NETWORK WORKING GROUP
Internet-Draft
Updates: 4120 (if approved)
Intended status: Standards Track
Expires: March 14, 2009

L. Zhu
P. Leach
Microsoft Corporation

September 10, 2008

Anonymity Support for Kerberos
draft-ietf-krb-wg-anon-09

Status of this Memo

Abstract

This document defines extensions to the Kerberos protocol for the Kerberos client to authenticate the Kerberos Key Distribution Center (KDC) and the Kerberos server, without revealing the client's identity or the client's realm to the server or to the KDC. It updates RFC 4120. These extensions can be used to secure communication between the anonymous client and the server.

Table of Contents

1. Introduction

In certain situations, the Kerberos [RFC4120] client may wish to authenticate a server and/or protect communications without revealing the client's own identity. For example, consider an application which provides read access to a research database, and which permits queries by arbitrary requestors. A client of such a service might wish to authenticate the service, to establish trust in the information received from it, but might not wish to disclose the client's identity to the service for privacy reasons.

Extensions to Kerberos are specified in this document by which a client can authenticate the Key Distribution Center (KDC) and request an anonymous ticket. The client can use the anonymous ticket to authenticate the server and protect subsequent client-server communications.

By using the extensions defined in this specification, the client can request an anonymous ticket where the client may reveal the client's identity to the client's own KDC, or the client can hide the client's identity completely by using anonymous Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) as defined in Section 4.1. Using the returned anonymous ticket, the client remains anonymous in subsequent Kerberos exchanges thereafter to KDCs on the cross-realm authentication path, and to the server with which it communicates.

In this specification, the client realm in the anonymous ticket is the anonymous realm name when anonymous PKINIT is used to obtain the ticket. The client realm is the client's real realm name if the client is authenticated using the client's long term keys. Note that the membership of a realm can imply a member of the community represented by the realm.

The interaction with Generic Security Service Application Program Interface (GSS-API) is described after the protocol description.

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 [RFC2119].

3. Definitions

The anonymous Kerberos realm name is defined as a well-known realm

name based on [KRBNAM], and the value of this well-known realm name is the literal "WELLKNOWN:ANONYMOUS".

The anonymous Kerberos principal name is defined as a well-known Kerberos principal name based on [KRBNAM]. The value of the name-type field is KRB_NT_WELLKNOWN [KRBNAM], and the value of the name-string field is a sequence of two KerberosString components: "WELLKNOWN", "ANONYMOUS".

The anonymous ticket flag is defined as bit 14 (with the first bit being bit 0) in the TicketFlags:

```
TicketFlags     ::= KerberosFlags
  -- anonymous(14)
  -- TicketFlags and KerberosFlags are defined in [RFC4120]
```

This is a new ticket flag that is used to indicate a ticket is an anonymous one.

An anonymous ticket is a ticket that has all of the following properties:

- The cname field contains the anonymous Kerberos principal name.
- The crealm field contains the client's realm name or the anonymous realm name.
- The anonymous ticket contains no information that can reveal the client's identity. However the ticket may contain the client realm, intermediate realms on the client's authentication path, and authorization data that may provide information related to the client's identity. For example, an anonymous principal that is identifiable only within a particular group of users can be implemented using authorization data and such authorization data, if included in the anonymous ticket, would disclose the client's membership of that group.
- The anonymous ticket flag is set.

The anonymous KDC option is defined as bit 14 (with the first bit being bit 0) in the KDCOptions:

```
KDCOptions      ::= KerberosFlags
  -- anonymous(14)
  -- KDCOptions and KerberosFlags are defined in [RFC4120]
```

As described in Section 4, the anonymous KDC option is set to request an anonymous ticket in an Authentication Service (AS) request or an

Ticket Granting Service (TGS) request.

4. Protocol Description

In order to request an anonymous ticket, the client sets the anonymous KDC option in an AS request or an TGS request.

The rest of this section is organized as follows: it first describes protocol actions specific to AS exchanges, then it describes those of TGS exchange. These are then followed by the decription of protocol actions common to both AS and TGS and those in subsequent exchanges.

4.1. Anonymity Support in AS Exchange

The client requests an anonymous ticket by setting the anonymous KDC option in an AS exchange.

The Kerberos client can use the client's long term keys, or the client's X.509 certificates [RFC4556], or any other preauthenication data, to authenticate to the KDC and requests an anonymous ticket in an AS exchange where the client's identity is known to the KDC.

If the client in the AS request is anonymous, the anonymous KDC option MUST be set in the request. Otherwise, the KDC MUST return a KRB-ERROR message with the code KDC_ERR_BADOPTION.

If the client is anonymous and the KDC does not have a key to encrypt the reply (this can happen when, for example, the KDC does not support PKINIT [RFC4556]), the KDC MUST return an error message with the code KDC_ERR_NULL_KEY [RFC4120].

When policy allows, the KDC issues an anonymous ticket. If the client name in the request is the anonymous principal, the client realm (crealm) in the reply is the anonymous realm, otherwise the client realm is the realm of the AS. According to [RFC4120] the client name and the client realm in the EncTicketPart of the reply MUST match with the corresponding client name and the client realm of the anonymous ticket in the reply; the client MUST use the client name and the client realm returned in the KDC-REP in subsequent message exchanges when using the obtained anonymous ticket.

Care MUST be taken by the KDC not to reveal the client's identity in the authorization data of the returned ticket when populating the authorization data in a returned anonymous ticket.

The AD-INITIAL-VERIFIED-CAS authorization data as defined in [RFC4556] contains the issuer name of the client certificate. This

authorization is not applicable and MUST NOT be present in the returned anonymous ticket when anonymous PKINIT is used. When the client is authenticated (i.e. anonymous PKINIT is not used), if it is undesirable to disclose such information about the client's identity, the AD-INITIAL-VERIFIED-CAS authorization data SHOULD be removed from the returned anonymous ticket.

The client can use the client keys to mutually authenticate with the KDC, request an anonymous TGT in the AS request. And in that case, the reply key is selected as normal according to Section 3.1.3 of [RFC4120].

4.1.1. Anonymous PKINIT

This sub-section defines anonymity PKINIT.

As described earlier in this section, the client can request an anonymous ticket by authenticating to the KDC using the client's identity; alternatively without revealing the client's identity to the KDC, the Kerberos client can request an anonymous ticket as follows: the client sets the client name as the anonymous principal in the AS exchange and provides a PA_PK_AS_REQ pre-authentication data [RFC4556] where both the signerInfos field and the certificates field of the SignedData [RFC3852] of the PA_PK_AS_REQ are empty. Because the anonymous client does not have an associated asymmetric key pair, the client MUST choose the Diffie-Hellman key agreement method by filling in the Diffie-Hellman domain parameters in the clientPublicValue [RFC4556]. This use of the anonymous client name in conjunction with PKINIT is referred to as anonymous PKINIT. If anonymous PKINIT is used, the realm name in the returned anonymous ticket MUST be the anonymous realm.

Upon receiving the anonymous PKINIT request from the client, the KDC processes the request according to Section 3.1.2 of [RFC4120]. The KDC skips the checks for the client's signature and the client's public key (such as the verification of the binding between the client's public key and the client name), but performs otherwise-applicable checks, and proceeds as normal according to [RFC4556]. For example, the AS MUST check if the client's Diffie-Hellman domain parameters are acceptable. The Diffie-Hellman key agreement method MUST be used and the reply key is derived according to Section 3.2.3.1 of [RFC4556]. If the clientPublicValue is not present in the request, the KDC MUST return a KRB-ERROR with the code KDC_ERR_PUBLIC_KEY_ENCRYPTION_NOT_SUPPORTED [RFC4556]. If all goes well, an anonymous ticket is generated according to Section 3.1.3 of [RFC4120] and a PA_PK_AS_REP [RFC4556] pre-authentication data is included in the KDC reply according to [RFC4556]. If the KDC does not have an asymmetric key pair, it MAY reply anonymously or reject

the authentication attempt. If the KDC replies anonymously, both the signerInfos field and the certificates field of the SignedData [RFC3852] of PA_PK_AS_REP in the reply are empty. The server name in the anonymous KDC reply contains the name of the TGS.

Upon receipt of the KDC reply that contains an anonymous ticket and a PA_PK_AS_REP [RFC4556] pre-authentication data, the client can then authenticate the KDC based on the KDC's signature in the PA_PK_AS_REP. If the KDC's signature is missing in the KDC reply (the reply is anonymous), the client MUST reject the returned ticket if it cannot authenticate the KDC otherwise.

A KDC that supports anonymous PKINIT MUST indicate the support of PKINIT according to Section 3.4 of [RFC4556].

Note that in order to obtain an anonymous ticket with the anonymous realm name, the client MUST set the client name as the anonymous principal in the request when requesting an anonymous ticket in an AS exchange. Anonymity PKINIT is the only way via which an anonymous ticket with the anonymous realm as the client realm can be generated in this specification.

4.2. Anonymity Support in TGS Exchange

The client requests an anonymous ticket by setting the anonymous KDC option in a TGS exchange, and in that request the client can use a normal Ticket Granting Ticket (TGT) with the client's identity, or an anonymous TGT, or an anonymous cross realm TGT. If the client uses a normal TGT, the client's identity is known to the TGS.

Note that the client can completely hide the client's identity in an AS exchange using anonymous PKINIT as described in the previous section.

If the ticket in the PA-TGS-REQ of the TGS request is an anonymous one, the anonymous KDC option MUST be set in the request. Otherwise, the KDC MUST return a KRB-ERROR message with the code KDC_ERR_BADOPTION.

When policy allows, the KDC issues an anonymous ticket. If the ticket in the TGS request is an anonymous one, the client name and the client realm are copied from that ticket; otherwise the ticket in the TGS request is a normal ticket, the returned anonymous ticket contains the client name as the anonymous principal and the client realm as the true realm of the client. In all cases, according to [RFC4120] the client name and the client realm in the EncTicketPart of the reply MUST match with the corresponding client name and the client realm of the anonymous ticket in the reply; the client MUST

use the client name and the client realm returned in the KDC-REP in subsequent message exchanges when using the obtained anonymous ticket.

Care MUST be taken by the TGS not to reveal the client's identity in the authorization data of the returned ticket. When propagating authorization data in the ticket or in the enc-authorization-data field of the request, the TGS MUST ensure that the client confidentiality is not violated in the returned anonymous ticket. The TGS MUST process the authorization data recursively according to Section 5.2.6 of [RFC4120] beyond the container levels such that all embedded authorization elements are interpreted. The TGS SHOULD NOT populate identity-based authorization data into an anonymous ticket in that such authorization data typically reveals the client's identity. The specification of a new authorization data type MUST specify the processing rules of the authorization data when an anonymous ticket is returned. If there is no processing rule defined for an authorization data element or the authorization data element is unknown, the TGS MUST process it when an anonymous ticket is returned as follows:

- If the authorization data element may reveal the client's identity, it MUST be removed unless otherwise specified.

- If the authorization data element, that could reveal's the client's identity. is intended to restrict the use of the ticket or limit the rights otherwise conveyed in the ticket, it cannot be removed in order to hide the client's identity. In this case, the authentication attempt MUST be rejected, and the TGS MUST return an error message with the code KDC_ERR_POLICY. Note this is applicable to both critical and optional authorization data.

- If the authorization data element is unknown, the TGS MAY remove it, or transfer it into the returned anonymous ticket, or reject the authentication attempt, based on local policy for that authorization data type unless otherwise specified. If there is no policy defined for a given unknown authorization data type, the authentication MUST be rejected. The error code is KDC_ERR_POLICY when the authentication is rejected.

The AD-INITIAL-VERIFIED-CAS authorization data as defined in [RFC4556] contains the issuer name of the client certificate. If it is undesirable to disclose such information about the client's identity, the AD-INITIAL-VERIFIED-CAS authorization data SHOULD be removed from an anonymous ticket.

The TGS encodes the name of the previous realm into the transited field according to Section 3.3.3.2 of [RFC4120]. Based on local

policy, the TGS MAY omit the previous realm if the cross realm TGT is an anonymous one in order to hide the authentication path of the client. The unordered set of realms in the transited field, if present, can reveal which realm may potentially be the realm of the client or the realm that issued the anonymous TGT. The anonymous Kerberos realm name MUST NOT be present in the transited field of a ticket. The true name of the realm that issued the anonymous ticket MAY be present in the transited field of a ticket.

4.3. Subsequent Exchanges and Protocol Actions Common to AS and TGS for Anonymity Support

In both AS and TGS exchanges, the realm field in the KDC request is always the realm of the target KDC, not the anonymous realm when the client requests an anonymous ticket.

Absent other information the KDC MUST NOT include any identifier in the returned anonymous ticket that could reveal the client's identity to the server.

Unless anonymous PKINIT is used, if a client requires anonymous communication then the client MUST check to make sure that the ticket in the reply is actually anonymous by checking the presence of the anonymous ticket flag in the flags field of the EncKDCRepPart. This is because KDCs ignore unknown KDC options. A KDC that does not understand the anonymous KDC option will not return an error, but will instead return a normal ticket.

The subsequent client and server communications then proceed as described in [RFC4120].

Note that the anonymous principal name and realm are only applicable to the client in Kerberos messages, the server cannot be anonymous in any Kerberos message per this specification.

A server accepting an anonymous service ticket may assume that subsequent requests using the same ticket originate from the same client. Requests with different tickets are likely to originate from different clients.

Upon receipt of an anonymous ticket, the transited policy check is preformed in the same way as that of a normal ticket if the client's realm is not the anonymous realm; if the client realm is the anonymous realm, absent other information any realm in the authentication path is allowed by the cross-realm policy check.

5. Interoperability Requirements

Conforming implementations MUST support the anonymous principal with a non-anonymous realm, and they MAY support the anonymous principal with the anonymous realm using anonymous PKINIT.

6. GSS-API Implementation Notes

GSS-API defines the name_type GSS_C_NT_ANONYMOUS [RFC2743] to represent the anonymous identity. In addition, Section 2.1.1 of [RFC1964] defines the single string representation of a Kerberos principal name with the name_type GSS_KRB5_NT_PRINCIPAL_NAME. The anonymous principal with the anonymous realm corresponds to the GSS-API anonymous principal. A principal with the anonymous principal name and a non-anonymous realm is an authenticated principal, hence such a principal does not correspond to the anonymous principal in GSS-API with the GSS_C_NT_ANONYMOUS name type. The [RFC1964] name syntax for GSS_KRB5_NT_PRINCIPAL_NAME MUST be used for importing the anonymous principal name with a non-anonymous realm name and for displaying and exporting these names.

At the GSS-API [RFC2743] level, an initiator/client requests the use of an anonymous principal with the anonymous realm by asserting the "anonymous" flag when calling GSS_Init_Sec_Context(). The GSS-API implementation MAY provide implementation-specific means for requesting the use of an anonymous principal with a non-anonymous realm.

GSS-API does not know or define "anonymous credentials", so the (printable) name of the anonymous principal will rarely be used by or relevant for the initiator/client. The printable name is relevant for the acceptor/server when performing an authorization decision based on the initiator name that is returned from the acceptor side upon the successful security context establishment.

A GSS-API initiator MUST carefully check the resulting context attributes from the initial call to GSS_Init_Sec_Context() when requesting anonymity, because (as in the GSS-API tradition and for backwards compatibility) anonymity is just another optional context attribute. It could be that the mechanism doesn't recognize the attribute at all or that anonymity is not available for some other reasons -- and in that case the initiator MUST NOT send the initial security context token to the acceptor, because it will likely reveal the initiators identity to the acceptor, something that can rarely be "un-done".

Portable initiators are RECOMMENDED to use default credentials

whenever possible, and request anonymity only through the input anon_req_flag [RFC2743] to GSS_Init_Sec_Context().

7. PKINIT Client Contribution to the Ticket Session Key

The definition in this section was motivated by protocol analysis of anonymous PKINIT (defined in this document) in building tunneling channels [FAST] and subsequent channel bindings. In order to enable applications of anonymous PKINIT to form channels, all implementations of anonymous PKINIT need to meet the requirements of this section. There is otherwise no connection to the rest of this document.

PKINIT is useful for constructing tunneling channels. To ensure that an attacker cannot create a channel with a given name, it is desirable that neither the KDC nor the client can unilaterally determine the ticket session key. To achieve that end, a KDC conforming to this definition MUST encrypt a randomly generated key, called the KDC contribution key, in the PA_PKINIT_KX padata (defined next in this section). The KDC contribution key is then combined with the reply key to form the ticket session key of the returned ticket. These two keys are then combined using the KRB-FX-CF2 operation defined in Section 7.1, where K1 is the KDC contribution key, K2 is the reply key, the input pepper1 is American Standard Code for Information Interchange (ASCII) [ASAX34] string "PKINIT", and the input pepper2 is ASCII string "KeyExchange".

```
PA_PKINIT_KX      135
  -- padata for PKINIT that contains an encrypted
  -- KDC contribution key.

PA-PKINIT-KX  ::= EncryptedData -- EncryptionKey
  -- Contains an encrypted key randomly
  -- generated by the KDC (known as the KDC contribution key).
  -- Both EncryptedData and EncryptionKey are defined in [RFC4120]
```

The PA_PKINIT_KX padata MUST be included in the KDC reply when anonymous PKINIT is used; it SHOULD be included if PKINIT is used with the Diffie-Helleman key exchange but the client is not anonymous; it MUST NOT be included otherwise (e.g. when PKINIT is used with the public key encryption as the key exchange).

The padata-value field of the PA-PKINIT-KX type padata contains the DER [X680] [X690] encoding of the Abstract Syntax Notation One (ASN.1) type PA-PKINIT-KX. The PA-PKINIT-KX structure is a EncryptedData. The clear text data being encrypted is the DER encoded Kerberos session key randomly generated by the KDC. The

encryption key is the reply key and the key usage number is KEY_USAGE_PA_PKINIT_KX (44).

The client then decrypts the KDC contribution key and verifies the ticket session key in the returned ticket is the combined key of the KDC contribution key and the reply key as described above. A conforming client MUST reject anonymous PKINIT authentication if the PA_PKINIT_KX padata is not present in the KDC reply or if the ticket session key of the returned ticket is not the combined key of the KDC contribution key and the reply key when PA-PKINIT-KX is present in the KDC reply.

7.1. Combinging Two protocol Keys

KRB-FX-CF2() combines two protocol keys based on the pseudo-random() function defined in [RFC3961].

Given two input keys, K1 and K2, where K1 and K2 can be of two different enctypes, the output key of KRB-FX-CF2(), K3, is derived as follows:

```
 KRB-FX-CF2(protocol key, protocol key, octet string,
           octet string)  ->  (protocol key)

 PRF+(K1, pepper1) -> octet-string-1
 PRF+(K2, pepper2) -> octet-string-2
 KRB-FX-CF2(K1, K2, pepper1, pepper2) ->
        random-to-key(octet-string-1 ^ octet-string-2)
```

Where ^ denotes the exclusive-OR operation. PRF+() is defined as follows:

```
PRF+(protocol key, octet string) -> (octet string)

PRF+(key, shared-info) -> pseudo-random( key,  1 || shared-info ) ||
             pseudo-random( key, 2 || shared-info ) ||
             pseudo-random( key, 3 || shared-info ) || ...
```

Here the counter value 1, 2, 3 and so on are encoded as a one-octet integer. The pseudo-random() operation is specified by the enctype of the protocol key. PRF+() uses the counter to generate enough bits as needed by the random-to-key() [RFC3961] function for the encryption type specified for the resulting key; unneeded bits are removed from the tail.

8. Security Considerations

Since KDCs ignore unknown options, a client requiring anonymous communication needs to make sure that the returned ticket is actually anonymous. This is because a KDC that that does not understand the anonymous option would not return an anonymous ticket.

By using the mechanism defined in this specification, the client does not reveal the client's identity to the server but the client identity may be revealed to the KDC of the server principal (when the server principal is in a different realm than that of the client), and any KDC on the cross-realm authentication path. The Kerberos client MUST verify the ticket being used is indeed anonymous before communicating with the server, otherwise the client's identity may be revealed unintentionally.

In cases where specific server principals must not have access to the client's identity (for example, an anonymous poll service), the KDC can define server principal specific policy that insure any normal service ticket can NEVER be issued to any of these server principals.

If the KDC that issued an anonymous ticket were to maintain records of the association of identities to an anonymous ticket, then someone obtaining such records could breach the anonymity. Additionally, the implementations of most (for now all) KDC's respond to requests at the time that they are received. Traffic analysis on the connection to the KDC will allow an attacker to match client identities to anonymous tickets issued. Because there are plaintext parts of the tickets that are exposed on the wire, such matching by a third party observer is relatively straightforward. A service that is authenticated by the anonymous principals may be able to infer the identity of the client by examining and linking quasi-static protocol information such as the IP address from which a request is received.

The client's real identity is not revealed when the client is authenticated as the anonymous principal. Application servers MAY reject the authentication in order to, for example, prevent information disclosure or as part of Denial of Service (DOS) prevention. Application servers MUST avoid accepting anonymous credentials in situations where they must record the client's identity; for example, when there must be an audit trail.

9. Acknowledgements

JK Jaganathan helped editing early revisions of this document.

Clifford Neuman contributed the core notions of this document.

Ken Raeburn reviewed the document and provided suggestions for improvements.

Martin Rex wrote the text for GSS-API considerations.

Nicolas Williams reviewed the GSS-API considerations section and suggested ideas for improvements.

Sam Hartman and Nicolas Williams were great champions of this work.

Miguel Garcia and Phillip Hallam-Baker reviewed the document and provided helpful suggestions.

In addition, the following individuals made significant contributions: Jeffrey Altman, Tom Yu, Chaskiel M Grundman, Love Hornquist Astrand, Jeffrey Hutzelman, and Olga Kornievskaia.

10. IANA Considerations

This document defines a new 'anonymous' Kerberos well-known name and a new 'anonymous' Kerberos well-known realm based on [KRBNAM]. IANA is requested to add these two values to the Kerberos naming registries that are created in [KRBNAM].

11. References

11.1. Normative References

[ASAX34] American Standard Code for Information Interchange, ASA X3.4-1963, American Standards Association, June 17, 1963.

[KRBNAM] Zhu, L., "Additional Kerberos Naming Constraints", draft-ietf-krb-wg-naming (work in progress), 2008.

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

[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.

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004.

[RFC3961] Raeburn, K., "Encryption and Checksum Specifications for Kerberos 5", RFC 3961, February 2005.

[RFC4120] Neuman, C., Yu, T., Hartman, S., and K. Raeburn, "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005.

[RFC4556] Zhu, L. and B. Tung, "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)", RFC 4556, June 2006.

[X680] ITU-T Recommendation X.680 (2002) | ISO/IEC 8824-1:2002, Information technology - Abstract Syntax Notation One (ASN.1): Specification of basic notation.

[X690] ITU-T Recommendation X.690 (2002) | ISO/IEC 8825-1:2002, Information technology - ASN.1 encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).

11.2. Informative References

[FAST] Zhu, L. and S. Hartman, "A Generalized Framework for Kerberos Pre-Authentication", draft-ietf-krb-wg-preauth-framework (work in progress), 2008.

Authors' Addresses

Larry Zhu
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Email: lzhu@microsoft.com

Paul Leach
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

Email: paulle@microsoft.com

Full Copyright Statement

Intellectual Property