Constraining Kerberos Names in X.509 Certificates
draft-rabinovich-krb-wg-x509-name-constraints-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on March 14, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).
Abstract

This document specifies mechanisms for constraining Kerberos names in X.509 certificates. These mechanisms are defined within the name constraints framework standardized in RFC 3280 [2] and apply to Kerberos names in X.509 certificates compliant with RFC 4556 [4].

Table of Contents

1. Introduction ............................................. 3
2. Conventions Used in This Document ......................... 4
3. Preliminaries ........................................... 5
   3.1. Names in X.509 Certificates .......................... 5
   3.2. Name Constraints in X.509 Certificates ............... 5
   3.3. Kerberos Names ...................................... 5
4. Kerberos Name Constraints ................................. 8
   4.1. General ............................................ 8
   4.2. Exact Full Name Match ............................... 8
   4.3. Exact Realm Name Match .............................. 9
   4.4. Suffix Realm Name Match ............................ 9
5. Other Name Constraints Applicable to Kerberos Names ....... 12
   5.1. Overview ........................................... 12
   5.2. rfc822Name Name Constraint ........................ 12
   5.3. dNSName Name Constraint ............................ 12
   5.4. x400Address Name Constraint ........................ 12
   5.5. directoryName Name Constraint ........................ 12
   5.6. uniformResourceIdName Constraint .................... 13
   5.7. iPAddress Name Constraint .......................... 13
6. Security Considerations .................................. 14
7. IANA Considerations ...................................... 15
8. References .............................................. 16
   8.1. Normative References ................................ 16
   8.2. Informative References .............................. 16
Author’s Address ........................................... 17
Intellectual Property and Copyright Statements ............... 18
1. Introduction

This document defines the syntax and semantics of constraints imposed on Kerberos names used in X.509 certificates.

The X.509 specification [7] and RFC 3280 [2] define the concept of name constraints that guide acceptance rules for names placed by Certification Authorities (CAs) in X.509 certificates they issue to other CAs or to end entities. Name constraints apply to names in the Subject field and the Subject Alternative Name extension of X.509 certificates.

RFC 4556 [4] defines syntax of Kerberos names used in X.509 certificates without defining mechanisms for constraining such names. This is the purpose of this document. Name constraints defined here are meant to be applied by relying parties to RFC 4556-style Kerberos names.
2. Conventions Used in This Document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].
3. Preliminaries

3.1. Names in X.509 Certificates

The X.509 specification [7] and RFC 3280 [2] stipulate the use of subject names at two locations in the certificates: (a) in the Subject field as an X.500 name and (b) in the Subject Alternative Name extension. Well-known name types that may be placed in the Subject Alternative Name extension include RFC 822- and X.400-compliant e-mail addresses, host names, additional X.500 names, URIs and IP addresses. An extension mechanism is provided for custom name types usable by specific organizations, applications or communities of interest. This extension mechanism is implemented through the otherName choice of the type GeneralName [2]:

OtherName ::= SEQUENCE {
    type-id    OBJECT IDENTIFIER,
    value      [0] EXPLICIT ANY DEFINED BY type-id
}

3.2. Name Constraints in X.509 Certificates

Sometimes CAs issuing X.509 certificates to other CAs want to constrain the subject names used by these (other) CAs and their subordinated CAs. For instance, an enterprise-wide CA for the domain example.com may want to allow CAs in the organizational units unit1.example.com and unit2.example.com to issue certificates only for those units. unit1.example.com’s CA will not be allowed to issue a certificate to the host host.unit2.example.com but will be allowed to issue a certificate to the host host.unit2.example.com (in truth they can issue such certificates but standards-compliant relying parties will reject them as violating name constraints placed by example.com’s CA). RFC 3280 [2] defines name constraints for hierarchical namespaces only. They can be expressed in terms of permitted or excluded subtrees. Every name type may have a corresponding set of name constraints specified higher in the certification path although the syntax and semantics of these constraints have been defined only for a subset of well-known name types and have not been defined at all for others [2]

3.3. Kerberos Names

RFC 4556 [4] specializes the type OtherName from RFC 3280 [2] for the needs of PKINIT, a protocol integrating X.509 certificate-based public key cryptography into the initial authentication exchange with Kerberos KDCs. RFC 4556 sets the type-id field of the type OtherName to
id-pkinit-san OBJECT IDENTIFIER ::= 
{ iso(1) org(3) dod(6) internet(1) security(5) kerberosv5(2) 
x509SanAN (2) }

and redefines the value field of the OtherName as a KRB5PrincipalName. KRB5PrincipalName is defined as

KRB5PrincipalName ::= SEQUENCE {
    realm            [0] Realm,
    principalName    [1] PrincipalName
}

The types Realm and PrincipalName are part of the definition of the Kerberos protocol itself given in RFC 4120 [3]:

Realm ::= KerberosString

PrincipalName ::= SEQUENCE {
    name-type        [0] Int32,
    name-string      [1] SEQUENCE OF KerberosString
}

Realm names may be in the style of a DNS domain name, X.500 name, "other" and reserved.

Finally, the name-type field of the type PrincipalName may take one of the following values (again per RFC 4120 [3]):

- NT-UNKNOWN: Name type not known
- NT-PRINCIPAL: Name of the principal
- NT-SRV-INST: Service and other unique instance (e.g., krbtgt)
- NT-SRV-HST: Host-bound (DNS name) instance of a service (e.g., telnet, r* commands)
- NT-SRV-XHST: Host-bound (X.500 name or other) instance of a service
- NT-UID: Unique ID
- NT-X500-PRINCIPAL: Encoded X.500 distinguished name
- NT-SMTP-NAME: Name in the form of an SMTP e-mail name (e.g., user@example.com)
o NT-ENTERPRISE: Enterprise name (may be mapped to a principal name)
4. Kerberos Name Constraints

4.1. General

Kerberos name constraints are defined within the general framework for name constraints in X.509 certificates specified in [2]. These constraints are applicable only to Kerberos names in the Subject Alternative Name extension defined according to RFC 4556 [4]. A relying party encountering such a name asserted in an X.509 certificate MUST apply Kerberos and other name constraints (see Section 5) according to the general rules in RFC 3280 [2] and the specific rules in this document.

A Kerberos name constraint has the same basic format as a Kerberos name. This format is defined in RFC 4556 [4]: the type-id field of the type OtherName is id-pkinit-san, and the value field of the type OtherName is a KRB5PrincipalName.

This document defines three types of Kerberos name constraints:

- Exact full name match: The asserted Kerberos name must exactly match the full Kerberos name specified in the constraint.
- Exact realm name match: The realm name of the asserted Kerberos name must exactly match the realm name specified in the constraint.
- Suffix realm name match: The suffix of the realm name in the asserted Kerberos name must match the realm name specified in the constraint.

Each Kerberos name constraint type is discussed in a separate section below.

4.2. Exact Full Name Match

An exact full name match occurs when the asserted Kerberos name exactly matches the full Kerberos name specified in the constraint. A relying party recognizes an exact full name match constraint when the value of the name-string field of the type PrincipalName is set to a non-empty SEQUENCE.

Since the name-type field of the type PrincipalName is used only as a hint for interpreting the meaning of the name, and it is not significant when checking for name equivalence [3], it SHOULD be set to NT-UNKNOWN.

Relying parties MUST use the rules of RFC 4120 [3] to determine if
the two Kerberos names (one asserted and the other specified in the constraint) match.

Example 1 (match). The Kerberos name ("EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) satisfies the exact full name match constraint ("EXAMPLE.COM", (NT-UNKNOWN, ("user1"))).

Example 2 (mismatch). The Kerberos name ("EXAMPLE.COM", (NT-PRINCIPAL, ("user2"))) does not satisfy the exact full name match constraint ("EXAMPLE.COM", (NT-UNKNOWN, ("user1"))).

Example 3 (mismatch). The Kerberos name ("EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) does not satisfy the exact full name match constraint ("EXAMPLE.NET", (NT-UNKNOWN, ("user1"))).

4.3. Exact Realm Name Match

An exact realm name match occurs when the realm name of the asserted Kerberos name exactly matches the realm name specified in the constraint. A relying party recognizes an exact realm name match constraint when the value of the name-string field of the type PrincipalName is set to an empty SEQUENCE and the realm field of the type KRB5PrincipalName contains a literal realm name (i.e., not a pattern as defined in Section 4.4).

The issuing CA SHOULD set the name-type field of the type PrincipalName to NT-UNKNOWN.

Relying parties MUST use the rules of RFC 4120 [3] to determine if the two realm names (one in the asserted Kerberos name and the other specified in the constraint) match.

Example 1 (match). The Kerberos name ("EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) satisfies the exact realm name match constraint ("EXAMPLE.COM", (NT-UNKNOWN, ())).

Example 2 (mismatch). The Kerberos name ("EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) does not satisfy the exact realm name match constraint ("EXAMPLE.NET", (NT-UNKNOWN, ())).

4.4. Suffix Realm Name Match

A suffix realm name match occurs when the suffix of the realm name in the asserted Kerberos name matches the realm name specified in the constraint.

Suffix realm name match constraints are defined only for the domain and X.500 styles of realm names specified in RFC 4120 [3]. This
To specify suffix matching for a domain-style realm name, the realm field of the type KRB5PrincipalName in the constraint MUST have a single "." (dot) character prepended to it. The rest of the realm name MUST be a valid domain-style realm name according to RFC 4120 [3]. An asserted Kerberos name satisfies a suffix realm name constraint if its realm name represents a subdomain of the domain specified in the constraint.

To specify suffix matching for an X.500-style realm name, the realm field of the type KRB5PrincipalName in the constraint MUST have a single "/" (slash) character appended to it. The rest of the realm name MUST be a valid X.500-style realm name according to RFC 4120 [3]. An asserted Kerberos name satisfies a suffix realm name constraint if its realm name represents a more specific X.500 name than the X.500 name specified in the constraint.

The issuing CA SHOULD set the name-type field of the type PrincipalName to NT-UNKNOWN.

Relying parties MUST use the rules of RFC 4120 [3] to determine if the two realm names (one in the asserted Kerberos name and the other specified in the constraint) match.

Example 1 (domain-style realm name, match). The Kerberos name ("REALM1.EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) satisfies the suffix realm name match constraint (".EXAMPLE.COM", (NT-UNKNOWN, ())).

Example 2 (domain-style realm name, mismatch). The Kerberos name ("REALM1.EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) does not satisfy the suffix realm name match constraint (".EXAMPLE.NET", (NT-UNKNOWN, ())).

Example 3 (domain-style realm name, mismatch). The Kerberos name ("EXAMPLE.COM", (NT-PRINCIPAL, ("user1"))) does not satisfy the suffix realm name match constraint (".EXAMPLE.COM", (NT-UNKNOWN, ())).

Example 4 (X.500-style realm name, match). The Kerberos name ("C=US/O=OSF/OU=DCE", (NT-PRINCIPAL, ("user1"))) satisfies the suffix realm name match constraint ("C=US/O=OSF/", (NT-UNKNOWN, ())).

Example 5 (X.500-style realm name, mismatch). The Kerberos name ("C=US/O=OSF/OU=DCE", (NT-PRINCIPAL, ("user1"))) does not satisfy the suffix realm name match constraint ("C=US/O=OSF1/", (NT-UNKNOWN,
Example 6 (X.500-style realm name, mismatch). The Kerberos name
("C=US/O=OSF", (NT-PRINCIPAL, ("user1"))) does not satisfy the suffix
realm name match constraint ("C=US/O=OSF/", (NT-UNKNOWN, ())).
5. Other Name Constraints Applicable to Kerberos Names

5.1. Overview

Several types of Kerberos names include components corresponding to other name types used in X.509 certificates. For example, an NT-SRV-HST name (the name-string field of the type PrincipalName) consists of two components: a service name (e.g., "telnet") and a host name [3]. Host names in X.509 certificates are usually constrained using the dNSName constraint [2]. Similarly, name constraints defined in [2] are applicable to several other Kerberos name types. Each subsection below is dedicated to a single type of name constraint from [2] and its applicability to Kerberos names.

5.2. rfc822Name Name Constraint

If present, an rfc822Name name constraint SHOULD be applied to all asserted Kerberos names with the name-type field of the type PrincipalName set to NT-SMTP-NAME. To satisfy the constraint the asserted Kerberos name’s name-string field MUST be a SEQUENCE with a single element that matches the rfc822Name in the name constraint according to the rules of RFC 3280 [2].

5.3. dNSName Name Constraint

If present, a dNSName name constraint SHOULD be applied to all asserted Kerberos names with the name-type field of the type PrincipalName set to NT-SRV-HST. To satisfy the constraint the asserted Kerberos name’s name-string field MUST be a SEQUENCE with two elements the second of which matches the dNSName in the name constraint according to the rules of RFC 3280 [2].

5.4. x400Address Name Constraint

Not applicable.

5.5. directoryName Name Constraint

If present, a directoryName name constraint SHOULD be applied to all asserted Kerberos names with the name-type field of the type PrincipalName set to NT-SRV-XHST and to all asserted Kerberos names with the name-type field of the type PrincipalName set to NT-X500-PRINCIPAL.

To satisfy the constraint the asserted NT-X500-PRINCIPAL Kerberos name’s name-string field MUST represent a valid sequence of string representations of relative distinguished names and MUST match the directoryName in the name constraint according to the rules of RFC
To satisfy the constraint the asserted NT-SRV-XHST Kerberos name’s name-string field MUST be a SEQUENCE with at least two components all but the first of which represent relative distinguished names [6] and, taken together, match the directoryName in the name constraint according to the rules of RFC 3280 [2].

5.6. uniformResourceIdentifier Name Constraint

   Not applicable.

5.7. iPAddress Name Constraint

   Not applicable.
6. Security Considerations

The IT infrastructures of many organizations use Kerberos names as a primary name form for end entities (e.g., users). Used in X.509 certificates a Kerberos name can provide a unique and stable end-entity identifier in PKI-aware non-Kerberized applications. It can also be used for cross-enterprise certificate-based authentication to uniquely identify external users.

X.509 name constraints allow Certification Authorities to restrict namespaces used by subordinate and other CAs to which they issue certificates: such CAs may issue certificates only to entities within their sphere of authority. Name constraints provide one mechanism to specify these spheres. As Kerberos names gain in importance, the notion of name constraints should be extended to Kerberos names as well. This document stipulates that relying parties MUST verify asserted Kerberos names against the Kerberos name constraints present in certificates located higher in the certification path.

RFC 3280 [2] requires name constraints to be marked critical. It means that a relying party not aware of Kerberos name constraints MUST fail validation and declare the end-entity certificate invalid.

Non-Kerberos name constraints may also apply to Kerberos names. It is RECOMMENDED that relying parties apply these name constraints as described in Section 5. Relying parties should keep in mind that NT-SMTP-NAMEs may represent names that are not, in fact, RFC 822 e-mail addresses but only look like e-mail addresses. Similarly, an NT-X500-PRINCIPAL name may look like a valid sequence of relative distinguished names but not represent any real distinguished name.

Finally, since the definition of name equivalence does not include the name-type field of the type PrincipalName [3], issuing CAs may circumvent the application of non-Kerberos name constraints by labeling the asserted Kerberos names as NT-PRINCIPALs or other name types not subject to such constraints. If validation of these constraints is of utmost importance to a relying party it SHOULD trust only those CAs whose Certificate Policies include language guaranteeing the proper use of Kerberos names in X.509 certificates by subordinate and other CAs downstream; such language SHOULD be enforced by proper auditing procedures. See RFC 3647 [5] for details on Certificate Policies.
7. IANA Considerations

This document has no actions for IANA.
8. References

8.1. Normative References


8.2. Informative References


Author’s Address

Paul Rabinovich
Exostar, LLC
13530 Dulles Technology Drive
Suite 200
Herndon, VA 20171
US

Email: paul.rabinovich@exostar.com