GSS-API Domain-Based Service Names and Name Type
draft-ietf-kitten-gssapi-domain-based-names-02.txt

Status of this Memo

Copyright Notice

Abstract

This document describes domainname-based service principal names and
the corresponding name type for the Generic Security Service
Application Programming Interface (GSS-API).

Domain-based service names are similar to host-based service names,
but using a domain name (not necessarily an Internet domain name)
instead of or in addition to a hostname. The primary purpose of
domain-based service names is to provide a way to name clustered
services after the domain which they service, thereby allowing their

   clients to authorize the service's servers based on authentication of
   their names.

Table of Contents

1. 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 [RFC2119].

[2](#). **Introduction**

   The use of hostbased principal names for domain-wide services
   presents the problem of how to distinguish between an instance of a
   hostbased service that is authorized to respond for a domain and one
   that isn't.

   Consider LDAP. LDAP [[RFC3377](#)] with SASL [[RFC2222](#)] and the Kerberos V
   mechanism [[RFC1964](#)] for the GSS-API [[RFC2743](#)] uses a hostbased
   principal with a service name of "ldap", a reasonable approach,
   provided there is only one logical LDAP directory in a Kerberos
   realm's domain, and that all ldap servers in that realm serve that
   one LDAP directory. An network might have multiple, distinct LDAP
   services, but only one LDAP "name service"; if so then clients could
   not tell which LDAP service principals are authorized to serve which
   directory, not without assuming a secure method for finding LDAP
   servers (e.g., DNSSEC). This is a significant, and oft-unstated
   restriction on users of LDAP.

   Domain based names can eliminate this problem: the use of domain-
   based names should imply that the given host is a server for the
   official LDAP name service of the given domain.

   Notwithstanding the LDAP example the use of domain-based principal
   names for LDAP is not actually specified here and will be specified
   in a separate document.

   A domain-based name consists of three required elements:

   o a service name

   o a domain name

   o a hostname

3. Name Type OID and Symbolic Name

The new name type has an OID of

[NOTE: OID assignment to be made with IANA.]

{iso(1) org(3) dod(6) internet(1) security(5) nametypes(6) gss-domain-based(5)}

The recommended symbolic name for this GSS-API name type is "GSS_C_NT_DOMAINBASED_SERVICE".

4. Query and Display Syntaxes

   There is a single name syntax for domain-based names.

   The syntax is:

      domain-based-name :=

         | <service> '@' <domain> '@' <hostname>

   Note that for Internet domain names the trailing '.' is not and MUST
   NOT be included in the domain name (or hostname) parts of the display
   form GSS-API domain-based MNs.

5. Examples

o ldap@example.tld@ds1.example.tld

o kadmin@example.tld@kdc1.example.tld

6. Security Considerations

Use of GSS-API domain-based names may not be negotiable by some GSS-API mechanisms, and some acceptors may not support GSS-API domain-based names. In such cases initiators are left to fallback on the use of hostbased names, in which case the initiators MUST also verify that the acceptor's hostbased name is authorized to provide the given service for the domain that the initiator had wanted.

The above security consideration also applies to all GSS-API initiators who lack support for domain-based service names.

7. References

7.1. Normative

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119, March 1997.

   [RFC2743]   Linn, J., "Generic Security Service Application Program
               Interface Version 2, Update 1", RFC 2743, January 2000.

7.2. Informative

   [RFC1964]   Linn, J., "The Kerberos Version 5 GSS-API Mechanism",
               RFC 1964, June 1996.

   [RFC2222]   Myers, J., "Simple Authentication and Security Layer
               (SASL)", RFC 2222, October 1997.

   [RFC3377]   Hodges, J. and R. Morgan, "Lightweight Directory Access
               Protocol (v3): Technical Specification", RFC 3377,
               September 2002.

Author's Address

    Nicolas Williams
    Sun Microsystems
    5300 Riata Trace Ct
    Austin, TX 78727
    US

    Email: Nicolas.Williams@sun.com

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment