INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.509

Corrigendum 4

(01/2007)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Directory

Recommendation X.509 (2000) |
ISO/IEC 9594-8:2001

Technical Corrigendum 4

CAUTION !

PREPUBLISHED RECOMMENDATION

This prepublication is an unedited version of a recently approved Recommendation. It will be replaced by the published version after editing. Therefore, there will be differences between this prepublication and the published version.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU [had/had not] received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Recommendation X.509 (2000) | ISO/IEC 9594-8:2001
Technical Corrigendum 4

(covering resolution to defect reports 310, 311 and 314)

This corrects the defects reported in defect report 310

Replace Note 4 in section 7.3 with the following text:

When an implementation processing a CRL encounters the serial number of the certificate of interest in a CRL entry, but does not recognize a critical extension in the **crlEntryExtensions** field from that CRL entry, that CRL cannot be used to determine the status of the certificate. When an implementation does not recognize a critical extension in the **crlExtensions** field, that CRL cannot be used to determine the status of the certificate, regardless of whether the serial number of the certificate of interest appears in that CRL or not.

> NOTE 4 – In these cases local policy may dictate actions in addition to and/or stronger than those stated in this Specification, such as seeking revocation status information from other sources.

Certificates for which revocation status cannot be determined should not be considered valid certificates.

This corrects the defects reported in defect report 311

Replace Note 5 in section 7.3 with the following text:

If an extension affects the treatment of the list (e.g. multiple CRLs need to be scanned to examine the entire list of revoked certificates, or an entry may represent a range of certificates), then either that extension or a related extension shall be indicated as critical in the **crlExtensions** field. Therefore, a critical extension in the **crlEntryExtensions** field of an entry shall affect only the certificate specified in that entry, unless there is a related critical extension in the crlExtensions field that advertises a special treatment for it. The only example of this situation defined in this Specification is the certificateIssuer CRL entry extension and the related issuingDistributionPoint CRL extension when the indirectCRL boolean from that extension is set to **TRUE**.

In 8.6.2.2, replace the first four paragraphs after the ASN.1with

The **distributionPoint** component contains the name of the distribution point in one or more name forms. If this field is absent, the CRL shall contain entries for all revoked certificates issued by the CRL issuer. After a certificate appears on a CRL, it may be deleted from a subsequent CRL after the certificate's expiry. If **onlyContainsUserCerts** is **TRUE**, the CRL only contains revocations for end-entity public-key certificates. If **onlyContainsAuthorityCerts** is **TRUE**, the CRL only contains revocations for CA certificates. If **onlyContainsAttributeCerts** is **TRUE**, the CRL only contains revocations for attribute certificates. At most one of **onlyContainsUserCerts**, **onlyContainsAuthorityCerts**, and **onlyContainsAttributeCerts** shall be set to **TRUE**. If **onlySomeReasons** is present, the CRL only contains revocations of certificates for the identified reason or reasons, otherwise the CRL contains revocations for all reasons. If **indirectCRL** is **TRUE**, then the CRL may contain revocation notifications for public-key certificates issued by authorities that have a name different from the name of the issuer of the CRL. The particular authority responsible for each entry is as indicated by the **certificateIssuer** CRL entry extension in that entry or in accordance with the defaulting rules described in 8.6.2.3. Consequently, a certificate using system that is capable of processing a CRL in which **indirectCRL** is set to **TRUE**, shall also be capable of processing the **certificateIssuer** CRL entry extension. In such a CRL, it is the responsibility of the CRL issuer to ensure that the CRL is complete in that it contains all revocation entries, consistent with **onlyContainsUserCerts**, **onlyContainsAuthorityCerts**, **onlyContainsAttributeCerts** and **onlySomeReasons** indicators, from all authorities that identify this CRL issuer in their public-key certificates.

This corrects the defects reported in defect report 314

Replace the text in section 8.4.2.2 with the following:

8.4.2.2 Name constraints field

This field, which shall be used only in a CA certificate, indicates one or more name forms which have constraints placed upon their name spaces, and in which all subject names in the same name form in subsequent certificates in a certification path must be located. If this extension is absent, then no constraints are placed on any name form. If this extension if present but a name form is not included in the extension, then no constraints are imposed on that name form.

NOTE – Because there can be an unbounded set of **registeredID** name forms then in general it is not possible to constrain every possible name form of subject names with this extension.

This field is defined as follows:

```
nameConstraints EXTENSION ::= {
        SYNTAX              NameConstraintsSyntax
        IDENTIFIED BY id-ce-nameConstraints }
NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees   [0]   GeneralSubtrees OPTIONAL,
        excludedSubtrees    [1]   GeneralSubtrees OPTIONAL }
(ALL EXCEPT ({ --none; at least one component shall be present--}))

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base                        GeneralName,
        minimum             [0]     BaseDistance DEFAULT 0,
        maximum             [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)
```

At least one of **permittedSubtrees** and **excludedSubtrees** shall be present.

If present, the **permittedSubtrees** component specifies one or more subtrees, for one or more name forms, within which subject names in acceptable certificates shall be contained**.** If present, the **excludedSubtrees** component specifies one or more subtrees for one or more name forms within which subject names in acceptable certificates shall not be contained. Subject names that are compared against specified subtrees include those present in both the **subject** field and the **subjectAltNames** extension of a certificate. Each subtree is defined by the name of the root of the subtree, the **base** component, and, optionally, within that subtree, an area that is bounded by upper and/or lower levels.

The **minimum** field specifies the upper bound of the area within the subtree. All names whose final name component is above the level specified are not contained within the area. A value of **minimum** equal to zero (the default) corresponds to the base, i.e. the top node of the subtree. For example, if **minimum** is set to one, then the subtree excludes the base node but includes subordinate nodes.

The **maximum** field specifies the lower bound of the area within the subtree. All names whose last component is below the level specified are not contained within the area. A value of **maximum** of zero corresponds to the base, i.e. the top of the subtree. An absent **maximum** component indicates that no lower limit should be imposed on the area within the subtree. For example, if **maximum** is set to one, then the subtree excludes all nodes except the subtree base and its immediate subordinates.

The set of all **permittedSubtrees** and **excludedSubtrees** for a name form together comprise the constrained name space for the name form. All subject names, in certificates issued by the subject CA and subsequent CAs in a certification path, which are of a constrained name form shall be located in the constrained name space for the certificate to be acceptable.

permittedSubtrees if present, specifies the subtrees within which all the subject names that are of a constrained name form shall lie, for the certificate to be acceptable..If **excludedSubtrees** is present, any certificate issued by the subject CA or subsequent CAs in the certification path that has a subject name within these subtrees is unacceptable. If both **permittedSubtrees** and **excludedSubtrees** are present for a name form and the name spaces overlap, the exclusion statement takes precedence.

If none of the name forms of the subject name in the certificate is constrained by this extension, the certificate is acceptable.

In some situations, more than one certificate may need to be issued to satisfy the name constraints requirements. Appendix G illustrates two of these situations. For example, if names constraints are defined for multiple name forms, but a certificate needs to meet the name constraints for only one of the name forms (logical OR on constraints), then multiple certificates should be issued, each constraining a single name form.

Of the name forms available through the **GeneralName** type, only those name forms that have a well-defined hierarchical structure may be used in these fields.

The **directoryName** name form satisfies this requirement; when using this name form a naming subtree corresponds to a DIT subtree. A **certificate** is considered subordinate to the **base** (and therefore a candidate to be within the subtree) if the **SEQUENCE** of **RDNs**, which forms the full DN in **base**, is identical to the initial **SEQUENCE** of the same number of **RDN**s which forms the first part of the DN of the subject (in the **subject** field or **directoryName** of **subjectAltNames** extension) of the **certificate**. The **DN** of the subject of the **certificate** may have additional trailing **RDN**s in its sequence that do not appear in the DN in **base**. The **distinguishedNameMatch** matching rule is used to compare the value of **base** with the initial sequence of **RDN**s in the DN of the subject of the certificate.

Conformant implementations are not required to recognize all possible name forms. If the extension is flagged critical and a certificate-using implementation does not recognize a name form used in any **base** component, the certificate shall be handled as if an unrecognized critical extension had been encountered. If the extension is flagged non-critical and a certificate-using implementation does not recognize a name form used in any **base** component, then that subtree may be ignored.

> NOTE – When testing certificate subject names for consistency with a name constraint, names in non-critical subject alternative name extensions shall be processed, not ignored.

This extension may, at the option of the certificate issuer, be either critical or non-critical. It is recommended that it be flagged critical, otherwise a certificate user may not check that subsequent certificates in a certification path are located in the constrained name spaces intended by the issuing CA.

If this extension is present and is flagged critical, then a certificate-using system shall check that the certification path being processed is consistent with the value in this extension.

Annex G contains examples of use of the name constraints extension.

In section 10.5.2, delete item c) which was added by TC1 and, starts with:

c) If the **nameConstraints** extension with a **requiredNameForms** component is present in the certificate, set the *required-name-forms* variable to the union of its previous value and the set consisting of the set of name forms

In section 10.5.2, rename item d), e), f), g), h) to c), d), e), f), g) respectively.

Replace the following ASN.1 definitions associated with the nameConstraints extension in Annex A.2 from TC1

```
nameConstraints EXTENSION ::= {
        SYNTAX        NameConstraintsSyntax
        IDENTIFIED BY      id-ce-nameConstraint }

NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees     [0]      GeneralSubtrees OPTIONAL,
```

```
        excludedSubtrees      [1]     GeneralSubtrees OPTIONAL,
        requiredNameForms     [2]     NameForms OPTIONAL  }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
        base            GeneralName,
        minimum         [0]     BaseDistance DEFAULT 0,
        maximum         [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)


NameForms  ::= SEQUENCE {
    basicNameForms   [0]     BasicNameForms OPTIONAL,
    otherNameForms   [1]     SEQUENCE SIZE (1..MAX) OF OBJECT IDENTIFIER OPTIONAL }
(ALL EXCEPT ({ -- none; i.e.: at least one component shall be present -- }))


BasicNameForms  ::= BIT STRING {
        rfc822Name      (0),
        dNSName         (1),
        x400Address     (2),
        directoryName           (3),
        ediPartyName    (4),
        uniformResourceIdentifier       (5),
        iPAddress       (6),
        registeredID    (7) }  (SIZE (1..MAX))
```

with the following

```
nameConstraints EXTENSION ::= {
        SYNTAX                  NameConstraintsSyntax
        IDENTIFIED BY id-ce-nameConstraints }
NameConstraintsSyntax ::= SEQUENCE {
        permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
        excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }
(ALL EXCEPT ({ --none; at least one component shall be present--}))


GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree


GeneralSubtree ::= SEQUENCE {
        base                            GeneralName,
        minimum                 [0]     BaseDistance DEFAULT 0,
        maximum                 [1]     BaseDistance OPTIONAL }


BaseDistance ::= INTEGER (0..MAX)
```

Replace the following object identifier assignment in Annex A.2 from TC1

id-ce-nameConstraint OBJECT IDENTIFIER ::= {id-ce 30 1}

with

id-ce-nameConstraints OBJECT IDENTIFIER ::= {id-ce 30}

Replace the following set of OIDs not used in this Specification in Annex A.2 from TC1

-- The following OBJECT IDENTIFIERS are not used by this Specification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}, {id-ce 30}

with

-- The following OBJECT IDENTIFIERS are not used by this Specification:
-- {id-ce 2}, {id-ce 3}, {id-ce 4}, {id-ce 5}, {id-ce 6}, {id-ce 7},
-- {id-ce 8}, {id-ce 10}, {id-ce 11}, {id-ce 12}, {id-ce 13},
-- {id-ce 22}, {id-ce 25}, {id-ce 26}

Remove Annex G.2 "Example 2: Use of name constraints".

Move Annex G.3 "Example 3: Use of policy mapping and policy constraints" to Annex G.2 "Example 2: Use of policy mapping and policy constraints".

Add a new Annex G.3 as follows:

G.3 Use of Name Constraints Extension

G.3.1 Examples of Certificate Format with Name Constraints Extension

CAs can impose various restrictions on the subject names (in the **subject** field or **subjectAltName** extension) of subsequent certificates in the certification path, by including the Name Constraints extension in CA-certificates they issue. This section describes examples of CA-certificates including the Name Constraints extension, along with an indication of the requirements for subsequent certificates to be acceptable in a related certification path.

To simplify these examples, only the DN (directoryName) name form is used in the Name Constraints extension..

G.3.1.1 Examples of *permittedSubtrees*

(1-1) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall be equal to or subordinate to the Acme Inc. in U.S. (i.e. {C=US, O=Acme Inc}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	(void)

(1-2) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall be equal to or immediately subordinate to the Acme Inc. in U.S. (i.e. {C=US, O=Acme Inc}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **maximum 1**}}	(void)

(1-3) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall be subordinate to the Acme Inc. in U.S. (i.e. {C=US, O=Acme Inc}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**}}	(void)

(1-4) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall be equal to or subordinate to the Acme Inc. in U.S. (i.e. {C=US, O=Acme Inc}), or equal to or subordinate to the Acme Ltd. in U.K. (i.e. {C=UK, O=Acme Ltd}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=UK, O=Acme Ltd}}}	(void)

G.3.1.2 Examples of *excludedSubtrees*

(2-1) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall not be equal to nor subordinate to the Acme Corp. in Canada. (i.e. {C=CA, O=Acme Corp}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
(void)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}}

(2-2) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall not be subordinate to each immediately subordinate of the Acme Corp. in Canada (i.e. {C=CA, O=Acme Corp}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
(void)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **minimum 2**}}

(2-3) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall not be equal to the Acme Corp. in Canada (i.e. {C=CA, O=Acme Corp}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
(void)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}, **maximum 0**}}

(2-4) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall not be equal to nor subordinate to the Acme Corp. in Canada (i.e. {C=CA, O=Acme Corp}), nor equal to nor subordinate to the Asia Acme in Japan (i.e. {C=JP, O=Asia Acme}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
(void)	{{**base**(**directoryName**) {C=CA, O=Acme Corp}}, {**base**(**directoryName**) {C=JP, O=Asia Acme}}}

G.3.1.3 Examples of permittedSubtrees and excludedSubtrees

(3-1) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall be equal to or subordinate to the Acme Inc. in U.S. (i.e. {C=US, O=Acme Inc}) except the R&D organization unit of Acme Inc. and the R&D organization's subordinates for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=R&D}}}

(3-2) If the CA-certificate contains the following Name Constraints extension, for all subsequent certificates in the certification path, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form, if it exists, shall be equal to one of immediately subordinates to the Acme Inc. in U.S. (i.e. {C=US, O=Acme Inc}) except the Purchasing organization unit (i.e. {C=US, O=Acme Inc, OU=Purchasing}) for that certificate to be acceptable.

nameConstraints extension	
permittedSubtrees	**excludedSubtrees**
{{**base**(**directoryName**) {C=US, O=Acme Inc}, **minimum 1**, **maximum 1**}}	{{**base**(**directoryName**) {C=US, O=Acme Inc, OU=Purchasing}}}

G.3.2 Examples of Certificate Handling with Name Constraint Extension

This section describes examples of how subject names (in the **subject** field or **subjectAltName** extension) are validated during certificate processing with the path processing state variables, namely *permitted-subtrees* and *excluded-subtrees.*

To simplify these examples, only the DN (**directoryName**) and rfc822 name (**rfc822Name**) name forms are used in the Name Constraints extension.

G.3.2.1 Name Spaces Constraints by *permitted-subtrees* in DN Name Form

In this case, for the certificate to be acceptable, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form appearing in the certificate in question shall satisfy the constraint imposed by path processing state variable *permitted-subtrees*.

(1-1) One permitted subtree for DN is present.

Path Processing State Variables	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}}	NONE

Acceptable Certificate Examples

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {} **subjectAltName** (**rfc822Name**) = manager@purchasing.acme.com Note: *DN missing*
6	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}

Unacceptable Certificate Examples

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName** (**directoryName**) = {C=US, O=Acme Ltd, OU=Accounting}

Path Processing State Variables	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}	NONE

Acceptable Certificate Examples

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing}
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Ltd, OU= Accounting}
6	**subject =** {} **subjectAltName(rfc822Name) =** manager@purchasing.acme.com

Unacceptable Certificate Examples

1	**subject** = {C=US, O=*Acme International*, OU=Accounting}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme International*, OU=Accounting}

3	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
4	**subject** = {C=US, O=*Acme International*, OU=Accounting} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Corp*, OU=Accounting}
5	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltNam** **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com

G.3.2.2 Name Spaces Constraints by *excluded-subtrees* in DN Name Form

In this case, for the certificate to be acceptable, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form appearing in the certificate in question shall satisfy the constraint by path processing state variable *excluded-subtrees*.

(2-1) One excluded subtree for DN is present and DN is required in *required-name-forms*.

Path Processing State Variables	
permitted-subtrees	*excluded-subtrees*
NONE	{{**base**(**directoryName**) {C=US, O=Acme Ltd}}}

Acceptable Certificate Examples

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing}
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
5	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
6	**subject =** {} **subjectAltName(rfc822Name) =** manager@purchasing.acme.com

Unacceptable Certificate Examples

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Ltd*, OU=Accounting}

Path Processing State Variables	
permitted-subtrees	*excluded-subtrees*
NONE	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**directoryName**) {C=US, O=Acme Ltd}}}

Acceptable Certificate Examples

1	**subject** = {C=US, O=Acme International, OU=Purchasing}
2	**subjaect** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing}
3	**subject** = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme N.Y, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com
5	**subject** = {} **subjectAltName(rfc822Name)** = purchasing@acme-international.com

Unacceptable Certificate Examples

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
3	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Accounting}
4	**subject** = {} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme International, OU=Purchasing} **subjectAltName**(**rfc822Name**) = purchasing@acme-international.com

G.3.2.3 Name Spaces Constraints by *permitted-subtrees* in Multiple Name Forms

In this case, for the certificate to be acceptable, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form or rfc822 name form appearing in the certificate in question shall satisfy the constraint by path processing state variable *permitted-subtrees*.

One permitted subtree for DN and another permitted subtree **rfc822Name** are present.

Path Processing State Variables	
permitted-subtrees	*excluded-subtrees*
{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) {acme.com}}	NONE

Acceptable Certificate Examples

1	**subject** = {C=US, O=Acme Inc, OU=Purchasing}
2	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=Acme Inc, OU=Accounting}
4	**subject** = {} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com

Unacceptable Certificate Examples

1	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing}
2	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme.com
3	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-inc.com*
4	**subject** = {C=US, O=*Acme Ltd*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme-ltd.com*
5	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = *http://purchasing.www.acme-inc.com*
6	**subject** = {C=US, O=Acme Inc, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = *http://purchasing.www.acme-inc.com*

G.3.2.4 Name Spaces Constraints by *excluded-subtrees* in Multiple Name Forms

In this case, for the certificate to be acceptable, each subject name (in the **subject** field or **subjectAltName** extension) in DN name form or rfc822 name form appearing in the certificate in question shall satisfy the constraint by path processing state variable *excluded-subtrees*.

Path Processing State Variables	
permitted-subtrees	*excluded-subtrees*
NONE	{{**base**(**directoryName**) {C=US, O=Acme Inc}}, {**base**(**rfc822Name**) {acme.com}}

Acceptable Certificate Examples

1	**subject** = {C=US, O=Acme Ltd, OU=Purchasing}
2	**subject** = {} **suajectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-ltd.com
4	**subject** = {} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-inc.com
5	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**uniformResourceIdentifier**) = http://purchasing.www.acme-ltd.com

Unacceptable Certificate Examples

1	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing}
2	**subject** = {} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
3	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
4	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = manager@purchasing.acme-inc.com
5	**subject** = {C=US, O=*Acme Inc*, OU=Purchasing} **subjectAltName**(**rfc822Name**) = *manager@purchasing.acme.com*
6	**subject** = {C=US, O=Acme Ltd, OU=Purchasing} **subjectAltName**(**directoryName**) = {C=US, O=*Acme Inc*, OU=Accounting}

G.3.3 Examples where multiple Cross Certificates with Name Constraint Extension are needed

In some cases it may be required that more than one certificate be issued from a CA to another CA in order to achieve the desired results. This might be the case if some of the name constraints requirements conflict, or if the disjunctive evaluation of different name forms is required.

G.3.3.1 Conflicting Name Space Constraints Requirements

Assume the Acme Corporation has 20 branches in the U.S.

The Widget Corporation wants to cross-certify the central CA of Acme Corporation, but only wants the Widget community to use Acme certificates for subjects that meet the following criteria:

- Branch1 to Branch19 of Acme Corporation, all sections are acceptable as subjects;
- Branch20 of Acme Corporation, all sections are unacceptable as subjects except for subjects in the Purchasing Section.

This could be achieved by issuing two certificates as follows; the first certificate would have a **permittedSubtrees** of {base: C=US, O=Acme} and an **excludedSubtrees** of {base: C=US, O=Acme, OU=branch20}. The second certificate would have a **permittedSubtrees** of {base: C=US, O=Acme, OU=branch20, OU=Purchasing}.

G.3.3.2 Disjunctive evaluation of Name Space Constraints

Assume that the CA of one organisation X issues certificates containing Internet domain names under the subtree x.com, whilst another CA of organisation Y issues certificates containing X.500 distinguished names under the subtree o=y, c=US. Assume further that the CA of organisation A has cross certified the CAs of both organisations X and Y and that a third CA of organisation B wishes to cross certify CA A and in addition to trust the certificates that are issued by CAs X and Y. If CA B issues one cross certificate to CA A containing a name constraints extension with permitted subtrees of x.com and o=y,c=US (in addition to the name space of CA A) then if either CA X or CA Y add additional name forms to their certificates that contain either distinguished names or domain names (respectively) then their certificates will no longer be valid for relying parties who have CA B as their trust anchor. One solution to this problem is that CA B should issue two cross certificates to CA A, one containing a name constraints extension with the permitted subtree of x.com, and the other containing the permitted subtree of o=y,c=US.