KERBEROS WORKING GROUP	Johansson	
Internet-Draft	SUNET	
Intended status: Standards Track	Nov 13, 2010	
Expires: May 17, 2011		

TOC

An information model for Kerberos version 5
draft-ietf-krb-wg-kdc-model-09

Abstract

This document describes an information model for Kerberos version 5 from the point of view of an administrative service. There is no standard for administrating a kerberos 5 KDC. This document describes the services exposed by an administrative interface to a KDC.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.
Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.
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.”
This Internet-Draft will expire on May 17, 2011.

such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

---

1. Introduction

TOC

The Kerberos version 5 authentication service described in [RFC4120] (Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network

Authentication Service (V5),” July 2005.) describes how a Key Distribution Center (KDC) provides authentication to clients. The standard does not stipulate how a KDC is managed and several "kadmin" servers have evolved. This document describes the services required to administer a KDC and the underlying information model assumed by a kadmin-type service.

The information model is written in terms of "attributes" and "services" or "interfaces" but the use of these particular words must not be taken to imply any particular modeling paradigm. Neither an object oriented model nor an LDAP schema is intended. The author has attempted to describe in natural language the intended semantics and syntax of the components of the model. An LDAP schema (for instance) based on this model will be more precise in the expression of the syntax while preserving the semantics of this model.

Implementations of this document MAY decide to change the names used (e.g. principalName). If so an implementation MUST provide a name to name mapping to this document.

---

2. Requirements notation

TOC

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] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

This document describes an information model for kerberos 5 but does not directly describe any mapping onto a particular schema- or modelling language. Hence an implementation of this model consists of a mapping to such a language - e.g. an LDAP or SQL schema. The precise interpretation of terms from [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) therefore require some extra explanation.

The terms MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT mean that an implementation MUST provide a feature but does not mean that this feature MUST be REQUIRED by the implementation - e.g. an attribute is available in an LDAP schema but marked as OPTIONAL. If a feature must be implemented and REQUIRED this is made explicit in this model. The term MAY, OPTIONAL and RECOMMENDED means that an implementation MAY need to REQUIRE the feature due to the particular nature of the schema/ modelling language. In some cases this is expressly forbidden by this model (feature X MUST NOT be REQUIRED by an implementation).

TOC

3. Information model demarcation

The information model specified in the next chapter describes objects, properties of those objects and relations between those objects. These elements comprise an abstract view of the data represented in a KDC. It is important to understand that the information model is not a schema. In particular the way objects are compared for equality beyond that which is implied by the specification of a syntax is not part of this specification. Nor is ordering specified between elements of a particular syntax.
Further work on Kerberos will undoubtedly prompt updates to this information model to reflect changes in the functions performed by the KDC. Such extensions to the information model should always use a normative reference to the relevant RFCs detailing the change in KDC function.
This model describes a number of elements related to password policy management. Not all of the elements in this model are unique to Kerberos; an LDAP implementation of this model should incorporate existing LDAP schema where functional overlap exists, rather than defining additional Kerberos-specific elements.

---

4. Information model specification

TOC

4.1. Principal

TOC

The fundamental entity stored in a KDC is the principal. The principal is associated to keys and generalizes the "user" concept. The principal MUST be implemented in full and MUST NOT be optional in an implementation

---

4.1.1. Principal: Attributes

TOC

4.1.1.1. principalName

TOC

The principalName MUST uniquely identify the principal within the administrative context of the KDC. The principalName MUST be equivalent

to the string representation of the principal name including, if applicable for the name type, the realm.
The attribute MAY be multi-valued if the implementation supports aliases and/or enterprise names. In that case exactly one of the principalName values MAY be designated the canonical principalName and if the implementation supports enctypes which require salt then exactly one of the values of principalName MAY be designated as the canonical salting principalName.
Implementations (i.e. schema) that support enterprise names and/or aliases SHOULD provide for efficient lookup of principal objects based on alias/enterprise name.

4.1.1.2. principalNotUsedBefore

TOC

The principal may not be used before this date. The syntax of the attribute MUST be semantically equivalent with the standard ISO date format. The attribute MUST be single-valued.

4.1.1.3. principalNotUsedAfter

TOC

The principal may not be used after this date. The syntax of the attribute MUST be semantically equivalent with the standard ISO date format. The attribute MUST be single-valued.

4.1.1.4. principalIsDisabled

TOC

A boolean attribute used to disable a principal. The attribute SHOULD default to false.

4.1.1.5. principalNumberOfFailedAuthenticationAttempts

TOC

This single-valued integer attribute contains a count of the number of times an authentication attempt was unsuccessful for this principal. Implementations SHOULD NOT allow this counter to be reset.

TOC

4.1.1.6. principalLastFailedAuthentication

This single-valued attribute contains the time and date for the last failed authentication attempt for this principal.

4.1.1.7. principalLastSuccessfulAuthentication

TOC

This single-valued attribute contains the time and date for the last successful authentication attempt for this principal.

4.1.1.8. principalLastCredentialChangeTime

TOC

This single-valued attribute contains the time and date for the last successful change of credential (e.g. password or private key) associated with this principal.

4.1.1.9. principalCreateTime

TOC

This single-valued attribute contains the time and date when this principal was created

---

4.1.1.10. principalModifyTime

TOC

This single-valued attribute contains the time and date when this principal was modified excluding credentials change.

4.1.1.11. principalMaximumTicketLifetime

TOC

This single-valued attribute contains the delta time in seconds representing the maximum lifetime for tickets issued for this principal.

TOC

4.1.1.12. principalMaximumRenewableTicketLifetime

This single-valued attribute contains the delta time in seconds representing the maximum amount of time a ticket may be renewed for.

4.1.1.13. principalAllowedEnctype

TOC

This OPTIONAL multi-valued attribute lists the enctypes allowed for this principal. If empty or absent any enctype supported by the implementation is allowed for this principal.
This attribute is intended as a policy attribute and restricts all uses of enctypes including server, client, and session keys. Data models MAY choose to use policy objects in order to represent more complex decision mechanisms.

4.1.2. Principal: Associations

TOC

Each principal MAY be associated with 0 or more KeySet and MAY be associated with 0 or more Policies. The KeySet is represented as an object in this model since it has attributes associated with it (the key version number). In typical situations the principal is associated with exactly 1 KeySet but implementations MUST NOT assume this case, i.e. an implementation of this standard MUST be able to handle the general case of multiple KeySet associated with each principal. Multiple KeySets may for instance be useful when performing a key rollover for a principal.

4.2. KeySet

TOC

A KeySet is a set of keys associated with exactly one principal. This object and its associations MUST NOT be REQUIRED by a data-model. It is expected that most Kerberos implementations will use the set/change password protocol for all aspects of key management [I-D.ietf-krb-wg-kerberos-set-passwd] (Williams, N., “Kerberos Set/Change Key/Password Protocol Version 2,” November 2008.). This information model only includes these objects for the sake of completeness.
If a server supports an enctype for a principal that enctype must be present in at least one key for the principal in question.

4.2.1. KeySet: Attributes

TOC

4.2.1.1. keySetVersionNumber

TOC

This is traditionally called the key version number (kvno). This is a single-valued attribute containing a positive integer.

4.2.2. KeySet: Associations

TOC

To each KeySet MUST be associated a set of 1 or more Keys.

4.2.3. KeySet: Remarks

TOC

The security of Kerberos 5 depends absolutely on the confidentiality and integrity of the keys stored in the KDC. Implementations of this standard MUST facilitate, to the extent possible, an administrator's ability to place more restrictive access controls on KeySets than on other principal data, and to arrange for more secure backup for KeySets.

4.3. Key

TOC

Implementations of this model MUST NOT REQUIRE keys to be represented.

4.3.1. Key: Attributes

TOC

4.3.1.1. keyEncryptionType

TOC

The enctype SHOULD be represented as an enumeration of the enctypes supported by the KDC using the string name ("encryption type") of the enctype from the IANA registry of Kerberos Encryption Type Numbers.

4.3.1.2. keyValue

TOC

The binary representation of the key data. This MUST be a single-valued octet string.

4.3.1.3. keySaltValue

TOC

The binary representation of the key salt. This MUST be a single-valued octet string.

4.3.1.4. keyStringToKeyParameter

TOC

This MUST be a single-valued octet string representing an opaque parameter associated with the enctype.

4.3.1.5. keyNotUsedBefore

TOC

This key MUST NOT be used before this date. The syntax of the attribute MUST be semantically equivalent with the standard ISO date format. This MUST be a single-valued attribute.

4.3.1.6. keyNotUsedAfter

TOC

This key MUST NOT be used after this date. The syntax of the attribute MUST be semantically equivalent with the standard ISO date format. This MUST be a single-valued attribute.

4.3.1.7. keyIsDisabled

TOC

This is a boolean attribute which SHOULD be set to false by default. If this attribute is true the key MUST NOT be used. This is used to temporarily disable a key.

4.3.2. Key: Associations

TOC

None

4.3.3. Key: Remarks

TOC

The security of the keys is an absolute requirement for the operation of Kerberos 5. If keys are implemented adequate protection from unauthorized modification and disclosure MUST be available and REQUIRED by the implementation.

4.4. Policy

TOC

Implementations SHOULD implement policy but MAY allow them to be OPTIONAL. The Policy should be thought of as a 'typed hole'. i.e. an opaque binary value paired with an identifier of type of data contained in the binary value. Both attributes (type and value) must be present.

4.4.1. Policy: Attributes

TOC

4.4.1.1. policyIdentifier

TOC

The policyIdentifier MUST be unique within the local administrative context and MUST be globally unique. Possible types of identifiers include:

> An Object Identifier (OID)
>
> A URI
>
> A UUID

The use of OIDs is RECOMMENDED for this purpose.

TOC

4.4.1.2. policyIsCritical

This boolean attribute indicates that the KDC MUST be able to correctly interpret and apply this policy for the key to be used.

4.4.1.3. policyContent

TOC

This is an optional single opaque binary value used to store a representation of the policy. In general a policy cannot be fully expressed using attribute-value pairs. The policyContent is OPTIONAL in the sense that an implementation MAY use it to store an opaque value for those policy-types which are not directly representable in that implementation.

4.4.1.4. policyUse

TOC

This is an optional single enumerated string value used to describe the use of the policy. Implementations SHOULD provide this attribute and MUST (if the attribute is implemented) describe the enumerated set of possible values. The intent is that this attribute be useful in providing an initial context-based filtering.

4.4.2. Mandatory-to-implement Policy

TOC

All implementations MUST be able to represent the policies listed in this section. Implementations are not required to use the same underlying data-representation for the policyContent binary value but SHOULD use the same OIDs as the policyIdentifier. In general the expression of policy may require a Turing-complete language. This specification does not attempt to model policy expression language.

4.4.2.1. Password Quality Policy

TOC

Password quality policy controls the requirements placed by the KDC on new passwords. This policy SHOULD be identified by the OID <TBD>.1.

TOC

4.4.2.2. Password Management Policy

Password management policy controls how passwords are changed. This policy SHOULD be identified by the OID <TBD>.2.

4.4.2.3. Keying Policy

TOC

A keying policy specifies the association of enctypes with new principals, e.g. when a principal is created one of the applicable keying policies is used to determine the set of keys to associate with the principal. This policy SHOULD be identified by the OID <TBD>.3.

4.4.2.4. Ticket Flag Policy

TOC

A ticket flag policy specifies the ticket flags allowed for tickets issued for a principal. This policy SHOULD be identified by the OID <TBD>.4.

---

5. Implementation Scenarios

TOC

There are several ways to implement an administrative service for Kerberos 5 based on this information model. In this section we list a few of them.

5.1. LDAP backend to KDC

TOC

Given an LDAP schema implementation of this information model it would be possible to build an administrative service by back-ending the KDC to a directory server where principals and keys are stored. Using the security mechanisms available on the directory server keys are protected from access by anyone apart from the KDC. Administration of the principals, policy, and other non-key data is done through the directory server while the keys are modified using the set/change password protocol [I-D.ietf-krb-wg-kerberos-set-passwd] (Williams, N., “Kerberos Set/Change Key/Password Protocol Version 2,” November 2008.).

TOC

5.2. LDAP frontend to KDC

An alternative way to provide a directory interface to the KDC is to implement an LDAP-frontend to the KDC which exposes all non-key objects as entries and attributes. As in the example above all keys are modified using the set/change password protocol [I-D.ietf-krb-wg-kerberos-set-passwd] (Williams, N., “Kerberos Set/Change Key/Password Protocol Version 2,” November 2008.). In this scenario the implementation would typically not use a traditional LDAP implementation but treat LDAP as an access protocol to data in the native KDC database.

5.3. SOAP

TOC

Given an XML schema implementation of this information model it would be possible to build a SOAP interface to the KDC. This demonstrates the value of creating an abstract information model which is mappable to multiple schema representations.

5.4. Netconf

TOC

Given a YAML implementation of this information model it would be possible to create a Netconf-based interface to the KDC, enabling management of the KDC from standard network management applications.

---

6. Security Considerations

TOC

This document describes an abstract information model for Kerberos 5. The Kerberos 5 protocol depends on the security of the keys stored in the KDC. The model described here assumes that keys MUST NOT be transported in the clear over the network and furthermore that keys are treated as write-only attributes that SHALL only be modified (using the administrative interface) by the change-password protocol [I-D.ietf-krb-wg-kerberos-set-passwd] (Williams, N., “Kerberos Set/Change Key/Password Protocol Version 2,” November 2008.).
Exposing the object model of a KDC typically implies that objects can be modified and/or deleted. In a KDC not all principals are created equal, so that for instance deleting krbtgt/EXAMPLE.COM@EXAMPLE.COM effectively disables the EXAMPLE.COM realm. Hence access control is paramount to the security of any implementation. This document does not mandate access control. This only implies that access control is beyond

the scope of the standard information model, i.e. that access control may not be accessible via any protocol based on this model. If access control objects are exposed via an extension to this model the presence of access control may in itself provide points of attack by giving away information about principals with elevated rights etc.

7. IANA Considerations

TOC

This document requires the allocation of several OIDs marked <TBD> in section 4.4.2 above. IANA should allocate a new arc under 1.3.6.1.5.2.5 (iso.org.dod.internet.security.kerberosV5.policies) named "kdcPolicy" and assign each of the policy OIDs a new number under this arc.

8. Acknowledgments

TOC

The author wishes to extend his thanks to Love Hörnquist-Åstrand <lha@kth.se> and Sam Hartman <hartmans@mit.edu> for their important contributions to this document.

9. References

TOC

9.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3961]	Raeburn, K., “Encryption and Checksum Specifications for Kerberos 5,” RFC 3961, February 2005 (TXT).
[RFC4120]	Neuman, C., Yu, T., Hartman, S., and K. Raeburn, “The Kerberos Network Authentication Service (V5),” RFC 4120, July 2005 (TXT).

9.2. Informative References

TOC

[I-D.ietf-krb-wg-kerberos-set-passwd]	Williams, N., “Kerberos Set/Change Key/Password Protocol Version 2,” draft-ietf-krb-wg-kerberos-set-passwd-08 (work in progress), November 2008 (TXT).

Author's Address

TOC

	Leif Johansson
	Swedish University Network
	Thulegatan 11
	Stockholm
Email:	leifj@sunet.se
URI:	http://www.sunet.se