anchor to the bridge CA than is used to validate all of the other end entity certificates.

5 Test Data Descriptions

This section describes the entire test data (certificates, CRLs, etc.,) used in the test procedures.

Each of the different types of test data is described in the following sections.

5.1 X.509 Certificates and CRLs

Each test certificate is based on one of several general certificates. These general, or base certificates, contain fields and values typically found in all of the certificates. Each test certificate will refer to exactly one base certificate. Only the differences between the test certificate and the base certificate will be listed so as not to have to repeat the same information in this document.

5.1.1 Base Root Certificate

ASN.1 Field or Type Name	Critical Flag	ASN. 1 Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer value of "2" indicates a version 3 certificate.
serialNumber			
CertificateSerialNumber		{ Always specified – no default }	Always specified
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	Uses RFC 2253 format.
validity			
notBefore			
Time			
UTCTime		050527145720Z	27 May 2005, 14:57:20 GMT

notAfter			
Time			
UTCTime		150819145720Z	19 August 2015, 14:57:20 GMT
subject			
Name		{ Always specified – no default }	Uses RFC 2253 format.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	
subjectPublicKey			
BIT STRING			Encapsulated form of RSAPublicKey
RSAPublicKey			
modulus		{Automatically generated}	Length is 1024 bits
publicExponent		65537	
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the subject public key.
basicConstraints	TRUE		
cA		TRUE	
pathLenConstraint		INTEGER	not present unless otherwise specified
KeyUsage	TRUE		
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	
cRLSign		1	
encipherOnly		0	
decipherOnly		0	
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.5	RSA with SHA-1
parameters		NULL	
signatureValue		BIT STRING	Signature calculated

5.1.2 Base Intermediate Certificate

ASN.1 Field or Type Name	Critical Flag	ASN. 1 Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber			
CertificateSerialNumber		{ Always specified – no default }	Always specified
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	X.500 Distinguished name of the issuer of the certificate.
validity			
notBefore			
Time			

UTCTime		050527145720Z	27 May 2005, 14:57:20 GMT
notAfter			
Time			
UTCTime		150819145720Z	19 August 2015, 14:57:20 GMT
subject			
Name		{ Always specified – no default }	X.500 Distinguished name of the owner of the certificate.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	
subjectPublicKey		BIT STRING	Contains the subject public key
BIT STRING			Encapsulated form of RSAPublicKey
RSAPublicKey			
modulus		{Automatically generated}	Length is 1024 bits
publicExponent		65537	
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the subject public key.
basicConstraints	TRUE		
cA		TRUE	
pathLenConstraint		INTEGER	not present unless otherwise specified
keyUsage	TRUE		
digitalSignature		0	
nonRepudiation		0	
keyEncipherment		0	
dataEncipherment		0	
keyAgreement		0	
keyCertSign		1	
cRLSign		1	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		No policy qualifiers included
PolicyInformation			
policyIdentifier			
CertPolicyId		NIST-test-policy-1	id-test-certificate-policy-1
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	
signatureValue		BIT STRING	Signature calculated

5.1.3 Base End Certificate

ASN.1 Field or Type Name	Critical Flag	ASN. 1 Value	Comments
Certificate			
tbsCertificate			Fields to be signed.
version		2	Integer Value of "2" for Version 3 certificate.
serialNumber			
CertificateSerialNumber		{ Always specified – no default }	Always specified
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	

issuer			
Name		{ Always specified – no default }	X.500 Distinguished name of the issuer of the certificate.
validity			
notBefore			
Time			
UTCTime		050527145720Z	27 May 2005, 14:57:20 GMT
notAfter			
Time			
UTCTime		150819145720Z	19 August 2015, 14:57:20 GMT
subject			
Name		{ Always specified – no default }	X.500 Distinguished name of the owner of the certificate.
subjectPublicKeyInfo			
algorithm			
AlgorithmIdentifier			Public key algorithm used.
algorithm		1.2.840.113549.1.1.1	RSA Encryption
parameters		NULL	
subjectPublicKey		BIT STRING	Contains the subject public key
BIT STRING			Encapsulated form of RSAPublicKey
RSAPublicKey			
modulus		{Automatically generated}	Length is 1024 bits
publicExponent		65537	
extensions			
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
subjectKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the subject public key.
basicConstraints	FALSE		this extension absent unless otherwise specified
cA		FALSE	
pathLenConstraint		{ Absent }	
keyUsage	TRUE		
digitalSignature		1	
nonRepudiation		1	
keyEncipherment		1	
dataEncipherment		1	
keyAgreement		0	
keyCertSign		0	
cRLSign		0	
encipherOnly		0	
decipherOnly		0	
certificatePolicies	FALSE		No policy qualifiers included
PolicyInformation			
policyIdentifier			
CertPolicyId		NIST-test-policy-1	id-test-certificate-policy-1
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters			
signatureValue		BIT STRING	Signature calculated

5.1.4 Base CRL

Field	Critical Flag	Value	Comments
CertificateList			
tbsCertList			Fields to be signed.
version		1	Integer Value of "1" for Version 2 CRL.
signature			
AlgorithmIdentifier			Must match Algorithm Identifier in

			signatureAlgorithm field.
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	
issuer			
Name		{ Always specified – no default }	X.500 Distinguished name of the issuer of the CRL.
thisUpdate			
Time			
UTCTime		050603214547Z	03 June 2005, 21:45:47 GMT
nextUpdate			
Time			
UTCTime		150601214547Z	01 June 2015, 21:45:47 GMT
revokedCertificates			absent unless otherwise specified
userCertificate			
CertificateSerialNumber			
revocationDate			
Time			
UTCTime		050527152305Z	27 May 2005, 15:23:05 GMT
crlEntryExtensions			
reasonCode	FALSE		
CRLReason		keyCompromise	
crlExtensions			
crlNumber	FALSE	1	
authorityKeyIdentifier	FALSE		
keyIdentifier		OCTET STRING	Derived using the SHA-1 hash of the issuer public key.
signatureAlgorithm			
AlgorithmIdentifier			
algorithm		1.2.840.113549.1.1.5	SHA-1WithRSAEncryption
parameters		NULL	
signatureValue		BIT STRING	signature calculated

5.1.5 Trust Anchors

5.1.5.1 Basic Directory Trust Anchor Root Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
self-signed

5.1.5.2 Basic Directory Trust Anchor Root CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert
post to certificateRevocationList

5.1.5.3 Basic LDAP URI Trust Anchor Root Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certific
ates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.5.4 Basic LDAP URI Trust Anchor Root CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor Root Cert
post to certificateRevocationList

5.1.5.5 Basic HTTP URI Trust Anchor Root Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1.p7c"
self-signed

5.1.5.6 Basic HTTP URI Trust Anchor Root CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.6 Rudimentary Path Discovery Directory Certificates and CRLs

5.1.6.1 Basic Directory Trust Anchor SubCA1 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA1, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.2 Basic Directory Trust Anchor SubCA1 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA1, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA1 Cert
post to certificateRevocationList

5.1.6.3 Basic Directory Trust Anchor SubSubCA1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA1, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubSubCA1, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA1 Cert

5.1.6.4 Basic Directory Trust Anchor SubSubCA1 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubSubCA1, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubSubCA1 Cert
post to certificateRevocationList

5.1.6.5 Rudimentary Directory Path Discovery Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubSubCA1, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test1, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubSubCA1 Cert

5.1.6.6 Basic Directory Trust Anchor SubCA2 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA2, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.7 Basic Directory Trust Anchor SubCA2 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA2, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA2 Cert
post to certificateRevocationList

5.1.6.8 Basic Directory Trust Anchor SubSubCA2 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA2, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubSubCA2, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA2 Cert

5.1.6.9 Basic Directory Trust Anchor SubSubCA2 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubSubCA2, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubSubCA2 Cert
post to certificateRevocationList

5.1.6.10 Rudimentary Directory Path Discovery Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubSubCA2, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test2, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubSubCA2 Cert

5.1.6.11 Basic Directory Trust Anchor SubCA3 Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA3, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.12 Basic Directory Trust Anchor SubCA3 Cert2:

base: Base Intermediate Certificate
serial number: 7
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA3, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.13 Basic Directory Trust Anchor SubCA3 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA3, o=Test Certificates, c=US"
revokedCertificates:
    serialNumber: 2
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic Directory Trust Anchor SubCA3 Cert2
post to certificateRevocationList

5.1.6.14 Rudimentary Directory Path Discovery Test3 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA3, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test3, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA3 Cert

5.1.6.15 Rudimentary Directory Path Discovery Test4 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Directory Trust Anchor SubCA3, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test4, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA3 Cert

5.1.6.16 Basic Directory Trust Anchor SubCA4 Cert:

base: Base Intermediate Certificate
serial number: 12
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA4, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.17 Basic Directory Trust Anchor SubCA4 Self-Issued Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA4, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA4 Cert

5.1.6.18 Basic Directory Trust Anchor SubCA4 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA4, o=Test Certificates, c=US"
revokedCertificates:
    serialNumber: 3
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic Directory Trust Anchor SubCA4 Cert
post to certificateRevocationList

5.1.6.19 Rudimentary Directory Path Discovery Test5 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Directory Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test5, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA4 Self-Issued Cert

5.1.6.20 Rudimentary Directory Path Discovery Test6 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic Directory Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test6, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA4 Self-Issued Cert

5.1.6.21 Basic Directory Trust Anchor SubCA5 Cert:

base: Base Intermediate Certificate
serial number: 13
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.22 Basic Directory Trust Anchor SubCA5 ARL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical
        onlyContainsAuthorityCerts: TRUE
signed by Basic Directory Trust Anchor SubCA5 Cert

post to authorityRevocationList

5.1.6.23 Basic Directory Trust Anchor SubCA5 Self-Issued Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA5 Cert

5.1.6.24 Basic Directory Trust Anchor SubCA5 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
revokedCertificates:
    serialNumber: 3
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic Directory Trust Anchor SubCA5 Self-Issued Cert
post to certificateRevocationList

5.1.6.25 Rudimentary Directory Path Discovery Test7 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test7, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA5 Cert

5.1.6.26 Rudimentary Directory Path Discovery Test8 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic Directory Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test8, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA5 Cert

5.1.6.27 Basic Directory Trust Anchor SubCA6 Cert:

base: Base Intermediate Certificate
serial number: 18
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA6, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.28 Basic Directory Trust Anchor SubCA6 ARL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA6, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical

onlyContainsAuthorityCerts: TRUE
revokedCertificates:
serialNumber: 1
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
signed by Basic Directory Trust Anchor SubCA6 Cert
post to authorityRevocationList

5.1.6.29 Basic Directory Trust Anchor SubSubCA6 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA6, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubSubCA6, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA6 Cert

5.1.6.30 Basic Directory Trust Anchor SubSubCA6 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubSubCA6, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 36
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
affiliationChanged
signed by Basic Directory Trust Anchor SubSubCA6 Cert
post to certificateRevocationList

5.1.6.31 Rudimentary Directory Path Discovery Test9 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic Directory Trust Anchor SubSubCA6, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test9, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubSubCA6 Cert

5.1.6.32 Basic Directory Trust Anchor SubCA7 Cert:

base: Base Intermediate Certificate
serial number: 19
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubCA7, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.33 Basic Directory Trust Anchor SubCA7 CRL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA7, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
onlyContainsUserCerts: TRUE

revokedCertificates:
    serialNumber: 1
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic Directory Trust Anchor SubCA7 Cert
post to certificateRevocationList at "cn=Basic Directory Trust Anchor SubCA7 EECRL, o=Test Certificates, c=US"

5.1.6.34 Basic Directory Trust Anchor SubCA7 ARL:

base: Base CRL
issuer: "cn=Basic Directory Trust Anchor SubCA7, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical
        onlyContainsAuthorityCerts: TRUE
revokedCertificates:
    serialNumber: 2
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                cACompromise
signed by Basic Directory Trust Anchor SubCA7 Cert
post to authorityRevocationList at "cn=Basic Directory Trust Anchor SubCA7 ARL, o=Test Certificates, c=US"

5.1.6.35 Rudimentary Directory Path Discovery Test10 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubCA7, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test10, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=Basic Directory Trust Anchor SubCA7 EECRL, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubCA7 Cert

5.1.6.36 Basic Directory Trust Anchor SubSubCA7 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Trust Anchor SubCA7, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor SubSubCA7, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=Basic Directory Trust Anchor SubCA7 ARL, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubCA7 Cert

5.1.6.37 Basic Directory Trust Anchor SubSubCA7 CRL:

base: Base CRL

issuer: "cn=Basic Directory Trust Anchor SubSubCA7, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor SubSubCA7 Cert
post to certificateRevocationList

5.1.6.38 Rudimentary Directory Path Discovery Test11 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic Directory Trust Anchor SubSubCA7, o=Test Certificates, c=US"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test11, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubSubCA7 Cert

5.1.6.39 Basic Directory Trust Anchor SubCA8 Cert:

base: Base Intermediate Certificate
serial number: 30
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "dc=BasicSubCA8, dc=testcertificates, dc=gov"
signed by Basic Directory Trust Anchor Root Cert

5.1.6.40 Basic Directory Trust Anchor SubCA8 CRL:

base: Base CRL
issuer: "dc=BasicSubCA8, dc=testcertificates, dc=gov"
signed by Basic Directory Trust Anchor SubCA8 Cert
post to certificateRevocationList

5.1.6.41 Basic Directory Trust Anchor SubSubCA8 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "dc=BasicSubCA8, dc=testcertificates, dc=gov"
subject: "dc=BasicSubSubCA8, dc=testcertificates, dc=gov"
signed by Basic Directory Trust Anchor SubCA8 Cert

5.1.6.42 Basic Directory Trust Anchor SubSubCA8 CRL:

base: Base CRL
issuer: "dc=BasicSubSubCA8, dc=testcertificates, dc=gov"
revokedCertificates:
    serialNumber: 2
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic Directory Trust Anchor SubSubCA8 Cert
post to certificateRevocationList

5.1.6.43 Rudimentary Directory Path Discovery Test12 EE:

base: Base End Certificate
serial number: 1
issuer: "dc=BasicSubSubCA8, dc=testcertificates, dc=gov"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test12, o=Test Certificates, c=US"
subjectAltNameExtension:

rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubSubCA8 Cert

5.1.6.44 Rudimentary Directory Path Discovery Test13 EE:

base: Base End Certificate
serial number: 2
issuer: "dc=BasicSubSubCA8, dc=testcertificates, dc=gov"
subject: "cn=Rudimentary Directory Path Discovery EE Certificate Test13, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Trust Anchor SubSubCA8 Cert

5.1.7 Rudimentary Path Discovery LDAP URI Certificates and CRLs

5.1.7.1 Basic LDAP URI Trust Anchor SubCA1 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA1, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.2 Basic LDAP URI Trust Anchor SubCA1 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA1, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor SubCA1 Cert
post to certificateRevocationList

5.1.7.3 Basic LDAP URI Trust Anchor SubSubCA1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA1, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubSubCA1, o=Test Certificates, c=US"

authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA1,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor SubCA1 Cert

5.1.7.4 Basic LDAP URI Trust Anchor SubSubCA1 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA1, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor SubSubCA1 Cert
post to certificateRevocationList

5.1.7.5 Rudimentary LDAP URI Path Discovery Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA1, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test1, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA1,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubSubCA1 Cert

5.1.7.6 Basic LDAP URI Trust Anchor SubCA2 Cert:

base: Base Intermediate Certificate

serial number: 4
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA2, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.7 Basic LDAP URI Trust Anchor SubCA2 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA2, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor SubCA2 Cert
post to certificateRevocationList

5.1.7.8 Basic LDAP URI Trust Anchor SubSubCA2 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA2, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubSubCA2, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA2,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA2,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor SubCA2 Cert

5.1.7.9 Basic LDAP URI Trust Anchor SubSubCA2 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA2, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor SubSubCA2 Cert
post to certificateRevocationList

5.1.7.10 Rudimentary LDAP URI Path Discovery Test3 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA2, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test3, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA2,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA2,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubSubCA2 Cert

5.1.7.11 Basic LDAP URI Trust Anchor SubCA3 Cert:

base: Base Intermediate Certificate
serial number: 8
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.12 Basic LDAP URI Trust Anchor SubCA3 Cert2:

base: Base Intermediate Certificate
serial number: 9
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
authorityInfoAccess: not critical

AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certific
ates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA3,o=Te
st%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certific
ates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.13 Basic LDAP URI Trust Anchor SubCA3 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 2
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic LDAP URI Trust Anchor SubCA3 Cert2
post to certificateRevocationList

5.1.7.14 Rudimentary LDAP URI Path Discovery Test5 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test5, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA3,o=Te
st%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA3,o=Te
st%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"

signed by Basic LDAP URI Trust Anchor SubCA3 Cert

5.1.7.15 Rudimentary LDAP URI Path Discovery Test6 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test6, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA3,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubCA3 Cert

5.1.7.16 Basic LDAP URI Trust Anchor SubCA4 Cert:

base: Base Intermediate Certificate
serial number: 14
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.17 Basic LDAP URI Trust Anchor SubCA4 Self-Issued Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor SubCA4 Cert

5.1.7.18 Basic LDAP URI Trust Anchor SubCA4 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic LDAP URI Trust Anchor SubCA4 Cert
post to certificateRevocationList

5.1.7.19 Rudimentary LDAP URI Path Discovery Test9 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test9, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical

distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubCA4 Self-Issued Cert

5.1.7.20 Rudimentary LDAP URI Path Discovery Test10 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic LDAP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test10, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA4,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubCA4 Self-Issued Cert

5.1.7.21 Basic LDAP URI Trust Anchor SubCA5 Cert:

base: Base Intermediate Certificate
serial number: 15
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certific
ates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.22 Basic LDAP URI Trust Anchor SubCA5 ARL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
onlyContainsAuthorityCerts: TRUE
signed by Basic LDAP URI Trust Anchor SubCA5 Cert
post to authorityRevocationList

5.1.7.23 Basic LDAP URI Trust Anchor SubCA5 Self-Issued Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Te
st%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Te
st%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Te
st%20Certificates,c=US?authorityRevocationList;binary"
signed by Basic LDAP URI Trust Anchor SubCA5 Cert

5.1.7.24 Basic LDAP URI Trust Anchor SubCA5 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic LDAP URI Trust Anchor SubCA5 Self-Issued Cert
post to certificateRevocationList

5.1.7.25 Rudimentary LDAP URI Path Discovery Test11 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test11, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubCA5 Cert

5.1.7.26 Rudimentary LDAP URI Path Discovery Test12 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic LDAP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test12, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA5,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubCA5 Cert

5.1.7.27 Basic LDAP URI Trust Anchor SubCA6 Cert:

base: Base Intermediate Certificate
serial number: 20
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA6, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers

accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA6,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.28 Basic LDAP URI Trust Anchor SubCA6 ARL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA6, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
onlyContainsAuthorityCerts: TRUE
revokedCertificates:
serialNumber: 1
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
signed by Basic LDAP URI Trust Anchor SubCA6 Cert
post to authorityRevocationList at "cn=Basic LDAP URI Trust Anchor SubCA6 ARL, o=Test Certificates, c=US"

5.1.7.29 Basic LDAP URI Trust Anchor SubSubCA6 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA6, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubSubCA6, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA6,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA6,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubCA6 ARL,o=Test%20Certificates,c=US?authorityRevocationList;binary"
signed by Basic LDAP URI Trust Anchor SubCA6 Cert

5.1.7.30 Basic LDAP URI Trust Anchor SubSubCA6 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA6, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor SubSubCA6 Cert
post to certificateRevocationList

5.1.7.31 Rudimentary LDAP URI Path Discovery Test17 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA6, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test17, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA6,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor%20SubSubCA6,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubSubCA6 Cert

5.1.7.32 Basic LDAP URI Trust Anchor SubCA7 Cert:

base: Base Intermediate Certificate
serial number: 31
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubCA7, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical

AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubCA7,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.7.33 Basic LDAP URI Trust Anchor SubCA7 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubCA7, o=Test Certificates, c=US"
signed by Basic LDAP URI Trust Anchor SubCA7 Cert
post to certificateRevocationList at "dc=BasicLDAPURISubCA7,dc=testcertificates,dc=gov"

5.1.7.34 Basic LDAP URI Trust Anchor SubSubCA7 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubCA7, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor SubSubCA7, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubCA7,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubSubCA7,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubCA7,dc=testcertificates,dc=gov?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor SubCA7 Cert

5.1.7.35 Basic LDAP URI Trust Anchor SubSubCA7 CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA7, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 2

crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic LDAP URI Trust Anchor SubSubCA7 Cert
post to certificateRevocationList at "dc=BasicLDAPURISubSubCA7,dc=testcertificates,dc=gov"

5.1.7.36 Rudimentary LDAP URI Path Discovery Test18 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA7, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test18, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubSubCA7,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubSubCA7,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubSubCA7 Cert

5.1.7.37 Rudimentary LDAP URI Path Discovery Test19 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Trust Anchor SubSubCA7, o=Test Certificates, c=US"
subject: "cn=Rudimentary LDAP URI Path Discovery EE Certificate Test19, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubSubCA7,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/dc=BasicLDAPURISubSubCA7,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Trust Anchor SubSubCA7 Cert

5.1.8 Rudimentary Path Discovery HTTP URI Certificates and CRLs

5.1.8.1 Basic HTTP URI Trust Anchor SubCA1 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA1, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.8.2 Basic HTTP URI Trust Anchor SubCA1 CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor SubCA1, o=Test Certificates, c=US"
signed by Basic HTTP URI Trust Anchor SubCA1 Cert

5.1.8.3 Basic HTTP URI Trust Anchor SubSubCA1 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubCA1, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubSubCA1, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubSubCA1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA1CRL.crl"
signed by Basic HTTP URI Trust Anchor SubCA1 Cert

5.1.8.4 Basic HTTP URI Trust Anchor SubSubCA1 CRL:

base: Base CRL

issuer: "cn=Basic HTTP URI Trust Anchor SubSubCA1, o=Test Certificates, c=US"
signed by Basic HTTP URI Trust Anchor SubSubCA1 Cert

5.1.8.5 Rudimentary HTTP URI Path Discovery Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubSubCA1, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test2, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubSubCA1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubSubCA1CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubSubCA1 Cert

5.1.8.6 Basic HTTP URI Trust Anchor SubCA2 Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA2, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.8.7 Basic HTTP URI Trust Anchor SubCA2 CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor SubCA2, o=Test Certificates, c=US"
signed by Basic HTTP URI Trust Anchor SubCA2 Cert

5.1.8.8 Basic HTTP URI Trust Anchor SubSubCA2 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubCA2, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubSubCA2, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:

URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA2.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA2CRL.crl"
signed by Basic HTTP URI Trust Anchor SubCA2 Cert

5.1.8.9 Basic HTTP URI Trust Anchor SubSubCA2 CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor SubSubCA2, o=Test Certificates, c=US"
signed by Basic HTTP URI Trust Anchor SubSubCA2 Cert

5.1.8.10 Rudimentary HTTP URI Path Discovery Test4 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubSubCA2, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test4, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubSubCA2.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubSubCA2CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubSubCA2 Cert

5.1.8.11 Basic HTTP URI Trust Anchor SubCA3 Cert:

base: Base Intermediate Certificate
serial number: 10
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA3.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.8.12 Basic HTTP URI Trust Anchor SubCA3 Cert2:

base: Base Intermediate Certificate
serial number: 11
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA3.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.8.13 Basic HTTP URI Trust Anchor SubCA3 CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
revokedCertificates:
    serialNumber: 2
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic HTTP URI Trust Anchor SubCA3 Cert2

5.1.8.14 Rudimentary HTTP URI Path Discovery Test7 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test7, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA3.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA3CRL.crl"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubCA3 Cert

5.1.8.15 Rudimentary HTTP URI Path Discovery Test8 EE:

base: Base End Certificate

serial number: 2
issuer: "cn=Basic HTTP URI Trust Anchor SubCA3, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test8, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA3.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA3CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubCA3 Cert

5.1.8.16 Basic HTTP URI Trust Anchor SubCA4 Cert:

base: Base Intermediate Certificate
serial number: 16
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA4.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.8.17 Basic HTTP URI Trust Anchor SubCA4 Self-Issued Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA4.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA4.p7c"
cRLDistributionPoints: not critical

distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA4CRL.crl"
signed by Basic HTTP URI Trust Anchor SubCA4 Cert

5.1.8.18 Basic HTTP URI Trust Anchor SubCA4 CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic HTTP URI Trust Anchor SubCA4 Cert

5.1.8.19 Rudimentary HTTP URI Path Discovery Test13 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test13, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA4.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA4CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubCA4 Self-Issued Cert

5.1.8.20 Rudimentary HTTP URI Path Discovery Test14 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic HTTP URI Trust Anchor SubCA4, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test14, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA4.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA4CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubCA4 Self-Issued Cert

5.1.8.21 Basic HTTP URI Trust Anchor SubCA5 Cert:

base: Base Intermediate Certificate
serial number: 17
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA5.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.8.22 Basic HTTP URI Trust Anchor SubCA5 ARL:

base: Base CRL
issuer: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical
        onlyContainsAuthorityCerts: TRUE
signed by Basic HTTP URI Trust Anchor SubCA5 Cert

5.1.8.23 Basic HTTP URI Trust Anchor SubCA5 Self-Issued Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA5.p7c"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1SubCA5.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA5ARL.crl"
signed by Basic HTTP URI Trust Anchor SubCA5 Cert

5.1.8.24 Basic HTTP URI Trust Anchor SubCA5 CRL:

base: Base CRL

issuer: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
revokedCertificates:
serialNumber: 3
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic HTTP URI Trust Anchor SubCA5 Self-Issued Cert

5.1.8.25 Rudimentary HTTP URI Path Discovery Test15 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test15, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA5.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA5CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubCA5 Cert

5.1.8.26 Rudimentary HTTP URI Path Discovery Test16 EE:

base: Base End Certificate
serial number: 3
issuer: "cn=Basic HTTP URI Trust Anchor SubCA5, o=Test Certificates, c=US"
subject: "cn=Rudimentary HTTP URI Path Discovery EE Certificate Test16, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1SubCA5.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorSubCA5CRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Trust Anchor SubCA5 Cert

5.1.9 Basic Path Discovery Directory Certificates and CRLs

5.1.9.1 Basic Directory Trust Anchor to Basic Directory Peer 1 Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 1 CA, o=Test Certificates, c=US"

signed by Basic Directory Trust Anchor Root Cert

5.1.9.2 Basic Directory Peer 1 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 1 CA, o=Test Certificates, c=US"
signed by Basic Directory Trust Anchor to Basic Directory Peer 1 Cert
post to certificateRevocationList

5.1.9.3 Basic Directory Peer 1 to Basic Directory Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 1 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
public key from Basic Directory Trust Anchor Root Cert
signed by Basic Directory Trust Anchor to Basic Directory Peer 1 Cert

5.1.9.4 Basic Directory Peer 2 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
self-signed

5.1.9.5 Basic Directory Peer 2 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 2 CA Cert
post to certificateRevocationList

5.1.9.6 Basic Directory Peer 1 to Basic Directory Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 1 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 2 CA Cert
signed by Basic Directory Trust Anchor to Basic Directory Peer 1 Cert

5.1.9.7 Basic Directory Peer 2 to Basic Directory Peer 1 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 1 CA, o=Test Certificates, c=US"
public key from Basic Directory Trust Anchor to Basic Directory Peer 1 Cert
signed by Basic Directory Peer 2 CA Cert

5.1.9.8 Basic Directory Peer 3 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 3 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 3 CA, o=Test Certificates, c=US"
self-signed

5.1.9.9 Basic Directory Peer 3 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 3 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 3 CA Cert
post to certificateRevocationList

5.1.9.10 Basic Directory Peer 3 to Basic Directory Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 3 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 2 CA Cert
signed by Basic Directory Peer 3 CA Cert

5.1.9.11 Basic Directory Peer 4 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 4 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 4 CA, o=Test Certificates, c=US"
self-signed

5.1.9.12 Basic Directory Peer 4 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 4 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 4 CA Cert
post to certificateRevocationList

5.1.9.13 Basic Directory Peer 4 to Basic Directory Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 4 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 2 CA Cert
signed by Basic Directory Peer 4 CA Cert

5.1.9.14 Basic Directory Peer 2 SubCA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic Directory Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 2 SubCA, o=Test Certificates, c=US"
signed by Basic Directory Peer 2 CA Cert

5.1.9.15 Basic Directory Peer 2 SubCA CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 2 SubCA, o=Test Certificates, c=US"
signed by Basic Directory Peer 2 SubCA Cert
post to certificateRevocationList

5.1.9.16 Basic Directory Path Discovery Test1 EE:

base: Base End Certificate

serial number: 1
issuer: "cn=Basic Directory Peer 2 SubCA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery EE Certificate Test1, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Peer 2 SubCA Cert

5.1.9.17 Basic Directory Peer 5 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
self-signed

5.1.9.18 Basic Directory Peer 5 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 5 CA Cert
post to certificateRevocationList

5.1.9.19 Basic Directory Trust Anchor to Basic Directory Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 5 CA Cert
signed by Basic Directory Trust Anchor Root Cert

5.1.9.20 Basic Directory Peer 5 to Basic Directory Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
public key from Basic Directory Trust Anchor Root Cert
signed by Basic Directory Peer 5 CA Cert

5.1.9.21 Basic Directory Peer 6 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 6 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 6 CA, o=Test Certificates, c=US"
self-signed

5.1.9.22 Basic Directory Peer 6 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 6 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 6 CA Cert
post to certificateRevocationList

5.1.9.23 Basic Directory Peer 6 to Basic Directory Peer 5 Cert:

base: Base Intermediate Certificate

serial number: 2
issuer: "cn=Basic Directory Peer 6 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 5 CA Cert
signed by Basic Directory Peer 6 CA Cert

5.1.9.24 Basic Directory Peer 7 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 7 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 7 CA, o=Test Certificates, c=US"
self-signed

5.1.9.25 Basic Directory Peer 7 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 7 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 7 CA Cert
post to certificateRevocationList

5.1.9.26 Basic Directory Peer 7 to Basic Directory Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 7 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 5 CA Cert
signed by Basic Directory Peer 7 CA Cert

5.1.9.27 Basic Directory Peer 5 to Basic Directory Peer 8 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 8 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 5 CA Cert

5.1.9.28 Basic Directory Peer 8 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 8 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 5 to Basic Directory Peer 8 Cert
post to certificateRevocationList

5.1.9.29 Basic Directory Peer 8 to Basic Directory Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 8 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 5 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 5 CA Cert
signed by Basic Directory Peer 5 to Basic Directory Peer 8 Cert

5.1.9.30 Basic Directory Peer 8 to Basic Directory Peer 9 Cert:

base: Base Intermediate Certificate
serial number: 2

issuer: "cn=Basic Directory Peer 8 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 9 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 5 to Basic Directory Peer 8 Cert

5.1.9.31 Basic Directory Peer 9 CRL:

base: Base CRL
issuer: "cn=Basic Directory Peer 9 CA, o=Test Certificates, c=US"
signed by Basic Directory Peer 8 to Basic Directory Peer 9 Cert
post to certificateRevocationList

5.1.9.32 Basic Directory Peer 9 to Basic Directory Peer 8 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic Directory Peer 9 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Peer 8 CA, o=Test Certificates, c=US"
public key from Basic Directory Peer 5 to Basic Directory Peer 8 Cert
signed by Basic Directory Peer 8 to Basic Directory Peer 9 Cert

5.1.9.33 Basic Directory Path Discovery Test2 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic Directory Peer 9 CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery EE Certificate Test2, o=Test Certificates, c=US"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Peer 8 to Basic Directory Peer 9 Cert

5.1.9.34 Basic Directory Bridge CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
self-signed

5.1.9.35 Basic Directory Bridge CA Cert2:

base: Base Root Certificate
serial number: 2
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
self-signed

5.1.9.36 Basic Directory Bridge CA Cert3:

base: Base Intermediate Certificate

serial number: 3
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
public key from Basic Directory Bridge CA Cert
signed by Basic Directory Bridge CA Cert2

5.1.9.37 Basic Directory Bridge CA Cert4:

base: Base Intermediate Certificate
serial number: 4
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
public key from Basic Directory Bridge CA Cert2
signed by Basic Directory Bridge CA Cert

5.1.9.38 Basic Directory Bridge CA CRL:

base: Base CRL
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
signed by Basic Directory Bridge CA Cert2
post to certificateRevocationList

5.1.9.39 Basic Directory Bridge CA CRL1:

base: Base CRL
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
onlyContainsUserCerts: TRUE
signed by Basic Directory Bridge CA Cert
post to certificateRevocationList at "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"

5.1.9.40 Basic Directory Bridge CA ARL1:

base: Base CRL
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"

onlyContainsAuthorityCerts: TRUE
signed by Basic Directory Bridge CA Cert
post to authorityRevocationList at "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"

5.1.9.41 Basic Directory Trust Anchor to Bridge Directory Cert:

base: Base Intermediate Certificate
serial number: 21
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
"2.16.840.1.101.3.2.1.48.6"
"2.16.840.1.101.3.2.1.48.7"
"2.16.840.1.101.3.2.1.48.10"
"2.16.840.1.101.3.2.1.48.4"
"2.16.840.1.101.3.2.1.48.5"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.9"
map "2.16.840.1.101.3.2.1.48.3" to "2.16.840.1.101.3.2.1.48.8"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
public key from Basic Directory Bridge CA Cert
signed by Basic Directory Trust Anchor Root Cert

5.1.9.42 Basic Directory Trust Anchor to Bridge Directory Cert2:

base: Base Intermediate Certificate
serial number: 22
issuer: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
public key from Basic Directory Bridge CA Cert
signed by Basic Directory Trust Anchor Root Cert

5.1.9.43 Basic Directory Bridge to Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "cn=Basic Directory Trust Anchor, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.9"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.1"

map "2.16.840.1.101.3.2.1.48.9" to "2.16.840.1.101.3.2.1.48.2"
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.3"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
public key from Basic Directory Trust Anchor Root Cert
signed by Basic Directory Bridge CA Cert

5.1.9.44 Basic Directory OU1 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
self-signed

5.1.9.45 Basic Directory OU1 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
signed by Basic Directory OU1 CA Cert
post to certificateRevocationList

5.1.9.46 Basic Directory Bridge to OU1 CA Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.7"
"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.10"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.7" to "2.16.840.1.101.3.2.1.48.37"
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.38"
map "2.16.840.1.101.3.2.1.48.10" to "2.16.840.1.101.3.2.1.48.39"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=Basic Directory OU1, o=Test Certificates, c=US"
minimum: 0
maximum: absent
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
public key from Basic Directory OU1 CA Cert
signed by Basic Directory Bridge CA Cert

5.1.9.47 Basic Directory OU1 CA to Bridge Directory Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"

certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
"2.16.840.1.101.3.2.1.48.38"
"2.16.840.1.101.3.2.1.48.39"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.37" to "2.16.840.1.101.3.2.1.48.7"
map "2.16.840.1.101.3.2.1.48.38" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.39" to "2.16.840.1.101.3.2.1.48.10"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=Basic Directory OU1, o=Test Certificates, c=US"
minimum: 0
maximum: absent
public key from Basic Directory Bridge CA Cert
signed by Basic Directory OU1 CA Cert

5.1.9.48 Basic Directory Path Discovery OU1 EE1:

base: Base End Certificate
serial number: 3
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU1 EE1, ou=Basic Directory OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU1 CA Cert

5.1.9.49 Basic Directory Path Discovery OU1 EE2:

base: Base End Certificate
serial number: 4
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU1 EE2, ou=Basic Directory OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.38"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU1 CA Cert

5.1.9.50 Basic Directory Path Discovery OU1 EE3:

base: Base End Certificate
serial number: 5
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU1 EE3, ou=Basic Directory OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.39"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU1 CA Cert

5.1.9.51 Basic Directory Path Discovery OU1 EE4:

base: Base End Certificate
serial number: 6

issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU1 EE4, ou=Basic Directory OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.40"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU1 CA Cert

5.1.9.52 Basic Directory Path Discovery OU1 EE5:

base: Base End Certificate
serial number: 7
issuer: "cn=CA, ou=Basic Directory OU1, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU1 EE5, ou=Basic Directory OU2, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
"2.16.840.1.101.3.2.1.48.38"
"2.16.840.1.101.3.2.1.48.39"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU1 CA Cert

5.1.9.53 Basic Directory Org2 CA Cert1:

base: Base Root Certificate
serial number: 1
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
self-signed

5.1.9.54 Basic Directory Org2 CA Cert2:

base: Base Root Certificate
serial number: 2
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
self-signed

5.1.9.55 Basic Directory Org2 CA Cert3:

base: Base Root Certificate
serial number: 3
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
self-signed

5.1.9.56 Basic Directory Org2 CA Cert4:

base: Base Root Certificate
serial number: 4
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"

self-signed

5.1.9.57 Basic Directory Org2 CA Cert5:

base: Base Intermediate Certificate
serial number: 5
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL2, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Org2 CA Cert1
signed by Basic Directory Org2 CA Cert2

5.1.9.58 Basic Directory Org2 CA Cert6:

base: Base Intermediate Certificate
serial number: 6
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Org2 CA Cert2
signed by Basic Directory Org2 CA Cert1

5.1.9.59 Basic Directory Org2 CA Cert7:

base: Base Intermediate Certificate
serial number: 7
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Org2 CA Cert2
signed by Basic Directory Org2 CA Cert3

5.1.9.60 Basic Directory Org2 CA Cert8:

base: Base Intermediate Certificate
serial number: 8
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
cRLDistributionPoints: not critical

distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Org2 CA Cert3
signed by Basic Directory Org2 CA Cert2

5.1.9.61 Basic Directory Org2 CA Cert9:

base: Base Intermediate Certificate
serial number: 9
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Org2 CA Cert3
signed by Basic Directory Org2 CA Cert4

5.1.9.62 Basic Directory Org2 CA Cert10:

base: Base Intermediate Certificate
serial number: 10
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Org2 CA Cert4
signed by Basic Directory Org2 CA Cert3

5.1.9.63 Basic Directory Org2 CA CRL:

base: Base CRL
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
revokedCertificates:
serialNumber: 10
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
serialNumber: 13
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
serialNumber: 15
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:

keyCompromise
signed by Basic Directory Org2 CA Cert1
post to certificateRevocationList

5.1.9.64 Basic Directory Org2 CA CRL1:

base: Base CRL
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
onlyContainsUserCerts: TRUE
revokedCertificates:
serialNumber: 13
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic Directory Org2 CA Cert1
post to certificateRevocationList at "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"

5.1.9.65 Basic Directory Org2 CA ARL1:

base: Base CRL
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
onlyContainsAuthorityCerts: TRUE
revokedCertificates:
serialNumber: 10
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
signed by Basic Directory Org2 CA Cert1
post to authorityRevocationList at "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"

5.1.9.66 Basic Directory Org2 CA ARL2:

base: Base CRL
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL2, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
onlyContainsAuthorityCerts: TRUE
signed by Basic Directory Org2 CA Cert2
post to authorityRevocationList at "cn=CRL2, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"

5.1.9.67 Basic Directory Org2 CA CRL3:

base: Base CRL
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
crlExtension:
    issuingDistributionPoint: critical
        distributionPoint:
            fullName:
                directoryName: "cn=CRL3, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
        onlyContainsUserCerts: TRUE
revokedCertificates:
    serialNumber: 15
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic Directory Org2 CA Cert1
post to certificateRevocationList at "cn=CRL3, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"

5.1.9.68 Basic Directory Bridge to Org2 CA Cert:

base: Base Intermediate Certificate
serial number: 7
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
    "2.16.840.1.101.3.2.1.48.8"
policyMappingsExtension: not critical
    map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.27"
nameConstraintsExtension: critical
    permittedSubtrees:
        directoryName: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
        minimum: 0
        maximum: absent
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
public key from Basic Directory Org2 CA Cert2
signed by Basic Directory Bridge CA Cert

5.1.9.69 Basic Directory Org2 CA to Bridge Directory Cert:

base: Base Intermediate Certificate
serial number: 11
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
public key from Basic Directory Bridge CA Cert
signed by Basic Directory Org2 CA Cert2

5.1.9.70 Basic Directory Path Discovery Org2 EE1:

base: Base End Certificate
serial number: 12
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic Directory Path Discovery Org2 EE1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Org2 CA Cert2

5.1.9.71 Basic Directory Path Discovery Org2 EE2:

base: Base End Certificate
serial number: 13
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic Directory Path Discovery Org2 EE2, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Org2 CA Cert2

5.1.9.72 Basic Directory Path Discovery Org2 EE3:

base: Base End Certificate
serial number: 14
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic Directory Path Discovery Org2 EE3, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL3, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Org2 CA Cert3

5.1.9.73 Basic Directory Path Discovery Org2 EE4:

base: Base End Certificate
serial number: 15
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"

subject: "cn=Basic Directory Path Discovery Org2 EE4, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL3, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Org2 CA Cert3

5.1.9.74 Basic Directory Path Discovery Org2 EE5:

base: Base End Certificate
serial number: 16
issuer: "dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic Directory Path Discovery Org2 EE5, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL3, dc=BasicDirectoryOrg2, dc=testcertificates, dc=gov"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory Org2 CA Cert4

5.1.9.75 Basic Directory OU3 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
self-signed

5.1.9.76 Basic Directory OU3 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
signed by Basic Directory OU3 CA Cert
post to certificateRevocationList

5.1.9.77 Basic Directory OU3 CA ARL1:

base: Base CRL
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
onlyContainsAuthorityCerts: TRUE
signed by Basic Directory OU3 CA Cert
post to authorityRevocationList at "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"

5.1.9.78 Basic Directory OU3 CA CRL1:

base: Base CRL
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical
        distributionPoint:
            fullName:
                directoryName: "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
        onlyContainsUserCerts: TRUE
signed by Basic Directory OU3 CA Cert
post to certificateRevocationList at "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"

5.1.9.79 Basic Directory Bridge to OU3 CA Cert:

base: Base Intermediate Certificate
serial number: 8
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
    "2.16.840.1.101.3.2.1.48.10"
    "2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: not critical
    map "2.16.840.1.101.3.2.1.48.10" to "2.16.840.1.101.3.2.1.48.32"
nameConstraintsExtension: critical
    permittedSubtrees:
        directoryName: "ou=Basic Directory OU3, o=Test Certificates, c=US"
        minimum: 0
        maximum: absent
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
public key from Basic Directory OU3 CA Cert
signed by Basic Directory Bridge CA Cert

5.1.9.80 Basic Directory OU3 CA to Bridge Directory Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
subject: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
    "2.16.840.1.101.3.2.1.48.29"
    "2.16.840.1.101.3.2.1.48.30"
    "2.16.840.1.101.3.2.1.48.31"
    "2.16.840.1.101.3.2.1.48.32"
policyMappingsExtension: not critical
    map "2.16.840.1.101.3.2.1.48.29" to "2.16.840.1.101.3.2.1.48.6"
    map "2.16.840.1.101.3.2.1.48.30" to "2.16.840.1.101.3.2.1.48.7"
    map "2.16.840.1.101.3.2.1.48.31" to "2.16.840.1.101.3.2.1.48.8"
    map "2.16.840.1.101.3.2.1.48.32" to "2.16.840.1.101.3.2.1.48.10"
nameConstraintsExtension: critical
    excludedSubtrees:
        directoryName: "ou=Basic Directory OU3, o=Test Certificates, c=US"

minimum: 0
maximum: absent
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
public key from Basic Directory Bridge CA Cert
signed by Basic Directory OU3 CA Cert

5.1.9.81 Basic Directory OU3 CA to OU3 SubCA1 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
subject: "cn=SubCA1, ou=Basic Directory OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
nameConstraintsExtension: not critical
permittedSubtrees:
directoryName: "ou=Basic Directory OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
signed by Basic Directory OU3 CA Cert

5.1.9.82 Basic Directory OU3 SubCA1 CRL:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic Directory OU3, o=Test Certificates, c=US"
signed by Basic Directory OU3 CA to OU3 SubCA1 Cert
post to certificateRevocationList

5.1.9.83 Basic Directory OU3 SubCA1 ARL1:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic Directory OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=SubCA1 CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
onlyContainsAuthorityCerts: TRUE
signed by Basic Directory OU3 CA to OU3 SubCA1 Cert

post to authorityRevocationList at "cn=SubCA1 CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"

5.1.9.84 Basic Directory OU3 SubCA1 CRL1:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic Directory OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
directoryName: "cn=SubCA1 CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
onlyContainsUserCerts: TRUE
signed by Basic Directory OU3 CA to OU3 SubCA1 Cert
post to certificateRevocationList at "cn=SubCA1 CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"

5.1.9.85 Basic Directory OU3 CA to OU3 PeerCA1 Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
subject: "cn=PeerCA1, dc=BasicDirectoryOrg3, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
signed by Basic Directory OU3 CA Cert

5.1.9.86 Basic Directory OU3 PeerCA1 to OU3 CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=PeerCA1, dc=BasicDirectoryOrg3, dc=testcertificates, dc=gov"
subject: "cn=CA, ou=Basic Directory OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
public key from Basic Directory OU3 CA Cert
signed by Basic Directory OU3 CA to OU3 PeerCA1 Cert

5.1.9.87 Basic Directory OU3 PeerCA1 CRL:

base: Base CRL
issuer: "cn=PeerCA1, dc=BasicDirectoryOrg3, dc=testcertificates, dc=gov"
signed by Basic Directory OU3 CA to OU3 PeerCA1 Cert
post to certificateRevocationList

5.1.9.88 Basic Directory Path Discovery OU3 EE1:

base: Base End Certificate
serial number: 1
issuer: "cn=SubCA1, ou=Basic Directory OU3, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU3 EE1, ou=Basic Directory OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
basicConstraintsExtension: critical
cA: FALSE
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=SubCA1 CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU3 CA to OU3 SubCA1 Cert

5.1.9.89 Basic Directory Path Discovery OU3 EE2:

base: Base End Certificate
serial number: 2
issuer: "cn=SubCA1, ou=Basic Directory OU3, o=Test Certificates, c=US"
subject: "cn=Basic Directory Path Discovery OU3 EE2, ou=Basic Directory OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
basicConstraintsExtension: critical
cA: FALSE
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=SubCA1 CRL1, ou=Basic Directory OU3, o=Test Certificates, c=US"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Directory OU3 CA to OU3 SubCA1 Cert

5.1.10 Basic Path Discovery LDAP URI Certificates and CRLs

5.1.10.1 Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 1 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical

AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%201%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.10.2 Basic LDAP URI Peer 1 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 1 CA, o=Test Certificates, c=US"
signed by Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert
post to certificateRevocationList

5.1.10.3 Basic LDAP URI Peer 1 to Basic URI Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 1 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%201%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%201%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Trust Anchor Root Cert
signed by Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert

5.1.10.4 Basic LDAP URI Peer 2 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"

subject: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certifi
cates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.5 Basic LDAP URI Peer 2 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 2 CA Cert
post to certificateRevocationList

5.1.10.6 Basic LDAP URI Peer 1 to Basic LDAP URI Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 1 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%201%20CA,o=Test%20Certifi
cates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certifi
cates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%201%20CA,o=Test%20Certifi
cates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 2 CA Cert
signed by Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert

5.1.10.7 Basic LDAP URI Peer 2 to Basic LDAP URI Peer 1 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 1 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers

accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%201%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert
signed by Basic LDAP URI Peer 2 CA Cert

5.1.10.8 Basic LDAP URI Peer 3 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 3 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 3 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%203%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.9 Basic LDAP URI Peer 3 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 3 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 3 CA Cert
post to certificateRevocationList

5.1.10.10 Basic LDAP URI Peer 3 to Basic LDAP URI Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 3 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%203%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"

subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%203%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 2 CA Cert
signed by Basic LDAP URI Peer 3 CA Cert

5.1.10.11 Basic LDAP URI Peer 4 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 4 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 4 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%204%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.12 Basic LDAP URI Peer 4 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 4 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 4 CA Cert
post to certificateRevocationList

5.1.10.13 Basic LDAP URI Peer 4 to Basic LDAP URI Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 4 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%204%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%204%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 2 CA Cert
signed by Basic LDAP URI Peer 4 CA Cert

5.1.10.14 Basic LDAP URI Peer 2 to Basic LDAP URI Peer 2 SubCA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic LDAP URI Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 2 SubCA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20SubCA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Peer 2 CA Cert

5.1.10.15 Basic LDAP URI Peer 2 SubCA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 2 SubCA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 2 to Basic LDAP URI Peer 2 SubCA Cert
post to certificateRevocationList

5.1.10.16 Basic LDAP URI Path Discovery Test1 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 2 SubCA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery EE Certificate Test1, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:

accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20SubCA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%202%20SubCA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Peer 2 to Basic LDAP URI Peer 2 SubCA Cert

5.1.10.17 Basic LDAP URI Peer 5 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.18 Basic LDAP URI Peer 5 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 5 CA Cert
post to certificateRevocationList

5.1.10.19 Basic URI Trust Anchor to Basic LDAP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 7
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 5 CA Cert
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.10.20 Basic LDAP URI Peer 5 to Basic URI Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Trust Anchor Root Cert
signed by Basic LDAP URI Peer 5 CA Cert

5.1.10.21 Basic LDAP URI Peer 6 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 6 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 6 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%206%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.22 Basic LDAP URI Peer 6 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 6 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 6 CA Cert
post to certificateRevocationList

5.1.10.23 Basic LDAP URI Peer 6 to Basic LDAP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 6 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%206%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%206%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 5 CA Cert
signed by Basic LDAP URI Peer 6 CA Cert

5.1.10.24 Basic LDAP URI Peer 7 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 7 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 7 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%207%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.25 Basic LDAP URI Peer 7 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 7 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 7 CA Cert

post to certificateRevocationList

5.1.10.26 Basic LDAP URI Peer 7 to Basic LDAP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 7 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%207%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%207%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 5 CA Cert
signed by Basic LDAP URI Peer 7 CA Cert

5.1.10.27 Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 8 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%208%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Peer 5 CA Cert

5.1.10.28 Basic LDAP URI Peer 8 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 8 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert
post to certificateRevocationList

5.1.10.29 Basic LDAP URI Peer 8 to Basic LDAP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 8 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%208%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%205%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%208%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 5 CA Cert
signed by Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert

5.1.10.30 Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 8 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 9 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%208%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical

AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%209%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%208%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
signed by Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert

5.1.10.31 Basic LDAP URI Peer 9 CA CRL:

base: Base CRL
issuer: "cn=Basic LDAP URI Peer 9 CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert
post to certificateRevocationList

5.1.10.32 Basic LDAP URI Peer 9 to Basic LDAP URI Peer 8 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic LDAP URI Peer 9 CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Peer 8 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%209%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%208%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%209%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert
signed by Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert

5.1.10.33 Basic LDAP URI Path Discovery Test3 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic LDAP URI Peer 9 CA, o=Test Certificates, c=US"

subject: "cn=Basic LDAP URI Path Discovery EE Certificate Test3, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%209%20CA,o=Test%20Certifi
cates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Peer%209%20CA,o=Test%20Certifi
cates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert

5.1.10.34 Basic LDAP URI Bridge CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=U
S?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certif
icates,c=US?authorityRevocationList;binary"
self-signed

5.1.10.35 Basic LDAP URI Bridge CA Cert2:

base: Base Root Certificate
serial number: 2
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=U
S?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certif
icates,c=US?authorityRevocationList;binary"
self-signed

5.1.10.36 Basic LDAP URI Bridge CA Cert3:

base: Base Intermediate Certificate
serial number: 3
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificat
es,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=U
S?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certif
icates,c=US?authorityRevocationList;binary"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
public key from Basic LDAP URI Bridge CA Cert
signed by Basic LDAP URI Bridge CA Cert2

5.1.10.37 Basic LDAP URI Bridge CA Cert4:

base: Base Intermediate Certificate
serial number: 4
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificat
es,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?authorityRevocationList;binary"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
public key from Basic LDAP URI Bridge CA Cert2
signed by Basic LDAP URI Bridge CA Cert

5.1.10.38 Basic LDAP URI Bridge CA CRL:

base: Base CRL
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
signed by Basic LDAP URI Bridge CA Cert2
post to certificateRevocationList

5.1.10.39 Basic LDAP URI Bridge CA CRL1:

base: Base CRL
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?certificateRevocationList;binary"
onlyContainsUserCerts: TRUE
signed by Basic LDAP URI Bridge CA Cert
post to certificateRevocationList at "cn=CRL1, ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"

5.1.10.40 Basic LDAP URI Bridge CA ARL1:

base: Base CRL
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?authorityRevocationList;binary"
onlyContainsAuthorityCerts: TRUE
signed by Basic LDAP URI Bridge CA Cert
post to authorityRevocationList at "cn=CRL1, ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"

5.1.10.41 Basic URI Trust Anchor to Bridge LDAP URI Cert:

base: Base Intermediate Certificate
serial number: 23
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"

subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certific
ates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificat
es,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c
=US?certificateRevocationList;binary"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
"2.16.840.1.101.3.2.1.48.6"
"2.16.840.1.101.3.2.1.48.7"
"2.16.840.1.101.3.2.1.48.10"
"2.16.840.1.101.3.2.1.48.4"
"2.16.840.1.101.3.2.1.48.5"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.9"
map "2.16.840.1.101.3.2.1.48.3" to "2.16.840.1.101.3.2.1.48.8"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
public key from Basic LDAP URI Bridge CA Cert
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.10.42 Basic URI Trust Anchor to Bridge LDAP URI Cert2:

base: Base Intermediate Certificate
serial number: 24
issuer: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certific
ates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:

accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificat
es,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c
=US?certificateRevocationList;binary"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
public key from Basic LDAP URI Bridge CA Cert
signed by Basic LDAP URI Trust Anchor Root Cert

5.1.10.43 Basic LDAP URI Bridge to Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Trust Anchor, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificat
es,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=Basic%20LDAP%20URI%20Trust%20Anchor,o=Test%20Certificates,c
=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certif
icates,c=US?authorityRevocationList;binary"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.9"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.1"
map "2.16.840.1.101.3.2.1.48.9" to "2.16.840.1.101.3.2.1.48.2"
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.3"

public key from Basic LDAP URI Trust Anchor Root Cert
signed by Basic LDAP URI Bridge CA Cert

5.1.10.44 Basic LDAP URI OU1 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.45 Basic LDAP URI OU1 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
signed by Basic LDAP URI OU1 CA Cert
post to certificateRevocationList

5.1.10.46 Basic LDAP URI Bridge to OU1 CA Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.7"
"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.10"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.7" to "2.16.840.1.101.3.2.1.48.37"
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.38"
map "2.16.840.1.101.3.2.1.48.10" to "2.16.840.1.101.3.2.1.48.39"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?authorityRevocationList;binary"
public key from Basic LDAP URI OU1 CA Cert
signed by Basic LDAP URI Bridge CA Cert

5.1.10.47 Basic LDAP URI OU1 CA to Bridge LDAP URI Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
"2.16.840.1.101.3.2.1.48.38"
"2.16.840.1.101.3.2.1.48.39"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.37" to "2.16.840.1.101.3.2.1.48.7"
map "2.16.840.1.101.3.2.1.48.38" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.39" to "2.16.840.1.101.3.2.1.48.10"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates,c=US?certificateRevocationList;binary"
public key from Basic LDAP URI Bridge CA Cert
signed by Basic LDAP URI OU1 CA Cert

5.1.10.48 Basic LDAP URI Path Discovery OU1 EE1:

base: Base End Certificate
serial number: 3
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery OU1 EE1, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
    "2.16.840.1.101.3.2.1.48.37"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?certificateRevocationList;binary"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU1 CA Cert

5.1.10.49 Basic LDAP URI Path Discovery OU1 EE2:

base: Base End Certificate
serial number: 4
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery OU1 EE2, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
    "2.16.840.1.101.3.2.1.48.38"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?certificateRevocationList;binary"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU1 CA Cert

5.1.10.50 Basic LDAP URI Path Discovery OU1 EE3:

base: Base End Certificate

serial number: 5
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery OU1 EE3, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.39"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU1 CA Cert

5.1.10.51 Basic LDAP URI Path Discovery OU1 EE4:

base: Base End Certificate
serial number: 6
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery OU1 EE4, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.40"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU1 CA Cert

5.1.10.52 Basic LDAP URI Path Discovery OU1 EE5:

base: Base End Certificate
serial number: 7
issuer: "cn=CA, ou=Basic LDAP URI OU1, o=Test Certificates, c=US"

subject: "cn=Basic LDAP URI Path Discovery OU1 EE5, ou=Basic LDAP URI OU2, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
"2.16.840.1.101.3.2.1.48.38"
"2.16.840.1.101.3.2.1.48.39"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU1,o=Test%20Certificates, c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU1 CA Cert

5.1.10.53 Basic LDAP URI Org2 CA Cert1:

base: Base Root Certificate
serial number: 1
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.54 Basic LDAP URI Org2 CA Cert2:

base: Base Root Certificate
serial number: 2
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.55 Basic LDAP URI Org2 CA Cert3:

base: Base Root Certificate
serial number: 3
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.56 Basic LDAP URI Org2 CA Cert4:

base: Base Root Certificate
serial number: 4
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
self-signed

5.1.10.57 Basic LDAP URI Org2 CA Cert5:

base: Base Intermediate Certificate
serial number: 5
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL2,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
public key from Basic LDAP URI Org2 CA Cert1
signed by Basic LDAP URI Org2 CA Cert2

5.1.10.58 Basic LDAP URI Org2 CA Cert6:

base: Base Intermediate Certificate
serial number: 6
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
public key from Basic LDAP URI Org2 CA Cert2
signed by Basic LDAP URI Org2 CA Cert1

5.1.10.59 Basic LDAP URI Org2 CA Cert7:

base: Base Intermediate Certificate
serial number: 7
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:

URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
public key from Basic LDAP URI Org2 CA Cert2
signed by Basic LDAP URI Org2 CA Cert3

5.1.10.60 Basic LDAP URI Org2 CA Cert8:

base: Base Intermediate Certificate
serial number: 8
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
public key from Basic LDAP URI Org2 CA Cert3
signed by Basic LDAP URI Org2 CA Cert2

5.1.10.61 Basic LDAP URI Org2 CA Cert9:

base: Base Intermediate Certificate
serial number: 9
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"

subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
public key from Basic LDAP URI Org2 CA Cert3
signed by Basic LDAP URI Org2 CA Cert4

5.1.10.62 Basic LDAP URI Org2 CA Cert10:

base: Base Intermediate Certificate
serial number: 10
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"

public key from Basic LDAP URI Org2 CA Cert4
signed by Basic LDAP URI Org2 CA Cert3

5.1.10.63 Basic LDAP URI Org2 CA CRL:

base: Base CRL
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
revokedCertificates:
    serialNumber: 10
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                cACompromise
    serialNumber: 13
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
    serialNumber: 15
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic LDAP URI Org2 CA Cert1
post to certificateRevocationList

5.1.10.64 Basic LDAP URI Org2 CA CRL1:

base: Base CRL
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
    issuingDistributionPoint: critical
        distributionPoint:
            fullName:
                URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certific
ateRevocationList;binary"
        onlyContainsUserCerts: TRUE
revokedCertificates:
    serialNumber: 13
    crlEntryExtensions:
        reasonCodeExtension: not critical
            reasons:
                keyCompromise
signed by Basic LDAP URI Org2 CA Cert1
post to certificateRevocationList at "cn=CRL1, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"

5.1.10.65 Basic LDAP URI Org2 CA ARL1:

base: Base CRL
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
    issuingDistributionPoint: critical
        distributionPoint:
            fullName:

URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
onlyContainsAuthorityCerts: TRUE
revokedCertificates:
serialNumber: 10
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
signed by Basic LDAP URI Org2 CA Cert1
post to authorityRevocationList at "cn=CRL1, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"

5.1.10.66 Basic LDAP URI Org2 CA ARL2:

base: Base CRL
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL2,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
onlyContainsAuthorityCerts: TRUE
signed by Basic LDAP URI Org2 CA Cert2
post to authorityRevocationList at "cn=CRL2, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"

5.1.10.67 Basic LDAP URI Org2 CA CRL3:

base: Base CRL
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL3,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certificateRevocationList;binary"
onlyContainsUserCerts: TRUE
revokedCertificates:
serialNumber: 15
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic LDAP URI Org2 CA Cert1
post to certificateRevocationList at "cn=CRL3, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"

5.1.10.68 Basic LDAP URI Bridge to Org2 CA Cert:

base: Base Intermediate Certificate
serial number: 7
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"

certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.8"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.27"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?authorityRevocationList;binary"
public key from Basic LDAP URI Org2 CA Cert2
signed by Basic LDAP URI Bridge CA Cert

5.1.10.69 Basic LDAP URI Org2 CA to Bridge LDAP URI Cert:

base: Base Intermediate Certificate
serial number: 11
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:

fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?authorityRevocationList;binary"
public key from Basic LDAP URI Bridge CA Cert
signed by Basic LDAP URI Org2 CA Cert2

5.1.10.70 Basic LDAP URI Path Discovery Org2 EE1:

base: Base End Certificate
serial number: 12
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic LDAP URI Path Discovery Org2 EE1, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Org2 CA Cert2

5.1.10.71 Basic LDAP URI Path Discovery Org2 EE2:

base: Base End Certificate
serial number: 13
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic LDAP URI Path Discovery Org2 EE2, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL1,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Org2 CA Cert2

5.1.10.72 Basic LDAP URI Path Discovery Org2 EE3:

base: Base End Certificate
serial number: 14
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic LDAP URI Path Discovery Org2 EE3, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL3,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Org2 CA Cert3

5.1.10.73 Basic LDAP URI Path Discovery Org2 EE4:

base: Base End Certificate
serial number: 15
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic LDAP URI Path Discovery Org2 EE4, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL3,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Org2 CA Cert3

5.1.10.74 Basic LDAP URI Path Discovery Org2 EE5:

base: Base End Certificate
serial number: 16
issuer: "dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic LDAP URI Path Discovery Org2 EE5, dc=BasicLDAPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=CRL3,dc=BasicLDAPURIOrg2,dc=testcertificates,dc=gov?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI Org2 CA Cert4

5.1.10.75 Basic LDAP URI OU3 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
self-signed

5.1.10.76 Basic LDAP URI OU3 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
signed by Basic LDAP URI OU3 CA Cert
post to certificateRevocationList

5.1.10.77 Basic LDAP URI OU3 CA ARL1:

base: Base CRL
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?authorityRevocationList;binary"
onlyContainsAuthorityCerts: TRUE
signed by Basic LDAP URI OU3 CA Cert
post to authorityRevocationList at "cn=CRL1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"

5.1.10.78 Basic LDAP URI OU3 CA CRL1:

base: Base CRL
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?certificateRevocationList;binary"
onlyContainsUserCerts: TRUE
signed by Basic LDAP URI OU3 CA Cert
post to certificateRevocationList at "cn=CRL1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"

5.1.10.79 Basic LDAP URI Bridge to OU3 CA Cert:

base: Base Intermediate Certificate
serial number: 8
issuer: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.10"
"2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.10" to "2.16.840.1.101.3.2.1.48.32"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:

accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?authorityRevocationList;binary"
public key from Basic LDAP URI OU3 CA Cert
signed by Basic LDAP URI Bridge CA Cert

5.1.10.80 Basic LDAP URI OU3 CA to Bridge LDAP URI Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subject: "ou=Basic LDAP URI Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.29" to "2.16.840.1.101.3.2.1.48.6"
map "2.16.840.1.101.3.2.1.48.30" to "2.16.840.1.101.3.2.1.48.7"
map "2.16.840.1.101.3.2.1.48.31" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.32" to "2.16.840.1.101.3.2.1.48.10"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/ou=Basic%20LDAP%20URI%20Bridge%20CA,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?authorityRevocationList;binary"
public key from Basic LDAP URI Bridge CA Cert
signed by Basic LDAP URI OU3 CA Cert

5.1.10.81 Basic LDAP URI OU3 CA to OU3 SubCA1 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subject: "cn=SubCA1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
nameConstraintsExtension: not critical
permittedSubtrees:
directoryName: "ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?authorityRevocationList;binary"
signed by Basic LDAP URI OU3 CA Cert

5.1.10.82 Basic LDAP URI OU3 SubCA1 CRL:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
signed by Basic LDAP URI OU3 CA to OU3 SubCA1 Cert
post to certificateRevocationList

5.1.10.83 Basic LDAP URI OU3 SubCA1 ARL1:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1%20CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?authorityRevocationList;binary"
onlyContainsAuthorityCerts: TRUE
signed by Basic LDAP URI OU3 CA to OU3 SubCA1 Cert
post to authorityRevocationList at "cn=SubCA1 CRL1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"

5.1.10.84 Basic LDAP URI OU3 SubCA1 CRL1:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1%20CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?certificateRevocationList;binary"
onlyContainsUserCerts: TRUE
signed by Basic LDAP URI OU3 CA to OU3 SubCA1 Cert
post to certificateRevocationList at "cn=SubCA1 CRL1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"

5.1.10.85 Basic LDAP URI OU3 CA to OU3 PeerCA1 Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subject: "cn=PeerCA1, dc=BasicLDAPURIOrg3, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:

URI:
"ldap://LDAPserver2.subdomain.tld/cn=PeerCA1,dc=BasicLDAPURIOrg3,dc=testcertificates,dc=gov?cA
Certificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificat
es,c=US?authorityRevocationList;binary"
signed by Basic LDAP URI OU3 CA Cert

5.1.10.86 Basic LDAP URI OU3 PeerCA1 to OU3 CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=PeerCA1, dc=BasicLDAPURIOrg3, dc=testcertificates, dc=gov"
subject: "cn=CA, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=PeerCA1,dc=BasicLDAPURIOrg3,dc=testcertificates,dc=gov?cA
Certificate;binary,crossCertificatePair;binary"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=CA,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certificates
,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver2.subdomain.tld/cn=PeerCA1,dc=BasicLDAPURIOrg3,dc=testcertificates,dc=gov?cert
ificateRevocationList;binary"
public key from Basic LDAP URI OU3 CA Cert
signed by Basic LDAP URI OU3 CA to OU3 PeerCA1 Cert

5.1.10.87 Basic LDAP URI OU3 PeerCA1 CRL:

base: Base CRL
issuer: "cn=PeerCA1, dc=BasicLDAPURIOrg3, dc=testcertificates, dc=gov"
signed by Basic LDAP URI OU3 CA to OU3 PeerCA1 Cert
post to certificateRevocationList

5.1.10.88 Basic LDAP URI Path Discovery OU3 EE1:

base: Base End Certificate

serial number: 1
issuer: "cn=SubCA1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery OU3 EE1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
basicConstraintsExtension: critical
cA: FALSE
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certifi
cates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1%20CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test
%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU3 CA to OU3 SubCA1 Cert

5.1.10.89 Basic LDAP URI Path Discovery OU3 EE2:

base: Base End Certificate
serial number: 2
issuer: "cn=SubCA1, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
subject: "cn=Basic LDAP URI Path Discovery OU3 EE2, ou=Basic LDAP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
basicConstraintsExtension: critical
cA: FALSE
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1,ou=Basic%20LDAP%20URI%20OU3,o=Test%20Certifi
cates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=SubCA1%20CRL1,ou=Basic%20LDAP%20URI%20OU3,o=Test
%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic LDAP URI OU3 CA to OU3 SubCA1 Cert

5.1.11 Basic Path Discovery HTTP URI Certificates and CRLs

5.1.11.1 Basic URI Trust Anchor to Basic HTTP URI Peer 1 Cert:

base: Base Intermediate Certificate
serial number: 8
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 1 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.11.2 Basic HTTP URI Peer 1 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 1 CA, o=Test Certificates, c=US"
signed by Basic URI Trust Anchor to Basic HTTP URI Peer 1 Cert

5.1.11.3 Basic HTTP URI Peer 1 to Basic URI Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 1 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer1CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer1CACRL.crl"
public key from Basic HTTP URI Trust Anchor Root Cert
signed by Basic URI Trust Anchor to Basic HTTP URI Peer 1 Cert

5.1.11.4 Basic HTTP URI Peer 2 CA Cert:

base: Base Root Certificate

serial number: 1
issuer: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer2.p7c"
self-signed

5.1.11.5 Basic HTTP URI Peer 2 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 2 CA Cert

5.1.11.6 Basic HTTP URI Peer 1 to Basic HTTP URI Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 1 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer1CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer2.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer1CACRL.crl"
public key from Basic HTTP URI Peer 2 CA Cert
signed by Basic URI Trust Anchor to Basic HTTP URI Peer 1 Cert

5.1.11.7 Basic HTTP URI Peer 2 to Basic HTTP URI Peer 1 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 1 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer2.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer1CA.p7c"

cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer2CACRL.crl"
public key from Basic URI Trust Anchor to Basic HTTP URI Peer 1 Cert
signed by Basic HTTP URI Peer 2 CA Cert

5.1.11.8 Basic HTTP URI Peer 3 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 3 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 3 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer3.p7c"
self-signed

5.1.11.9 Basic HTTP URI Peer 3 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 3 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 3 CA Cert

5.1.11.10 Basic HTTP URI Peer 3 to Basic HTTP URI Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 3 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer3.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer2.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer3CACRL.crl"
public key from Basic HTTP URI Peer 2 CA Cert
signed by Basic HTTP URI Peer 3 CA Cert

5.1.11.11 Basic HTTP URI Peer 4 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 4 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 4 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical

AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer4.p7c"
self-signed

5.1.11.12 Basic HTTP URI Peer 4 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 4 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 4 CA Cert

5.1.11.13 Basic HTTP URI Peer 4 to Basic HTTP URI Peer 2 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 4 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer4.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer2.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer4CACRL.crl"
public key from Basic HTTP URI Peer 2 CA Cert
signed by Basic HTTP URI Peer 4 CA Cert

5.1.11.14 Basic HTTP URI Peer 2 to Basic HTTP URI Peer 2 SubCA Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic HTTP URI Peer 2 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 2 SubCA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer2.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer2SubCA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer2CACRL.crl"

signed by Basic HTTP URI Peer 2 CA Cert

5.1.11.15 Basic HTTP URI Peer 2 SubCA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 2 SubCA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 2 to Basic HTTP URI Peer 2 SubCA Cert

5.1.11.16 Basic HTTP URI Path Discovery Test2 EE:

base: Base End Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 2 SubCA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery EE Certificate Test2, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer2SubCA.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer2SubCACRL.crl"
subjectAltNameExtension:
    rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Peer 2 to Basic HTTP URI Peer 2 SubCA Cert

5.1.11.17 Basic HTTP URI Peer 5 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer5.p7c"
self-signed

5.1.11.18 Basic HTTP URI Peer 5 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 5 CA Cert

5.1.11.19 Basic URI Trust Anchor to Basic HTTP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 9
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:

URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer5.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
public key from Basic HTTP URI Peer 5 CA Cert
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.11.20 Basic HTTP URI Peer 5 to Basic URI Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer5.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer5CACRL.crl"
public key from Basic HTTP URI Trust Anchor Root Cert
signed by Basic HTTP URI Peer 5 CA Cert

5.1.11.21 Basic HTTP URI Peer 6 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 6 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 6 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer6.p7c"
self-signed

5.1.11.22 Basic HTTP URI Peer 6 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 6 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 6 CA Cert

5.1.11.23 Basic HTTP URI Peer 6 to Basic HTTP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 6 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer6.p7c"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer5.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer6CACRL.crl"
public key from Basic HTTP URI Peer 5 CA Cert
signed by Basic HTTP URI Peer 6 CA Cert

5.1.11.24 Basic HTTP URI Peer 7 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 7 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 7 CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer7.p7c"
self-signed

5.1.11.25 Basic HTTP URI Peer 7 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 7 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 7 CA Cert

5.1.11.26 Basic HTTP URI Peer 7 to Basic HTTP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 7 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer7.p7c"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository

accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer5.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer7CACRL.crl"
public key from Basic HTTP URI Peer 5 CA Cert
signed by Basic HTTP URI Peer 7 CA Cert

5.1.11.27 Basic HTTP URI Peer 5 to Basic HTTP URI Peer 8 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 8 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer5.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer8.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer5CACRL.crl"
signed by Basic HTTP URI Peer 5 CA Cert

5.1.11.28 Basic HTTP URI Peer 8 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 8 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 5 to Basic HTTP URI Peer 8 Cert

5.1.11.29 Basic HTTP URI Peer 8 to Basic HTTP URI Peer 5 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 8 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 5 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer8.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer5.p7c"
cRLDistributionPoints: not critical
distributionPoint:

fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer8CACRL.crl"
public key from Basic HTTP URI Peer 5 CA Cert
signed by Basic HTTP URI Peer 5 to Basic HTTP URI Peer 8 Cert

5.1.11.30 Basic HTTP URI Peer 8 to Basic HTTP URI Peer 9 Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 8 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 9 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer8.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer9.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer8CACRL.crl"
signed by Basic HTTP URI Peer 5 to Basic HTTP URI Peer 8 Cert

5.1.11.31 Basic HTTP URI Peer 9 CA CRL:

base: Base CRL
issuer: "cn=Basic HTTP URI Peer 9 CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Peer 8 to Basic HTTP URI Peer 9 Cert

5.1.11.32 Basic HTTP URI Peer 9 to Basic HTTP URI Peer 8 Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=Basic HTTP URI Peer 9 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Peer 8 CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer9.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIPeer8.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer9CACRL.crl"
public key from Basic HTTP URI Peer 5 to Basic HTTP URI Peer 8 Cert
signed by Basic HTTP URI Peer 8 to Basic HTTP URI Peer 9 Cert

5.1.11.33 Basic HTTP URI Path Discovery Test4 EE:

base: Base End Certificate
serial number: 2
issuer: "cn=Basic HTTP URI Peer 9 CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery EE Certificate Test4, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIPeer9.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIPeer9CACRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Peer 8 to Basic HTTP URI Peer 9 Cert

5.1.11.34 Basic HTTP URI Bridge CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
self-signed

5.1.11.35 Basic HTTP URI Bridge CA Cert2:

base: Base Root Certificate
serial number: 2
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
self-signed

5.1.11.36 Basic HTTP URI Bridge CA Cert3:

base: Base Intermediate Certificate

serial number: 3
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIBridge.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
public key from Basic HTTP URI Bridge CA Cert
signed by Basic HTTP URI Bridge CA Cert2

5.1.11.37 Basic HTTP URI Bridge CA Cert4:

base: Base Intermediate Certificate
serial number: 4
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIBridge.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
public key from Basic HTTP URI Bridge CA Cert2
signed by Basic HTTP URI Bridge CA Cert

5.1.11.38 Basic HTTP URI Bridge CA CRL:

base: Base CRL
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
signed by Basic HTTP URI Bridge CA Cert2

5.1.11.39 Basic HTTP URI Bridge CA CRL1:

base: Base CRL
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical
        distributionPoint:
            fullName:
                URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCACRL1.crl"
        onlyContainsUserCerts: TRUE
signed by Basic HTTP URI Bridge CA Cert

5.1.11.40 Basic HTTP URI Bridge CA ARL1:

base: Base CRL
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
crlExtension:
    issuingDistributionPoint: critical
        distributionPoint:
            fullName:
                URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
        onlyContainsAuthorityCerts: TRUE
signed by Basic HTTP URI Bridge CA Cert

5.1.11.41 Basic URI Trust Anchor to Bridge HTTP URI Cert:

base: Base Intermediate Certificate
serial number: 25
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caIssuers
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
    AccessDescription:
        accessMethod: id-ad-caRepository
        accessLocation:
            URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
    distributionPoint:
        fullName:
            URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
certificatePoliciesExtension: not critical
    "2.16.840.1.101.3.2.1.48.1"
    "2.16.840.1.101.3.2.1.48.2"
    "2.16.840.1.101.3.2.1.48.3"
    "2.16.840.1.101.3.2.1.48.6"
    "2.16.840.1.101.3.2.1.48.7"
    "2.16.840.1.101.3.2.1.48.10"
    "2.16.840.1.101.3.2.1.48.4"
    "2.16.840.1.101.3.2.1.48.5"
policyMappingsExtension: not critical
    map "2.16.840.1.101.3.2.1.48.1" to "2.16.840.1.101.3.2.1.48.8"

map "2.16.840.1.101.3.2.1.48.2" to "2.16.840.1.101.3.2.1.48.9"
map "2.16.840.1.101.3.2.1.48.3" to "2.16.840.1.101.3.2.1.48.8"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
public key from Basic HTTP URI Bridge CA Cert
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.11.42 Basic URI Trust Anchor to Bridge HTTP URI Cert2:

base: Base Intermediate Certificate
serial number: 26
issuer: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToTrustAnchor1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURITrustAnchorRootCRL.crl"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.1"
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.3"
policyConstraintsExtension: critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
public key from Basic HTTP URI Bridge CA Cert
signed by Basic HTTP URI Trust Anchor Root Cert

5.1.11.43 Basic HTTP URI Bridge to Trust Anchor Cert:

base: Base Intermediate Certificate
serial number: 5
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Trust Anchor, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIBridge.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByTrustAnchor1.p7c"
cRLDistributionPoints: not critical
distributionPoint:

fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.9"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.1"
map "2.16.840.1.101.3.2.1.48.9" to "2.16.840.1.101.3.2.1.48.2"
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.3"
public key from Basic HTTP URI Trust Anchor Root Cert
signed by Basic HTTP URI Bridge CA Cert

5.1.11.44 Basic HTTP URI OU1 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU1CA.p7c"
self-signed

5.1.11.45 Basic HTTP URI OU1 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
signed by Basic HTTP URI OU1 CA Cert
post to certificateRevocationList

5.1.11.46 Basic HTTP URI Bridge to OU1 CA Cert:

base: Base Intermediate Certificate
serial number: 6
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.7"
"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.10"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.7" to "2.16.840.1.101.3.2.1.48.37"
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.38"
map "2.16.840.1.101.3.2.1.48.10" to "2.16.840.1.101.3.2.1.48.39"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:

URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIBridge.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
public key from Basic HTTP URI OU1 CA Cert
signed by Basic HTTP URI Bridge CA Cert

5.1.11.47 Basic HTTP URI OU1 CA to Bridge HTTP URI Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
"2.16.840.1.101.3.2.1.48.38"
"2.16.840.1.101.3.2.1.48.39"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.37" to "2.16.840.1.101.3.2.1.48.7"
map "2.16.840.1.101.3.2.1.48.38" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.39" to "2.16.840.1.101.3.2.1.48.10"
nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU1CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU1CACRL.crl"
public key from Basic HTTP URI Bridge CA Cert
signed by Basic HTTP URI OU1 CA Cert

5.1.11.48 Basic HTTP URI Path Discovery OU1 EE1:

base: Base End Certificate
serial number: 3
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"

subject: "cn=Basic HTTP URI Path Discovery OU1 EE1, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU1CACRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU1 CA Cert

5.1.11.49 Basic HTTP URI Path Discovery OU1 EE2:

base: Base End Certificate
serial number: 4
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery OU1 EE2, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.38"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU1CACRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU1 CA Cert

5.1.11.50 Basic HTTP URI Path Discovery OU1 EE3:

base: Base End Certificate
serial number: 5
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery OU1 EE3, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.39"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:

fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU1CACRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU1 CA Cert

5.1.11.51 Basic HTTP URI Path Discovery OU1 EE4:

base: Base End Certificate
serial number: 6
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery OU1 EE4, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.40"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU1CACRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU1 CA Cert

5.1.11.52 Basic HTTP URI Path Discovery OU1 EE5:

base: Base End Certificate
serial number: 7
issuer: "cn=CA, ou=Basic HTTP URI OU1, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery OU1 EE5, ou=Basic HTTP URI OU2, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.37"
"2.16.840.1.101.3.2.1.48.38"
"2.16.840.1.101.3.2.1.48.39"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU1CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU1CACRL.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU1 CA Cert

5.1.11.53 Basic HTTP URI Org2 CA Cert1:

base: Base Root Certificate

serial number: 1
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
self-signed

5.1.11.54 Basic HTTP URI Org2 CA Cert2:

base: Base Root Certificate
serial number: 2
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
self-signed

5.1.11.55 Basic HTTP URI Org2 CA Cert3:

base: Base Root Certificate
serial number: 3
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
self-signed

5.1.11.56 Basic HTTP URI Org2 CA Cert4:

base: Base Root Certificate
serial number: 4
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
self-signed

5.1.11.57 Basic HTTP URI Org2 CA Cert5:

base: Base Intermediate Certificate

serial number: 5
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL2.crl"
public key from Basic HTTP URI Org2 CA Cert1
signed by Basic HTTP URI Org2 CA Cert2

5.1.11.58 Basic HTTP URI Org2 CA Cert6:

base: Base Intermediate Certificate
serial number: 6
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
public key from Basic HTTP URI Org2 CA Cert2
signed by Basic HTTP URI Org2 CA Cert1

5.1.11.59 Basic HTTP URI Org2 CA Cert7:

base: Base Intermediate Certificate
serial number: 7
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"

authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
public key from Basic HTTP URI Org2 CA Cert2
signed by Basic HTTP URI Org2 CA Cert3

5.1.11.60 Basic HTTP URI Org2 CA Cert8:

base: Base Intermediate Certificate
serial number: 8
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
public key from Basic HTTP URI Org2 CA Cert3
signed by Basic HTTP URI Org2 CA Cert2

5.1.11.61 Basic HTTP URI Org2 CA Cert9:

base: Base Intermediate Certificate
serial number: 9
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"

subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
public key from Basic HTTP URI Org2 CA Cert3
signed by Basic HTTP URI Org2 CA Cert4

5.1.11.62 Basic HTTP URI Org2 CA Cert10:

base: Base Intermediate Certificate
serial number: 10
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.5.29.32.0"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
public key from Basic HTTP URI Org2 CA Cert4
signed by Basic HTTP URI Org2 CA Cert3

5.1.11.63 Basic HTTP URI Org2 CA CRL:

base: Base CRL
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
revokedCertificates:
serialNumber: 10
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
serialNumber: 13
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
serialNumber: 15
crlEntryExtensions:
reasonCodeExtension: not critical

reasons:
keyCompromise
signed by Basic HTTP URI Org2 CA Cert1

5.1.11.64 Basic HTTP URI Org2 CA CRL1:

base: Base CRL
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL1.crl"
onlyContainsUserCerts: TRUE
revokedCertificates:
serialNumber: 13
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic HTTP URI Org2 CA Cert1

5.1.11.65 Basic HTTP URI Org2 CA ARL1:

base: Base CRL
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
onlyContainsAuthorityCerts: TRUE
revokedCertificates:
serialNumber: 10
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
cACompromise
signed by Basic HTTP URI Org2 CA Cert1

5.1.11.66 Basic HTTP URI Org2 CA ARL2:

base: Base CRL
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL2.crl"
onlyContainsAuthorityCerts: TRUE
signed by Basic HTTP URI Org2 CA Cert2

5.1.11.67 Basic HTTP URI Org2 CA CRL3:

base: Base CRL
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"

crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL3.crl"
onlyContainsUserCerts: TRUE
revokedCertificates:
serialNumber: 15
crlEntryExtensions:
reasonCodeExtension: not critical
reasons:
keyCompromise
signed by Basic HTTP URI Org2 CA Cert1

5.1.11.68 Basic HTTP URI Bridge to Org2 CA Cert:

base: Base Intermediate Certificate
serial number: 7
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.8"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.27"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIBridge.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
public key from Basic HTTP URI Org2 CA Cert2
signed by Basic HTTP URI Bridge CA Cert

5.1.11.69 Basic HTTP URI Org2 CA to Bridge HTTP URI Cert:

base: Base Intermediate Certificate
serial number: 11
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers

accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CAARL1.crl"
public key from Basic HTTP URI Bridge CA Cert
signed by Basic HTTP URI Org2 CA Cert2

5.1.11.70 Basic HTTP URI Path Discovery Org2 EE1:

base: Base End Certificate
serial number: 12
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic HTTP URI Path Discovery Org2 EE1, dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL1.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Org2 CA Cert2

5.1.11.71 Basic HTTP URI Path Discovery Org2 EE2:

base: Base End Certificate
serial number: 13
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic HTTP URI Path Discovery Org2 EE2, dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:

URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL1.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Org2 CA Cert2

5.1.11.72 Basic HTTP URI Path Discovery Org2 EE3:

base: Base End Certificate
serial number: 14
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic HTTP URI Path Discovery Org2 EE3, dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL3.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Org2 CA Cert3

5.1.11.73 Basic HTTP URI Path Discovery Org2 EE4:

base: Base End Certificate
serial number: 15
issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic HTTP URI Path Discovery Org2 EE4, dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL3.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Org2 CA Cert3

5.1.11.74 Basic HTTP URI Path Discovery Org2 EE5:

base: Base End Certificate
serial number: 16

issuer: "dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
subject: "cn=Basic HTTP URI Path Discovery Org2 EE5, dc=BasicHTTPURIOrg2, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.26"
"2.16.840.1.101.3.2.1.48.27"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOrg2CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOrg2CACRL3.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI Org2 CA Cert4

5.1.11.75 Basic HTTP URI OU3 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU3CA.p7c"
self-signed

5.1.11.76 Basic HTTP URI OU3 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
signed by Basic HTTP URI OU3 CA Cert

5.1.11.77 Basic HTTP URI OU3 CA ARL1:

base: Base CRL
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3CAARL1.crl"
onlyContainsAuthorityCerts: TRUE
signed by Basic HTTP URI OU3 CA Cert

5.1.11.78 Basic HTTP URI OU3 CA CRL1:

base: Base CRL
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical

distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3CACRL1.crl"
onlyContainsUserCerts: TRUE
signed by Basic HTTP URI OU3 CA Cert

5.1.11.79 Basic HTTP URI Bridge to OU3 CA Cert:

base: Base Intermediate Certificate
serial number: 8
issuer: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.10"
"2.16.840.1.101.3.2.1.48.2"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.10" to "2.16.840.1.101.3.2.1.48.32"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIBridge.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU3CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIBridgeCAARL1.crl"
public key from Basic HTTP URI OU3 CA Cert
signed by Basic HTTP URI Bridge CA Cert

5.1.11.80 Basic HTTP URI OU3 CA to Bridge HTTP URI Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subject: "ou=Basic HTTP URI Bridge CA, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.29" to "2.16.840.1.101.3.2.1.48.6"
map "2.16.840.1.101.3.2.1.48.30" to "2.16.840.1.101.3.2.1.48.7"
map "2.16.840.1.101.3.2.1.48.31" to "2.16.840.1.101.3.2.1.48.8"
map "2.16.840.1.101.3.2.1.48.32" to "2.16.840.1.101.3.2.1.48.10"

nameConstraintsExtension: critical
excludedSubtrees:
directoryName: "ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU3CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIBridge.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3CAARL1.crl"
public key from Basic HTTP URI Bridge CA Cert
signed by Basic HTTP URI OU3 CA Cert

5.1.11.81 Basic HTTP URI OU3 CA to OU3 SubCA1 Cert:

base: Base Intermediate Certificate
serial number: 3
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subject: "cn=SubCA1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
nameConstraintsExtension: not critical
permittedSubtrees:
directoryName: "ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
minimum: 0
maximum: absent
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
inhibitPolicyMapping: 0
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU3CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU3SubCA1.p7c"
cRLDistributionPoints: not critical
distributionPoint:

fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3CAARL1.crl"
signed by Basic HTTP URI OU3 CA Cert

5.1.11.82 Basic HTTP URI OU3 SubCA1 CRL:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
signed by Basic HTTP URI OU3 CA to OU3 SubCA1 Cert

5.1.11.83 Basic HTTP URI OU3 SubCA1 ARL1:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3SubCA1ARL1.crl"
onlyContainsAuthorityCerts: TRUE
signed by Basic HTTP URI OU3 CA to OU3 SubCA1 Cert

5.1.11.84 Basic HTTP URI OU3 SubCA1 CRL1:

base: Base CRL
issuer: "cn=SubCA1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
crlExtension:
issuingDistributionPoint: critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3SubCA1CRL1.crl"
onlyContainsUserCerts: TRUE
signed by Basic HTTP URI OU3 CA to OU3 SubCA1 Cert

5.1.11.85 Basic HTTP URI OU3 CA to OU3 PeerCA1 Cert:

base: Base Intermediate Certificate
serial number: 4
issuer: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subject: "cn=PeerCA1, dc=BasicHTTPURIOrg3, dc=testcertificates, dc=gov"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU3CA.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU3PeerCA1.p7c"
cRLDistributionPoints: not critical

distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3CAARL1.crl"
signed by Basic HTTP URI OU3 CA Cert

5.1.11.86 Basic HTTP URI OU3 PeerCA1 to OU3 CA Cert:

base: Base Intermediate Certificate
serial number: 1
issuer: "cn=PeerCA1, dc=BasicHTTPURIOrg3, dc=testcertificates, dc=gov"
subject: "cn=CA, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver2.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU3PeerCA1.p7c"
subjectInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caRepository
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedByBasicHTTPURIOU3CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver2.subdomain.tld/CRLdirectory/BasicHTTPURIOU3PeerCA1CRL.crl"
public key from Basic HTTP URI OU3 CA Cert
signed by Basic HTTP URI OU3 CA to OU3 PeerCA1 Cert

5.1.11.87 Basic HTTP URI OU3 PeerCA1 CRL:

base: Base CRL
issuer: "cn=PeerCA1, dc=BasicHTTPURIOrg3, dc=testcertificates, dc=gov"
signed by Basic HTTP URI OU3 CA to OU3 PeerCA1 Cert

5.1.11.88 Basic HTTP URI Path Discovery OU3 EE1:

base: Base End Certificate
serial number: 1
issuer: "cn=SubCA1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery OU3 EE1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.29"
"2.16.840.1.101.3.2.1.48.30"
"2.16.840.1.101.3.2.1.48.31"
"2.16.840.1.101.3.2.1.48.32"
basicConstraintsExtension: critical
cA: FALSE
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers

accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU3SubCA1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3SubCA1CRL1.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU3 CA to OU3 SubCA1 Cert

5.1.11.89 Basic HTTP URI Path Discovery OU3 EE2:

base: Base End Certificate
serial number: 2
issuer: "cn=SubCA1, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
subject: "cn=Basic HTTP URI Path Discovery OU3 EE2, ou=Basic HTTP URI OU3, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.2"
basicConstraintsExtension: critical
cA: FALSE
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicHTTPURIOU3SubCA1.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicHTTPURIOU3SubCA1CRL1.crl"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic HTTP URI OU3 CA to OU3 SubCA1 Cert

5.1.12 Basic Path Discovery Combined Certificates and CRLs

5.1.12.1 Basic Combined OU4 CA Cert:

base: Base Root Certificate
serial number: 1
issuer: "cn=CA, ou=Basic Combined OU4, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic Combined OU4, o=Test Certificates, c=US"
self-signed

5.1.12.2 Basic Combined OU4 CA CRL:

base: Base CRL
issuer: "cn=CA, ou=Basic Combined OU4, o=Test Certificates, c=US"
signed by Basic Combined OU4 CA Cert

5.1.12.3 Basic Directory Bridge to Combined OU4 CA Cert:

base: Base Intermediate Certificate
serial number: 9
issuer: "ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
subject: "cn=CA, ou=Basic Combined OU4, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical

"2.16.840.1.101.3.2.1.48.8"
"2.16.840.1.101.3.2.1.48.9"
policyMappingsExtension: not critical
map "2.16.840.1.101.3.2.1.48.8" to "2.16.840.1.101.3.2.1.48.16"
map "2.16.840.1.101.3.2.1.48.9" to "2.16.840.1.101.3.2.1.48.17"
nameConstraintsExtension: critical
permittedSubtrees:
directoryName: "ou=Basic Combined OU4, o=Test Certificates, c=US"
minimum: 0
maximum: absent
cRLDistributionPoints: not critical
distributionPoint:
fullName:
directoryName: "cn=CRL1, ou=Basic Directory Bridge CA, o=Test Certificates, c=US"
public key from Basic Combined OU4 CA Cert
signed by Basic Directory Bridge CA Cert

5.1.12.4 Basic Combined OU4 to OU4 subCA Cert:

base: Base Intermediate Certificate
serial number: 2
issuer: "cn=CA, ou=Basic Combined OU4, o=Test Certificates, c=US"
subject: "cn=subCA, ou=Basic Combined OU4, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.16"
"2.16.840.1.101.3.2.1.48.17"
policyConstraintsExtension: not critical
requireExplicitPolicy: 0
authorityInfoAccess: not critical
AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI: "http://Webserver1.subdomain.tld/p7cdirectory/IssuedToBasicCombinedOU4CA.p7c"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI: "http://Webserver1.subdomain.tld/CRLdirectory/BasicCombinedOU4CACRL.crl"
signed by Basic Combined OU4 CA Cert

5.1.12.5 Basic Combined OU4 subCA CRL:

base: Base CRL
issuer: "cn=subCA, ou=Basic Combined OU4, o=Test Certificates, c=US"
signed by Basic Combined OU4 to OU4 subCA Cert
post to certificateRevocationList

5.1.12.6 Basic Combined Path Discovery OU4 EE1:

base: Base End Certificate
serial number: 1
issuer: "cn=subCA, ou=Basic Combined OU4, o=Test Certificates, c=US"
subject: "cn=Basic Combined Path Discovery OU4 EE1, ou=Basic Combined OU4, o=Test Certificates, c=US"
certificatePoliciesExtension: not critical
"2.16.840.1.101.3.2.1.48.17"
authorityInfoAccess: not critical

AccessDescription:
accessMethod: id-ad-caIssuers
accessLocation:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=subCA,ou=Basic%20Combined%20OU4,o=Test%20Certificates,c=US?cACertificate;binary,crossCertificatePair;binary"
cRLDistributionPoints: not critical
distributionPoint:
fullName:
URI:
"ldap://LDAPserver1.subdomain.tld/cn=subCA,ou=Basic%20Combined%20OU4,o=Test%20Certificates,c=US?certificateRevocationList;binary"
subjectAltNameExtension:
rfc822Name: "sender@testcertificates.gov"
signed by Basic Combined OU4 to OU4 subCA Cert

5.2 Cross Certificate Pairs

RFC 2587 states that "[t]he forward elements of the **crossCertificatePair** attribute of a CA's directory entry shall be used to store all, except self-issued certificates issued to this CA. Optionally, the reverse elements of the **crossCertificatePair** attribute, of a CA's directory entry may contain a subset of certificates issued by this CA to other CAs." This section specifies the **crossCertificatePairs** that are to be generated for each cross-certificate specified in the previous section.

For each **crossCertificatePair** in which the **forward** [**issuedToThisCA**] element is populated, the **crossCertificatePair** is placed in the directory entry identified by the subject DN of the certificate. For each **crossCertificatePair** in which the **reverse** [**issuedByThisCA**] element is populated, the **crossCertificatePair** is stored in the directory entry identified by the issuer DN of the certificate.

5.2.1 Rudimentary Directory Cross Certificate Pairs

5.2.1.1 Basic Directory Trust Anchor SubCA1 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA1 Cert
reverse: absent

5.2.1.2 Basic Directory Trust Anchor SubCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA1 Cert

5.2.1.3 Basic Directory Trust Anchor SubSubCA1 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubSubCA1 Cert
reverse: absent

5.2.1.4 Basic Directory Trust Anchor SubSubCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubSubCA1 Cert

5.2.1.5 Basic Directory Trust Anchor SubCA2 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA2 Cert
reverse: absent

5.2.1.6 Basic Directory Trust Anchor SubSubCA2 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubSubCA2 Cert
reverse: absent

5.2.1.7 Basic Directory Trust Anchor SubCA3 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA3 Cert
reverse: absent

5.2.1.8 Basic Directory Trust Anchor SubCA3 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA3 Cert

5.2.1.9 Basic Directory Trust Anchor SubCA3 Cert forward crossCertificatePair2:

forward: Basic Directory Trust Anchor SubCA3 Cert2
reverse: absent

5.2.1.10 Basic Directory Trust Anchor SubCA3 Cert reverse crossCertificatePair2:

forward: absent
reverse: Basic Directory Trust Anchor SubCA3 Cert2

5.2.1.11 Basic Directory Trust Anchor SubCA4 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA4 Cert
reverse: absent

5.2.1.12 Basic Directory Trust Anchor SubCA4 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA4 Cert

5.2.1.13 Basic Directory Trust Anchor SubCA5 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA5 Cert
reverse: absent

5.2.1.14 Basic Directory Trust Anchor SubCA5 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA5 Cert

5.2.1.15 Basic Directory Trust Anchor SubCA6 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA6 Cert
reverse: absent

5.2.1.16 Basic Directory Trust Anchor SubCA6 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA6 Cert

5.2.1.17 Basic Directory Trust Anchor SubSubCA6 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubSubCA6 Cert
reverse: absent

5.2.1.18 Basic Directory Trust Anchor SubSubCA6 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubSubCA6 Cert

5.2.1.19 Basic Directory Trust Anchor SubCA7 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA7 Cert
reverse: absent

5.2.1.20 Basic Directory Trust Anchor SubCA7 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA7 Cert

5.2.1.21 Basic Directory Trust Anchor SubSubCA7 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubSubCA7 Cert
reverse: absent

5.2.1.22 Basic Directory Trust Anchor SubSubCA7 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubSubCA7 Cert

5.2.1.23 Basic Directory Trust Anchor SubCA8 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubCA8 Cert
reverse: absent

5.2.1.24 Basic Directory Trust Anchor SubCA8 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubCA8 Cert

5.2.1.25 Basic Directory Trust Anchor SubSubCA8 Cert forward crossCertificatePair:

forward: Basic Directory Trust Anchor SubSubCA8 Cert
reverse: absent

5.2.1.26 Basic Directory Trust Anchor SubSubCA8 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Trust Anchor SubSubCA8 Cert

5.2.2 Rudimentary LDAP URI Cross Certificate Pairs

5.2.2.1 Basic LDAP URI Trust Anchor SubCA1 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA1 Cert
reverse: absent

5.2.2.2 Basic LDAP URI Trust Anchor SubCA1 Cert reverse crossCertificatePair:

forward: absent

reverse: Basic LDAP URI Trust Anchor SubCA1 Cert

5.2.2.3 Basic LDAP URI Trust Anchor SubSubCA1 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubSubCA1 Cert
reverse: absent

5.2.2.4 Basic LDAP URI Trust Anchor SubSubCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubSubCA1 Cert

5.2.2.5 Basic LDAP URI Trust Anchor SubCA2 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA2 Cert
reverse: absent

5.2.2.6 Basic LDAP URI Trust Anchor SubSubCA2 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubSubCA2 Cert
reverse: absent

5.2.2.7 Basic LDAP URI Trust Anchor SubCA3 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA3 Cert
reverse: absent

5.2.2.8 Basic LDAP URI Trust Anchor SubCA3 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubCA3 Cert

5.2.2.9 Basic LDAP URI Trust Anchor SubCA3 Cert forward crossCertificatePair2:

forward: Basic LDAP URI Trust Anchor SubCA3 Cert2
reverse: absent

5.2.2.10 Basic LDAP URI Trust Anchor SubCA3 Cert reverse crossCertificatePair2:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubCA3 Cert2

5.2.2.11 Basic LDAP URI Trust Anchor SubCA4 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA4 Cert
reverse: absent

5.2.2.12 Basic LDAP URI Trust Anchor SubCA4 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubCA4 Cert

5.2.2.13 Basic LDAP URI Trust Anchor SubCA5 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA5 Cert
reverse: absent

5.2.2.14 Basic LDAP URI Trust Anchor SubCA5 Cert reverse crossCertificatePair:

forward: absent

reverse: Basic LDAP URI Trust Anchor SubCA5 Cert

5.2.2.15 Basic LDAP URI Trust Anchor SubCA6 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA6 Cert
reverse: absent

5.2.2.16 Basic LDAP URI Trust Anchor SubCA6 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubCA6 Cert

5.2.2.17 Basic LDAP URI Trust Anchor SubSubCA6 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubSubCA6 Cert
reverse: absent

5.2.2.18 Basic LDAP URI Trust Anchor SubSubCA6 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubSubCA6 Cert

5.2.2.19 Basic LDAP URI Trust Anchor SubCA7 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubCA7 Cert
reverse: absent

5.2.2.20 Basic LDAP URI Trust Anchor SubCA7 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubCA7 Cert

5.2.2.21 Basic LDAP URI Trust Anchor SubSubCA7 Cert forward crossCertificatePair:

forward: Basic LDAP URI Trust Anchor SubSubCA7 Cert
reverse: absent

5.2.2.22 Basic LDAP URI Trust Anchor SubSubCA7 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Trust Anchor SubSubCA7 Cert

5.2.3 Basic Directory Cross Certificate Pairs

5.2.3.1 Basic Directory Trust Anchor and Peer 1 crossCertificatePair 1:

forward: Basic Directory Trust Anchor to Basic Directory Peer 1 Cert
reverse: Basic Directory Peer 1 to Basic Directory Trust Anchor Cert

5.2.3.2 Basic Directory Trust Anchor and Peer 1 crossCertificatePair 2:

forward: Basic Directory Peer 1 to Basic Directory Trust Anchor Cert
reverse: Basic Directory Trust Anchor to Basic Directory Peer 1 Cert

5.2.3.3 Basic Directory Peer 1 and Peer 2 crossCertificatePair 1:

forward: Basic Directory Peer 1 to Basic Directory Peer 2 Cert
reverse: Basic Directory Peer 2 to Basic Directory Peer 1 Cert

5.2.3.4 Basic Directory Peer 1 and Peer 2 crossCertificatePair 2:

forward: Basic Directory Peer 2 to Basic Directory Peer 1 Cert
reverse: Basic Directory Peer 1 to Basic Directory Peer 2 Cert

5.2.3.5 Basic Directory Peer 3 to Peer 2 Cert forward crossCertificatePair:

forward: Basic Directory Peer 3 to Basic Directory Peer 2 Cert
reverse: absent

5.2.3.6 Basic Directory Peer 3 to Peer 2 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Peer 3 to Basic Directory Peer 2 Cert

5.2.3.7 Basic Directory Peer 4 to Peer 2 Cert forward crossCertificatePair:

forward: Basic Directory Peer 4 to Basic Directory Peer 2 Cert
reverse: absent

5.2.3.8 Basic Directory Peer 4 to Peer 2 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Peer 4 to Basic Directory Peer 2 Cert

5.2.3.9 Basic Directory Peer 2 SubCA Cert forward crossCertificatePair:

forward: Basic Directory Peer 2 SubCA Cert
reverse: absent

5.2.3.10 Basic Directory Peer 2 Sub CA Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Peer 2 SubCA Cert

5.2.3.11 Basic Directory Trust Anchor and Peer 5 crossCertificatePair 1:

forward: Basic Directory Trust Anchor to Basic Directory Peer 5 Cert
reverse: Basic Directory Peer 5 to Basic Directory Trust Anchor Cert

5.2.3.12 Basic Directory Trust Anchor and Peer 5 crossCertificatePair 2:

forward: Basic Directory Peer 5 to Basic Directory Trust Anchor Cert
reverse: Basic Directory Trust Anchor to Basic Directory Peer 5 Cert

5.2.3.13 Basic Directory Peer 6 to Peer 5 Cert forward crossCertificatePair:

forward: Basic Directory Peer 6 to Basic Directory Peer 5 Cert
reverse: absent

5.2.3.14 Basic Directory Peer 6 to Peer 5 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Peer 6 to Basic Directory Peer 5 Cert

5.2.3.15 Basic Directory Peer 7 to Peer 5 Cert forward crossCertificatePair:

forward: Basic Directory Peer 7 to Basic Directory Peer 5 Cert
reverse: absent

5.2.3.16 Basic Directory Peer 7 to Peer 5 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Peer 7 to Basic Directory Peer 5 Cert

5.2.3.17 Basic Directory Peer 5 and Peer 8 crossCertificatePair 1:

forward: Basic Directory Peer 5 to Basic Directory Peer 8 Cert
reverse: Basic Directory Peer 8 to Basic Directory Peer 5 Cert

5.2.3.18 Basic Directory Peer 5 and Peer 8 crossCertificatePair 2:

forward: Basic Directory Peer 8 to Basic Directory Peer 5 Cert
reverse: Basic Directory Peer 5 to Basic Directory Peer 8 Cert

5.2.3.19 Basic Directory Peer 8 and Peer 9 crossCertificatePair 1:

forward: Basic Directory Peer 8 to Basic Directory Peer 9 Cert
reverse: Basic Directory Peer 9 to Basic Directory Peer 8 Cert

5.2.3.20 Basic Directory Peer 8 and Peer 9 crossCertificatePair 2:

forward: Basic Directory Peer 9 to Basic Directory Peer 8 Cert
reverse: Basic Directory Peer 8 to Basic Directory Peer 9 Cert

5.2.3.21 Basic Directory Trust Anchor and Bridge crossCertificatePair 1:

forward: Basic Directory Trust Anchor to Bridge Directory Cert
reverse: Basic Directory Bridge to Trust Anchor Cert

5.2.3.22 Basic Directory Trust Anchor and Bridge crossCertificatePair 2:

forward: Basic Directory Bridge to Trust Anchor Cert
reverse: Basic Directory Trust Anchor to Bridge Directory Cert

5.2.3.23 Basic Directory Trust Anchor and Bridge crossCertificatePair 3:

forward: Basic Directory Trust Anchor to Bridge Directory Cert2
reverse: Basic Directory Bridge to Trust Anchor Cert

5.2.3.24 Basic Directory Trust Anchor and Bridge crossCertificatePair 4:

forward: Basic Directory Bridge to Trust Anchor Cert
reverse: Basic Directory Trust Anchor to Bridge Directory Cert2

5.2.3.25 Basic Directory Bridge and OU1 CA crossCertificatePair 1:

forward: Basic Directory Bridge to OU1 CA Cert
reverse: Basic Directory OU1 CA to Bridge Directory Cert

5.2.3.26 Basic Directory Bridge and OU1 CA crossCertificatePair 2:

forward: Basic Directory OU1 CA to Bridge Directory Cert
reverse: Basic Directory Bridge to OU1 CA Cert

5.2.3.27 Basic Directory Bridge and Org2 CA crossCertificatePair 1:

forward: Basic Directory Bridge to Org2 CA Cert
reverse: Basic Directory Org2 CA to Bridge Directory Cert

5.2.3.28 Basic Directory Bridge and Org2 CA crossCertificatePair 2:

forward: Basic Directory Org2 CA to Bridge Directory Cert
reverse: Basic Directory Bridge to Org2 CA Cert

5.2.3.29 Basic Directory Bridge and OU3 CA crossCertificatePair 1:

forward: Basic Directory Bridge to OU3 CA Cert
reverse: Basic Directory OU3 CA to Bridge Directory Cert

5.2.3.30 Basic Directory Bridge and OU3 CA crossCertificatePair 2:

forward: Basic Directory OU3 CA to Bridge Directory Cert
reverse: Basic Directory Bridge to OU3 CA Cert

5.2.3.31 Basic Directory OU3 CA to OU3 SubCA1 forward crossCertificatePair:

forward: Basic Directory OU3 CA to OU3 SubCA1 Cert
reverse: absent

5.2.3.32 Basic Directory OU3 CA to OU3 SubCA1 reverse crossCertificatePair:

forward: absent
reverse: Basic Directory OU3 CA to OU3 SubCA1 Cert

5.2.3.33 Basic Directory OU3 CA and OU3 PeerCA1 crossCertificatePair1:

forward: Basic Directory OU3 CA to OU3 PeerCA1 Cert
reverse: Basic Directory OU3 PeerCA1 to OU3 CA Cert

5.2.3.34 Basic Directory OU3 CA and OU3 PeerCA1 crossCertificatePair2:

forward: Basic Directory OU3 PeerCA1 to OU3 CA Cert
reverse: Basic Directory OU3 CA to OU3 PeerCA1 Cert

5.2.3.35 Basic Directory Bridge to Combined OU4 CA reverse crossCertificatePair:

forward: absent
reverse: Basic Directory Bridge to Combined OU4 CA Cert

5.2.4 Basic LDAP URI Cross Certificate Pairs

5.2.4.1 Basic URI Trust Anchor and Basic LDAP URI Peer 1 crossCertificatePair 1:

forward: Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert
reverse: Basic LDAP URI Peer 1 to Basic URI Trust Anchor Cert

5.2.4.2 Basic URI Trust Anchor and Basic LDAP URI Peer 1 crossCertificatePair 2:

forward: Basic LDAP URI Peer 1 to Basic URI Trust Anchor Cert
reverse: Basic URI Trust Anchor to Basic LDAP URI Peer 1 Cert

5.2.4.3 Basic LDAP URI Peer 1 and Basic LDAP URI Peer 2 crossCertificatePair 1:

forward: Basic LDAP URI Peer 1 to Basic LDAP URI Peer 2 Cert
reverse: Basic LDAP URI Peer 2 to Basic LDAP URI Peer 1 Cert

5.2.4.4 Basic LDAP URI Peer 1 and Basic LDAP URI Peer 2 crossCertificatePair 2:

forward: Basic LDAP URI Peer 2 to Basic LDAP URI Peer 1 Cert

reverse: Basic LDAP URI Peer 1 to Basic LDAP URI Peer 2 Cert

5.2.4.5 Basic LDAP URI Peer 3 to Peer 2 Cert forward crossCertificatePair:

forward: Basic LDAP URI Peer 3 to Basic LDAP URI Peer 2 Cert
reverse: absent

5.2.4.6 Basic LDAP URI Peer 3 to Peer 2 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Peer 3 to Basic LDAP URI Peer 2 Cert

5.2.4.7 Basic LDAP URI Peer 4 to Peer 2 Cert forward crossCertificatePair:

forward: Basic LDAP URI Peer 4 to Basic LDAP URI Peer 2 Cert
reverse: absent

5.2.4.8 Basic LDAP URI Peer 4 to Peer 2 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Peer 4 to Basic LDAP URI Peer 2 Cert

5.2.4.9 Basic LDAP URI Peer 2 to Peer 2 SubCA Cert forward crossCertificatePair:

forward: Basic LDAP URI Peer 2 to Basic LDAP URI Peer 2 SubCA Cert
reverse: absent

5.2.4.10 Basic LDAP URI Peer 2 to Peer 2 SubCA Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Peer 2 to Basic LDAP URI Peer 2 SubCA Cert

5.2.4.11 Basic URI Trust Anchor and Basic LDAP URI Peer 5 crossCertificatePair 1:

forward: Basic URI Trust Anchor to Basic LDAP URI Peer 5 Cert
reverse: Basic LDAP URI Peer 5 to Basic URI Trust Anchor Cert

5.2.4.12 Basic URI Trust Anchor and Basic LDAP URI Peer 5 crossCertificatePair 2:

forward: Basic LDAP URI Peer 5 to Basic URI Trust Anchor Cert
reverse: Basic URI Trust Anchor to Basic LDAP URI Peer 5 Cert

5.2.4.13 Basic LDAP URI Peer 6 to Peer 5 Cert forward crossCertificatePair:

forward: Basic LDAP URI Peer 6 to Basic LDAP URI Peer 5 Cert
reverse: absent

5.2.4.14 Basic LDAP URI Peer 6 to Peer 5 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI Peer 6 to Basic LDAP URI Peer 5 Cert

5.2.4.15 Basic LDAP URI Peer 7 to Peer 5 Cert forward crossCertificatePair:

forward: Basic LDAP URI Peer 7 to Basic LDAP URI Peer 5 Cert
reverse: absent

5.2.4.16 Basic LDAP URI Peer 7 to Peer 5 Cert reverse crossCertificatePair:

forward: absent

reverse: Basic LDAP URI Peer 7 to Basic LDAP URI Peer 5 Cert

5.2.4.17 Basic LDAP URI Peer 5 and Basic LDAP URI Peer 8 crossCertificatePair 1:

forward: Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert
reverse: Basic LDAP URI Peer 8 to Basic LDAP URI Peer 5 Cert

5.2.4.18 Basic LDAP URI Peer 5 and Basic LDAP URI Peer 8 crossCertificatePair 2:

forward: Basic LDAP URI Peer 8 to Basic LDAP URI Peer 5 Cert
reverse: Basic LDAP URI Peer 5 to Basic LDAP URI Peer 8 Cert

5.2.4.19 Basic LDAP URI Peer 8 and Basic LDAP URI Peer 9 crossCertificatePair 1:

forward: Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert
reverse: Basic LDAP URI Peer 9 to Basic LDAP URI Peer 8 Cert

5.2.4.20 Basic LDAP URI Peer 8 and Basic LDAP URI Peer 9 crossCertificatePair 2:

forward: Basic LDAP URI Peer 9 to Basic LDAP URI Peer 8 Cert
reverse: Basic LDAP URI Peer 8 to Basic LDAP URI Peer 9 Cert

5.2.4.21 Basic URI Trust Anchor and LDAP Bridge crossCertificatePair 1:

forward: Basic URI Trust Anchor to Bridge LDAP URI Cert
reverse: Basic LDAP URI Bridge to Trust Anchor Cert

5.2.4.22 Basic URI Trust Anchor and LDAP Bridge crossCertificatePair 2:

forward: Basic LDAP URI Bridge to Trust Anchor Cert
reverse: Basic URI Trust Anchor to Bridge LDAP URI Cert

5.2.4.23 Basic URI Trust Anchor and LDAP Bridge crossCertificatePair 3:

forward: Basic URI Trust Anchor to Bridge LDAP URI Cert2
reverse: Basic LDAP URI Bridge to Trust Anchor Cert

5.2.4.24 Basic URI Trust Anchor and LDAP Bridge crossCertificatePair 4:

forward: Basic LDAP URI Bridge to Trust Anchor Cert
reverse: Basic URI Trust Anchor to Bridge LDAP URI Cert2

5.2.4.25 Basic LDAP URI Bridge and OU1 CA crossCertificatePair 1:

forward: Basic LDAP URI Bridge to OU1 CA Cert
reverse: Basic LDAP URI OU1 CA to Bridge LDAP URI Cert

5.2.4.26 Basic LDAP URI Bridge and OU1 CA crossCertificatePair 2:

forward: Basic LDAP URI OU1 CA to Bridge LDAP URI Cert
reverse: Basic LDAP URI Bridge to OU1 CA Cert

5.2.4.27 Basic LDAP URI Bridge and Org2 CA crossCertificatePair 1:

forward: Basic LDAP URI Bridge to Org2 CA Cert
reverse: Basic LDAP URI Org2 CA to Bridge LDAP URI Cert

5.2.4.28 Basic LDAP URI Bridge and Org2 CA crossCertificatePair 2:

forward: Basic LDAP URI Org2 CA to Bridge LDAP URI Cert

reverse: Basic LDAP URI Bridge to Org2 CA Cert

5.2.4.29 Basic LDAP URI Bridge and OU3 CA crossCertificatePair 1:

forward: Basic LDAP URI Bridge to OU3 CA Cert
reverse: Basic LDAP URI OU3 CA to Bridge LDAP URI Cert

5.2.4.30 Basic LDAP URI Bridge and OU3 CA crossCertificatePair 2:

forward: Basic LDAP URI OU3 CA to Bridge LDAP URI Cert
reverse: Basic LDAP URI Bridge to OU3 CA Cert

5.2.4.31 Basic LDAP URI OU3 to OU3 SubCA1 Cert forward crossCertificatePair:

forward: Basic LDAP URI OU3 CA to OU3 SubCA1 Cert
reverse: absent

5.2.4.32 Basic LDAP URI OU3 to OU3 SubCA1 Cert reverse crossCertificatePair:

forward: absent
reverse: Basic LDAP URI OU3 CA to OU3 SubCA1 Cert

5.2.4.33 Basic LDAP URI OU3 and OU3 PeerCA1 crossCertificatePair 1:

forward: Basic LDAP URI OU3 CA to OU3 PeerCA1 Cert
reverse: Basic LDAP URI OU3 PeerCA1 to OU3 CA Cert

5.2.4.34 Basic LDAP URI OU3 and OU3 PeerCA1 crossCertificatePair 2:

forward: Basic LDAP URI OU3 PeerCA1 to OU3 CA Cert
reverse: Basic LDAP URI OU3 CA to OU3 PeerCA1 Cert

5.2.5 Basic Combined Cross Certificate Pairs

5.2.5.1 Basic Combined OU4 to OU4 subCA forward crossCertificatePair:

forward: Basic Combined OU4 to OU4 subCA Cert
reverse: absent

5.3 S/MIME Messages

5.3.1 Base Signed Message

Syntax Field or Type Name	Value	Comments
RFC822message		
MIME-message-headers		
version	1.0	Indicates message body formatted according to MIME v1.0
fields		RFC 822 header fields
dates		
orig-date		
date-time		Current time
day-of-week	{Automatically generated}	i.e., “Thu”
date	{Automatically generated}	d mmm yyyy (ex: “6 Sep 2001”)
time	{Automatically generated}	hh:mm:ss zzz (ex: “15:42:00 -0500”)
source		
trace	{Absent}	

originator		
authentic		
from		
mailbox		
addr-spec	sender@testcertificates.gov	
destinations		One or more
destination		
toAddresses		One for each recipient
address		
mailbox		
addr-spec	{Always specified}	
optionalFields		
subject	{Always specified}	Indicates test case
entity-headers		MIME entity header fields
content	application/pkcs7-mime	
encoding	base64	
description	attachment	
body		Base64 encoding of ContentInfo
ContentInfo		
contentType	1.2.840.113549.1.7.2	id-signedData
content		
signedData		
version	1	Integer value of "1" indicates CMSVersion 1
digestAlgorithms		
AlgorithmIdentifier		
algorithm	1.3.14.3.2.26	SHA-1
parameters	{Absent}	
encapContentInfo		
eContentType	1.2.840.113549.1.7.1	id-data
eContent	Content-Type: text/plain; charset=iso-8859-1 Content-Transfer-Encoding: 7bit This is a sample signed message.	Located in first MIME body part
certificates		Signer's certificate
crls		
signerInfos		
SignerInfo		
version	1	Integer value of "1" indicates CMSVersion 1
sid		
issuerAndSerialNumber		
issuer	{Automatically generated}	issuer DN of signer's cert
serialNumber	{Automatically generated}	serial number of signer's cert
digestAlgorithm		
AlgorithmIdentifier		
algorithm	1.3.14.3.2.26	SHA-1
parameters	{Absent}	
signedAttrs	{Absent}	
signatureAlgorithm		
AlgorithmIdentifier		
algorithm	1.2.840.113549.1.1.1	RSA Encryption
parameters	NULL	
signature		
OCTET STRING	{Automatically generated}	Calculated signature value
unsignedAttrs	{Absent}	

5.3.2 Test Signed Messages

5.3.2.1 Signed Rudimentary Directory Path Discovery Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test1"
signer: Rudimentary Directory Path Discovery Test1 EE

5.3.2.2 Signed Rudimentary Directory Path Discovery Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test2"
signer: Rudimentary Directory Path Discovery Test2 EE

5.3.2.3 Signed Rudimentary Directory Path Discovery Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test3"
signer: Rudimentary Directory Path Discovery Test3 EE

5.3.2.4 Signed Rudimentary Directory Path Discovery Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test4"
signer: Rudimentary Directory Path Discovery Test4 EE

5.3.2.5 Signed Rudimentary Directory Path Discovery Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test5"
signer: Rudimentary Directory Path Discovery Test5 EE

5.3.2.6 Signed Rudimentary Directory Path Discovery Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test6"
signer: Rudimentary Directory Path Discovery Test6 EE

5.3.2.7 Signed Rudimentary Directory Path Discovery Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test7"
signer: Rudimentary Directory Path Discovery Test7 EE

5.3.2.8 Signed Rudimentary Directory Path Discovery Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test8"
signer: Rudimentary Directory Path Discovery Test8 EE

5.3.2.9 Signed Rudimentary Directory Path Discovery Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test9"
signer: Rudimentary Directory Path Discovery Test9 EE

5.3.2.10 Signed Rudimentary Directory Path Discovery Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test10"
signer: Rudimentary Directory Path Discovery Test10 EE

5.3.2.11 Signed Rudimentary Directory Path Discovery Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test11"
signer: Rudimentary Directory Path Discovery Test11 EE

5.3.2.12 Signed Rudimentary Directory Path Discovery Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test12"
signer: Rudimentary Directory Path Discovery Test12 EE

5.3.2.13 Signed Rudimentary Directory Path Discovery Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary Directory Path Discovery Test13"
signer: Rudimentary Directory Path Discovery Test13 EE

5.3.2.14 Signed Rudimentary LDAP Path Discovery Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test1"
signer: Rudimentary LDAP URI Path Discovery Test1 EE

5.3.2.15 Signed Rudimentary HTTP Path Discovery Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test2"
signer: Rudimentary HTTP URI Path Discovery Test2 EE

5.3.2.16 Signed Rudimentary LDAP Path Discovery Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test3"
signer: Rudimentary LDAP URI Path Discovery Test3 EE

5.3.2.17 Signed Rudimentary HTTP Path Discovery Test4:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test4"
signer: Rudimentary HTTP URI Path Discovery Test4 EE

5.3.2.18 Signed Rudimentary LDAP Path Discovery Test5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test5"
signer: Rudimentary LDAP URI Path Discovery Test5 EE

5.3.2.19 Signed Rudimentary LDAP Path Discovery Test6:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test6"
signer: Rudimentary LDAP URI Path Discovery Test6 EE

5.3.2.20 Signed Rudimentary HTTP Path Discovery Test7:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test7"
signer: Rudimentary HTTP URI Path Discovery Test7 EE

5.3.2.21 Signed Rudimentary HTTP Path Discovery Test8:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test8"
signer: Rudimentary HTTP URI Path Discovery Test8 EE

5.3.2.22 Signed Rudimentary LDAP Path Discovery Test9:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test9"
signer: Rudimentary LDAP URI Path Discovery Test9 EE

5.3.2.23 Signed Rudimentary LDAP Path Discovery Test10:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test10"
signer: Rudimentary LDAP URI Path Discovery Test10 EE

5.3.2.24 Signed Rudimentary LDAP Path Discovery Test11:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test11"
signer: Rudimentary LDAP URI Path Discovery Test11 EE

5.3.2.25 Signed Rudimentary LDAP Path Discovery Test12:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test12"

signer: Rudimentary LDAP URI Path Discovery Test12 EE

5.3.2.26 Signed Rudimentary HTTP Path Discovery Test13:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test13"
signer: Rudimentary HTTP URI Path Discovery Test13 EE

5.3.2.27 Signed Rudimentary HTTP Path Discovery Test14:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test14"
signer: Rudimentary HTTP URI Path Discovery Test14 EE

5.3.2.28 Signed Rudimentary HTTP Path Discovery Test15:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test15"
signer: Rudimentary HTTP URI Path Discovery Test15 EE

5.3.2.29 Signed Rudimentary HTTP Path Discovery Test16:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary HTTP Path Discovery Test16"
signer: Rudimentary HTTP URI Path Discovery Test16 EE

5.3.2.30 Signed Rudimentary LDAP Path Discovery Test17:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test17"
signer: Rudimentary LDAP URI Path Discovery Test17 EE

5.3.2.31 Signed Rudimentary LDAP Path Discovery Test18:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test18"
signer: Rudimentary LDAP URI Path Discovery Test18 EE

5.3.2.32 Signed Rudimentary LDAP Path Discovery Test19:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Rudimentary LDAP Path Discovery Test19"
signer: Rudimentary LDAP URI Path Discovery Test19 EE

5.3.2.33 Signed Basic Directory Mesh Path Discovery Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Mesh Path Discovery Test1"
signer: Basic Directory Path Discovery Test1 EE

5.3.2.34 Signed Basic Directory Mesh Path Discovery Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Mesh Path Discovery Test2"
signer: Basic Directory Path Discovery Test2 EE

5.3.2.35 Signed Basic Directory Path Discovery OU1 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU1 EE1"
signer: Basic Directory Path Discovery OU1 EE1

5.3.2.36 Signed Basic Directory Path Discovery OU1 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU1 EE2"
signer: Basic Directory Path Discovery OU1 EE2

5.3.2.37 Signed Basic Directory Path Discovery OU1 EE3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU1 EE3"
signer: Basic Directory Path Discovery OU1 EE3

5.3.2.38 Signed Basic Directory Path Discovery OU1 EE4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU1 EE4"
signer: Basic Directory Path Discovery OU1 EE4

5.3.2.39 Signed Basic Directory Path Discovery OU1 EE5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU1 EE5"
signer: Basic Directory Path Discovery OU1 EE5

5.3.2.40 Signed Basic Directory Path Discovery Org2 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery Org2 EE1"
signer: Basic Directory Path Discovery Org2 EE1

5.3.2.41 Signed Basic Directory Path Discovery Org2 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery Org2 EE2"
signer: Basic Directory Path Discovery Org2 EE2

5.3.2.42 Signed Basic Directory Path Discovery Org2 EE3:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery Org2 EE3"
signer: Basic Directory Path Discovery Org2 EE3

5.3.2.43 Signed Basic Directory Path Discovery Org2 EE4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery Org2 EE4"
signer: Basic Directory Path Discovery Org2 EE4

5.3.2.44 Signed Basic Directory Path Discovery Org2 EE5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery Org2 EE5"
signer: Basic Directory Path Discovery Org2 EE5

5.3.2.45 Signed Basic Directory Path Discovery OU3 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU3 EE1"
signer: Basic Directory Path Discovery OU3 EE1

5.3.2.46 Signed Basic Directory Path Discovery OU3 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Directory Path Discovery OU3 EE2"
signer: Basic Directory Path Discovery OU3 EE2

5.3.2.47 Signed Basic LDAP Mesh Path Discovery Test1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP Mesh Path Discovery Test1"
signer: Basic LDAP URI Path Discovery Test1 EE

5.3.2.48 Signed Basic HTTP Mesh Path Discovery Test2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP Mesh Path Discovery Test2"
signer: Basic HTTP URI Path Discovery Test2 EE

5.3.2.49 Signed Basic LDAP Mesh Path Discovery Test3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP Mesh Path Discovery Test3"
signer: Basic LDAP URI Path Discovery Test3 EE

5.3.2.50 Signed Basic HTTP Mesh Path Discovery Test4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP Mesh Path Discovery Test4"

signer: Basic HTTP URI Path Discovery Test4 EE

5.3.2.51 Signed Basic LDAP URI Path Discovery OU1 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU1 EE1"
signer: Basic LDAP URI Path Discovery OU1 EE1

5.3.2.52 Signed Basic LDAP URI Path Discovery OU1 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU1 EE2"
signer: Basic LDAP URI Path Discovery OU1 EE2

5.3.2.53 Signed Basic LDAP URI Path Discovery OU1 EE3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU1 EE3"
signer: Basic LDAP URI Path Discovery OU1 EE3

5.3.2.54 Signed Basic LDAP URI Path Discovery OU1 EE4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU1 EE4"
signer: Basic LDAP URI Path Discovery OU1 EE4

5.3.2.55 Signed Basic LDAP URI Path Discovery OU1 EE5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU1 EE5"
signer: Basic LDAP URI Path Discovery OU1 EE5

5.3.2.56 Signed Basic LDAP URI Path Discovery Org2 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery Org2 EE1"
signer: Basic LDAP URI Path Discovery Org2 EE1

5.3.2.57 Signed Basic LDAP URI Path Discovery Org2 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery Org2 EE2"
signer: Basic LDAP URI Path Discovery Org2 EE2

5.3.2.58 Signed Basic LDAP URI Path Discovery Org2 EE3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery Org2 EE3"
signer: Basic LDAP URI Path Discovery Org2 EE3

5.3.2.59 Signed Basic LDAP URI Path Discovery Org2 EE4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery Org2 EE4"
signer: Basic LDAP URI Path Discovery Org2 EE4

5.3.2.60 Signed Basic LDAP URI Path Discovery Org2 EE5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery Org2 EE5"
signer: Basic LDAP URI Path Discovery Org2 EE5

5.3.2.61 Signed Basic LDAP URI Path Discovery OU3 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU3 EE1"
signer: Basic LDAP URI Path Discovery OU3 EE1

5.3.2.62 Signed Basic LDAP URI Path Discovery OU3 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic LDAP URI Path Discovery OU3 EE2"
signer: Basic LDAP URI Path Discovery OU3 EE2

5.3.2.63 Signed Basic HTTP URI Path Discovery OU1 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU1 EE1"
signer: Basic HTTP URI Path Discovery OU1 EE1

5.3.2.64 Signed Basic HTTP URI Path Discovery OU1 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU1 EE2"
signer: Basic HTTP URI Path Discovery OU1 EE2

5.3.2.65 Signed Basic HTTP URI Path Discovery OU1 EE3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU1 EE3"
signer: Basic HTTP URI Path Discovery OU1 EE3

5.3.2.66 Signed Basic HTTP URI Path Discovery OU1 EE4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU1 EE4"
signer: Basic HTTP URI Path Discovery OU1 EE4

5.3.2.67 Signed Basic HTTP URI Path Discovery OU1 EE5:

Base: Base Signed Message

to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU1 EE5"
signer: Basic HTTP URI Path Discovery OU1 EE5

5.3.2.68 Signed Basic HTTP URI Path Discovery Org2 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery Org2 EE1"
signer: Basic HTTP URI Path Discovery Org2 EE1

5.3.2.69 Signed Basic HTTP URI Path Discovery Org2 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery Org2 EE2"
signer: Basic HTTP URI Path Discovery Org2 EE2

5.3.2.70 Signed Basic HTTP URI Path Discovery Org2 EE3:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery Org2 EE3"
signer: Basic HTTP URI Path Discovery Org2 EE3

5.3.2.71 Signed Basic HTTP URI Path Discovery Org2 EE4:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery Org2 EE4"
signer: Basic HTTP URI Path Discovery Org2 EE4

5.3.2.72 Signed Basic HTTP URI Path Discovery Org2 EE5:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery Org2 EE5"
signer: Basic HTTP URI Path Discovery Org2 EE5

5.3.2.73 Signed Basic HTTP URI Path Discovery OU3 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU3 EE1"
signer: Basic HTTP URI Path Discovery OU3 EE1

5.3.2.74 Signed Basic HTTP URI Path Discovery OU3 EE2:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic HTTP URI Path Discovery OU3 EE2"
signer: Basic HTTP URI Path Discovery OU3 EE2

5.3.2.75 Signed Basic Combined Path Discovery OU4 EE1:

Base: Base Signed Message
to: "recipient@testcertificates.gov"
subject: "Basic Combined Path Discovery OU4 EE1"

signer: Basic Combined Path Discovery OU4 EE1