Network Working Group
Request for Comments: 4985
Category: Standards Track

S. Santesson
Microsoft

August 2007

Internet X.509 Public Key Infrastructure Subject Alternative Name for Expression of Service Name

Status of This Memo

Abstract

This document defines a new name form for inclusion in the otherName field of an X.509 Subject Alternative Name extension that allows a certificate subject to be associated with the service name and domain name components of a DNS Service Resource Record.

Table of Contents

1. Introduction

This document specifies a name form for inclusion in X.509 certificates that may be used by a certificate relying party to verify that a particular host is authorized to provide a specific service within a domain.

RFC 2782 [N3] defines a DNS RR (Resource Record) for specifying the location of services (SRV RR), which allows clients to ask for a specific service/protocol for a specific domain and get back the names of any available servers.

Existing name forms in X.509 certificates support authentication of a host name. This is useful when the name of the host is known by the client prior to authentication.

When a server host name is discovered through DNS RR lookup query based on service name, the client may need to authenticate the server's authorization to provide the requested service in addition to the server's host name.

While DNS servers may have the capacity to provide trusted information, there may be many other situations where the binding between the name of the host and the provided service needs to be supported by additional credentials.

Current dNSName GeneralName Subject Alternative name form only provides for DNS host names to be expressed in "preferred name syntax", as specified by RFC 1034 [N4]. This definition is therefore not broad enough to allow expression of a service related to that domain.

1.1. Terminology

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 [N1].

2. Name Definitions

This section defines the SRVName name as a form of otherName from the GeneralName structure in SubjectAltName defined in RFC 3280 [N2].

```
id-on-dnsSRV OBJECT IDENTIFIER ::= { id-on 7 }

SRVName ::= IA5String (SIZE (1..MAX))
```

The SRVName, if present, MUST contain a service name and a domain name in the following form:

_Service.Name

The content of the components of this name form MUST be consistent with the corresponding definition of these components in an SRV RR according to RFC 2782 [N3].

The content of these components are:

Service
The symbolic name of the desired service, as defined in Assigned Numbers [N5] or locally. An underscore (_) is prepended to the service identifier to avoid collisions with DNS labels that occur in nature. Some widely used services, notably POP, don't have a single universal name. If Assigned Numbers names the service indicated, that name is the only name that is allowed in the service component of this name form. The Service is case insensitive.

Name
The DNS domain name of the domain where the specified service is located.

If the domain name is an Internationalized Domain Name (IDN), then encoding in ASCII form SHALL be done as defined in section 3.

Even though this name form is based on the service resource record (SRV RR) definition in RFC 2782 [N3] and may be used to enhance subsequent authentication of DNS-based service discovery, this standard does not define any new conditions or requirements regarding use of SRV RR for service discovery or where and when such use is appropriate.

The format of a DNS RR, according to RFC 2782, also includes a protocol component (_Service._Proto.Name). This protocol component is not included in the SRVName specified in this document. The purpose of the SRVName is limited to authorization of service provision within a domain. It is outside the scope of the SRVName to provide any means to verify that the host is using any intended protocol. By omitting the protocol component from the SRVName two important advantages have been achieved:

* One certificate with a single SRVName can be issued to a host that offers multiple protocol alternatives.

* Name constraints processing rules (specified in section 4)are significantly less complex to define without the protocol component.

A present SRVName in a certificate MUST NOT be used to identify a host unless one of the following conditions applies:

* Use of this name form is specified by the security protocol being used and the identified service has a defined service name according to RFC 2782, or;

* Use of this name form is configured by local policy.

3. Internationalized Domain Names

IA5String is limited to the set of ASCII characters. To accommodate internationalized domain names in the current structure, conforming implementations MUST convert internationalized domain names to the ASCII Compatible Encoding (ACE) format as specified in section 4 of RFC 3490 [N6] before storage in the Name part of SRVName. Specifically, conforming implementations MUST perform the conversion operation specified in section 4 of RFC 3490 [N6], with the following clarifications:

* in step 1, the domain name SHALL be considered a "stored string". That is, the AllowUnassigned flag SHALL NOT be set;

* in step 3, set the flag called "UseSTD3ASCIIRules";

* in step 4, process each label with the "ToASCII" operation; and

* in step 5, change all label separators to U+002E (full stop).

When comparing DNS names for equality, conforming implementations MUST perform a case-insensitive exact match on the entire domain name. When evaluating name constraints, conforming implementations MUST perform a case-insensitive exact match on a label-by-label basis.

Implementations SHOULD convert IDNs to Unicode before display. Specifically, conforming implementations SHOULD perform the conversion operation specified in section 4 of RFC 3490 [N6], with the following clarifications:

* in step 1, the domain name SHALL be considered a "stored string". That is, the AllowUnassigned flag SHALL NOT be set;

* in step 3, set the flag called "UseSTD3ASCIIRules";

* in step 4, process each label with the "ToUnicode" operation; and

* skip step 5.

Note: Implementations MUST allow for increased space requirements for IDNs. An IDN ACE label will begin with the four additional characters "xn--" and may require as many as five ASCII characters to specify a single international character.

4. Name Constraints Matching Rules

Name constraining, as specified in RFC 3280, MAY be applied to the SRVName by adding name restriction in the name constraints extension in the form of an SRVName.

SRVName restrictions are expressed as a complete SRVName (_mail.example.com), just a service name (_mail), or just as a DNS name (example.com). The name restriction of the service name part and the DNS name part of SRVName are handled separately.

If a service name is included in the restriction, then that restriction can only be satisfied by an SRVName that includes a corresponding service name. If the restriction has an absent service name, then that restriction is satisfied by any SRVName that matches the domain part of the restriction.

DNS name restrictions are expressed as host.example.com. Any DNS name that can be constructed by simply adding subdomains to the left-hand side of the name satisfies the DNS name part of the name constraint. For example, www.host.example.com would satisfy the constraint (host.example.com) but 1host.example.com would not.

Examples:

Name Constraints SRVName restriction	Matching SRVName	non-matching SRVName
example.com	_mail.example.com _ntp.example.com _mail.1.example.com	_mail.1example.com
_mail	_mail.example.com _mail.1example.com	_ntp.example.com
_mail.example.com	_mail.example.com _mail.1.example.com	_mail.1example.com _ntp.example.com

5. Security Considerations

Assignment of services to hosts may be subject to change. Implementers should be aware of the need to revoke old certificates that no longer reflect the current assignment of services and thus make sure that all issued certificates are up to date.

When X.509 certificates enhanced with the name form specified in this standard is used to enhance authentication of service discovery based on an SRV RR query to a DNS server, all security considerations of RFC 2782 applies.

6. Normative References

[N1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[N2] Housley, R., Polk, W., Ford, W., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[N3] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[N4] Mockapetris, P., "DOMAIN NAMES - CONCEPTS AND FACILITIES", STD 13, RFC 1034, November 1987

[N5] Reynolds, J., "Assigned Numbers: RFC 1700 is Replaced by an On-line Database", RFC 3232, January 2002.

[N6] Faltstrom, P., Hoffman, P., and A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, March 2003.

Appendix A. ASN.1 Syntax

As in RFC 2459, ASN.1 modules are supplied in two different variants of the ASN.1 syntax.

This section describes data objects used by conforming Public Key Infrastructure (PKI) components in an "ASN.1-like" syntax. This syntax is a hybrid of the 1988 and 1993 ASN.1 syntaxes. The 1988 ASN.1 syntax is augmented with the 1993 UNIVERSAL Type UTF8String.

The ASN.1 syntax does not permit the inclusion of type statements in the ASN.1 module, and the 1993 ASN.1 standard does not permit use of the new UNIVERSAL types in modules using the 1988 syntax. As a result, this module does not conform to either version of the ASN.1 standard.

Appendix A.1 may be parsed by an 1988 ASN.1-parser by replacing the definitions for the UNIVERSAL Types with the 1988 catch-all "ANY".

Appendix A.2 may be parsed "as is" by a 1997-compliant ASN.1 parser.

In case of discrepancies between these modules, the 1988 module is the normative one.

Appendix A.1. 1988 ASN.1 Module

```
PKIXServiceNameSAN88 {iso(1) identified-organization(3) dod(6)
      internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-dns-srv-name-88(39) }

DEFINITIONS EXPLICIT TAGS ::=

   BEGIN

   -- EXPORTS ALL --

   IMPORTS

-- UTF8String, / move hyphens before slash if UTF8String does not
-- resolve with your compiler

     id-pkix
           FROM PKIX1Explicit88 { iso(1) identified-organization(3)
           dod(6) internet(1) security(5) mechanisms(5) pkix(7)
           id-mod(0) id-pkix1-explicit(18) } ;
           -- from RFC3280 [N2]
```

```
     -- Service Name Object Identifier and Syntax
     -- id-pkix OBJECT IDENTIFIER ::= {1 3 6 1 5 5 7}

     id-on   OBJECT IDENTIFIER ::= { id-pkix 8 }

     id-on-dnsSRV OBJECT IDENTIFIER ::= { id-on 7 }

     SRVName ::= IA5String    (SIZE (1..MAX))

   END
```

Appendix A.2. 1993 ASN.1 Module

```
   PKIXServiceNameSAN93 {iso(1) identified-organization(3) dod(6)
       internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
       id-mod-dns-srv-name-93(40) }

   DEFINITIONS EXPLICIT TAGS ::=

   BEGIN

   -- EXPORTS ALL --

   IMPORTS

      id-pkix
            FROM PKIX1Explicit88 { iso(1) identified-organization(3)
            dod(6) internet(1) security(5) mechanisms(5) pkix(7)
            id-mod(0) id-pkix1-explicit(18) } ;
             -- from RFC 3280 [N2]


   -- In the GeneralName definition using the 1993 ASN.1 syntax
   -- includes:

   OTHER-NAME ::= TYPE-IDENTIFIER


   -- Service Name Object Identifier

   id-on   OBJECT IDENTIFIER ::= { id-pkix 8 }

   id-on-dnsSRV OBJECT IDENTIFIER ::= { id-on 7 }
```

```
   -- Service Name

   srvName OTHER-NAME ::= { SRVName IDENTIFIED BY { id-on-dnsSRV }}

   SRVName ::= IA5String (SIZE (1..MAX))

   END
```

Author's Address

Stefan Santesson
Microsoft
Tuborg Boulevard 12
2900 Hellerup
Denmark

EMail: stefans@microsoft.com

Full Copyright Statement

Intellectual Property