[MS-PKCA-Diff]:

Public Key Cryptography for Initial Authentication (PKINIT) in Kerberos Protocol

---

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation ("this documentation") for protocols, file formats, data portability, computer languages, and standards support. Additionally, overview documents cover inter-protocol relationships and interactions.
- **Copyrights**. This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you can make copies of it in order to develop implementations of the technologies that are described in this documentation and can distribute portions of it in your implementations that use these technologies or in your documentation as necessary to properly document the implementation. You can also distribute in your implementation, with or without modification, any schemas, IDLs, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications documentation.
- **No Trade Secrets**. Microsoft does not claim any trade secret rights in this documentation.
- **Patents**. Microsoft has patents that might cover your implementations of the technologies described in the Open Specifications documentation. Neither this notice nor Microsoft's delivery of this documentation grants any licenses under those patents or any other Microsoft patents. However, a given Open Specifications document might be covered by the Microsoft Open Specifications Promise or the Microsoft Community Promise. If you would prefer a written license, or if the technologies described in this documentation are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **License Programs**. To see all of the protocols in scope under a specific license program and the associated patents, visit the Patent Map.
- **Trademarks**. The names of companies and products contained in this documentation might be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights. For a list of Microsoft trademarks, visit www.microsoft.com/trademarks.
- **Fictitious Names**. The example companies, organizations, products, domain names, email addresses, logos, people, places, and events that are depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than as specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications documentation does not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments, you are free to take advantage of them. Certain Open Specifications documents are intended for use in conjunction with publicly available standards specifications and network programming art and, as such, assume that the reader either is familiar with the aforementioned material or has immediate access to it.

Support. For questions and support, please contact dochelp@microsoft.com.

Revision Summary

Date	Revision History	Revision Class	Comments
3/2/2007	1.0	New	Version 1.0 release
4/3/2007	1.1	Minor	Version 1.1 release
5/11/2007	1.2	Minor	Version 1.2 release
6/1/2007	1.2.1	Editorial	Changed language and formatting in the technical content.
7/3/2007	1.2.2	Editorial	Changed language and formatting in the technical content.
8/10/2007	1.2.3	Editorial	Changed language and formatting in the technical content.
9/28/2007	1.2.4	Editorial	Changed language and formatting in the technical content.
10/23/2007	2.0	Major	Converted document to unified format.
1/25/2008	2.1	Minor	Clarified the meaning of the technical content.
3/14/2008	2.1.1	Editorial	Changed language and formatting in the technical content.
6/20/2008	2.1.2	Editorial	Changed language and formatting in the technical content.
7/25/2008	2.1.3	Editorial	Changed language and formatting in the technical content.
8/29/2008	2.1.4	Editorial	Changed language and formatting in the technical content.
10/24/2008	2.1.5	Editorial	Changed language and formatting in the technical content.
12/5/2008	2.2	Minor	Clarified the meaning of the technical content.
1/16/2009	2.2.1	Editorial	Changed language and formatting in the technical content.
2/27/2009	2.2.2	Editorial	Changed language and formatting in the technical content.
4/10/2009	2.2.3	Editorial	Changed language and formatting in the technical content.
5/22/2009	2.2.4	Editorial	Changed language and formatting in the technical content.
7/2/2009	2.3	Minor	Clarified the meaning of the technical content.
8/14/2009	2.4	Minor	Clarified the meaning of the technical content.
9/25/2009	2.5	Minor	Clarified the meaning of the technical content.
11/6/2009	3.0	Major	Updated and revised the technical content.
12/18/2009	3.1	Minor	Clarified the meaning of the technical content.
1/29/2010	3.2	Minor	Clarified the meaning of the technical content.
3/12/2010	3.3	Minor	Clarified the meaning of the technical content.
4/23/2010	4.0	Major	Updated and revised the technical content.
6/4/2010	5.0	Major	Updated and revised the technical content.
7/16/2010	5.1	Minor	Clarified the meaning of the technical content.
8/27/2010	6.0	Major	Updated and revised the technical content.

Date	Revision History	Revision Class	Comments
10/8/2010	6.0	None	No changes to the meaning, language, or formatting of the technical content.
11/19/2010	6.0	None	No changes to the meaning, language, or formatting of the technical content.
1/7/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
2/11/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
3/25/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
5/6/2011	6.0	None	No changes to the meaning, language, or formatting of the technical content.
6/17/2011	6.1	Minor	Clarified the meaning of the technical content.
9/23/2011	6.1	None	No changes to the meaning, language, or formatting of the technical content.
12/16/2011	7.0	Major	Updated and revised the technical content.
3/30/2012	7.0	None	No changes to the meaning, language, or formatting of the technical content.
7/12/2012	7.1	Minor	Clarified the meaning of the technical content.
10/25/2012	7.1	None	No changes to the meaning, language, or formatting of the technical content.
1/31/2013	7.1	None	No changes to the meaning, language, or formatting of the technical content.
8/8/2013	8.0	Major	Updated and revised the technical content.
11/14/2013	8.0	None	No changes to the meaning, language, or formatting of the technical content.
2/13/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
5/15/2014	8.0	None	No changes to the meaning, language, or formatting of the technical content.
6/30/2015	9.0	Major	Significantly changed the technical content.
10/16/2015	9.0	None	No changes to the meaning, language, or formatting of the technical content.
7/14/2016	9.0	None	No changes to the meaning, language, or formatting of the technical content.
6/1/2017	10.0	Major	Significantly changed the technical content.
9/15/2017	11.0	Major	Significantly changed the technical content.
9/12/2018	12.0	Major	Significantly changed the technical content.
4/7/2021	13.0	Major	Significantly changed the technical content.

Table of Contents

1 Introduction

The Public Key Cryptography for Initial Authentication in Kerberos (PKINIT) protocol [RFC4556] enables the use of public key cryptography in the initial authentication exchange (that is, in the Authentication Service (AS) exchange) of the Kerberos protocol [MS-KILE]. This specification describes the Public Key Cryptography for Initial Authentication in Kerberos (PKINIT): Microsoft Extensions protocol (PKCA) and how the protocol differs from what is specified in [RFC4556].

In an implementation of [RFC4120] or KILE, the security of the AS exchange depends on the strength of the password used to protect it. This also affects the security of subsequent protocol requests.

By using public key cryptography to protect the initial authentication, the Kerberos protocol [MS-KILE] is substantially strengthened and can be used with already existing public key authentication mechanisms such as smart cards.

This document references the PKINIT methods and data formats [RFC4556] and [RFC5349], that the client and the KDC can use both to mutually authenticate during the AS exchange with public and private key pairs and to negotiate the AS-REP key, which allows the KDC to encrypt the AS-REP key sent to the client.

Sections 1.5, 1.8, 1.9, 2, and 3 of this specification are normative. All other sections and examples in this specification are informative.

1.1 Glossary

This document uses the following terms:

Active Directory: The Windows implementation of a general-purpose directory service, which uses LDAP as its primary access protocol. Active Directory stores information about a variety of objects in the network such as user accounts, computer accounts, groups, and all related credential information used by Kerberos [MS-KILE]. Active Directory is either deployed as Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS), which are both described in [MS-ADOD]: Active Directory Protocols Overview.

Authentication Service (AS) exchange: The Kerberos subprotocol in which the Authentication Service (AS) component of the key distribution center (KDC) accepts an initial logon or authentication request from a client and provides the client with a ticket-granting ticket (TGT) and necessary cryptographic keys to make use of the ticket. This is specified in [RFC4120] section 3.1. The AS exchange is always initiated by the client, usually in response to the initial logon of a principal such as a user.

authorization data: An extensible field within a Kerberos ticket, used to pass authorization data about the principal on whose behalf the ticket was issued to the application service.

certification authority (CA): A third party that issues public key certificates. Certificates serve to bind public keys to a user identity. Each user and certification authority (CA) can decide whether to trust another user or CA for a specific purpose, and whether this trust should be transitive. For more information, see [RFC3280].

elliptic curve cryptography (ECC): A public-key cryptosystem that is based on high-order elliptic curves over finite fields. For more information, see [IEEE1363].

key: In cryptography, a generic term used to refer to cryptographic data that is used to initialize a cryptographic algorithm. Keys are also sometimes referred to as keying material.

Key Distribution Center (KDC): The Kerberos service that implements the authentication and ticket granting services specified in the Kerberos protocol. The service runs on computers selected by the administrator of the realm or domain; it is not present on every machine on the network. It must have access to an account database for the realm that it serves. KDCs are

integrated into the domain controller role. It is a network service that supplies tickets to clients for use in authenticating to services.

object identifier (OID): In the context of a directory service, a number identifying an object class or attribute. Object identifiers are issued by the ITU and form a hierarchy. An OID is represented as a dotted decimal string (for example, "1.2.3.4"). For more information on OIDs, see [X660] and [RFC3280] Appendix A. OIDs are used to uniquely identify certificate templates available to the certification authority (CA). Within a certificate, OIDs are used to identify standard extensions, as described in [RFC3280] section 4.2.1.x, as well as non-standard extensions.

one-way function (OWF): The calculation of a hash of the password using the Rivest-Shamir-Adleman (RSA) MD4 function. OWF is used to refer to the resulting value of the hash operation.

pre-authentication: In Kerberos, a state in which a key distribution center (KDC) demands that the requestor in the Authentication Service (AS) exchange demonstrate knowledge of the key associated with the account. If the requestor cannot demonstrate this knowledge, the KDC will not issue a ticket-granting ticket (TGT) ([RFC4120] sections 5.2.7 and 7.5.2).

privilege attribute certificate (PAC): A Microsoft-specific authorization data present in the authorization data field of a ticket. The PAC contains several logical components, including group membership data for authorization, alternate credentials for non-Kerberos authentication protocols, and policy control information for supporting interactive logon.

public key infrastructure (PKI): The laws, policies, standards, and software that regulate or manipulate certificates and public and private keys. In practice, it is a system of digital certificates, certificate authorities (CAs), and other registration authorities that verify and authenticate the validity of each party involved in an electronic transaction. For more information, see [X509] section 6.

realm: A collection of key distribution centers (KDCs) with a common set of principals, as described in [RFC4120] section 1.2.

service: A process or agent that is available on the network, offering resources or services for clients. Examples of services include file servers, web servers, and so on.

ticket: A record generated by the key distribution center (KDC) that helps a client authenticate to a service. It contains the client's identity, a unique cryptographic key for use with this ticket (the session key), a time stamp, and other information, all sealed using the service's secret key. It only serves to authenticate a client when presented along with a valid authenticator.

ticket-granting service (TGS): A service that issues tickets for admission to other services in its own domain or for admission to the ticket-granting service in another domain.

ticket-granting ticket (TGT): A special type of ticket that can be used to obtain other tickets. The TGT is obtained after the initial authentication in the Authentication Service (AS) exchange; thereafter, users do not need to present their credentials, but can use the TGT to obtain subsequent tickets.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as defined in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

Links to a document in the Microsoft Open Specifications library point to the correct section in the most recently published version of the referenced document. However, because individual documents in the library are not updated at the same time, the section numbers in the documents may not match. You can confirm the correct section numbering by checking the Errata.

1.2.1 (Updated Section) Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information.

[FIPS140] FIPS PUBS, "Security Requirements for Cryptographic Modules", FIPS PUB 140, December 2002, ~~http~~https://csrc.nist.gov/csrc/media/publications/fips/~~fips140-~~140/2/final/documents/fips1402.pdf

[ITUX680] ITU-T, "Abstract Syntax Notation One (ASN.1): Specification of Basic Notation", Recommendation X.680, July 2002, http://www.itu.int/ITU-T/studygroups/com17/languages/X.680-0207.pdf

[MS-ADA1] Microsoft Corporation, "Active Directory Schema Attributes A-L".

[MS-ADA2] Microsoft Corporation, "Active Directory Schema Attributes M".

[MS-ADA3] Microsoft Corporation, "Active Directory Schema Attributes N-Z".

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification".

[MS-KILE] Microsoft Corporation, "Kerberos Protocol Extensions".

[MS-NLMP] Microsoft Corporation, "NT LAN Manager (NTLM) Authentication Protocol".

[MS-PAC] Microsoft Corporation, "Privilege Attribute Certificate Data Structure".

[MS-SPNG] Microsoft Corporation, "Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) Extension".

[RFC1964] Linn, J., "The Kerberos Version 5 GSS-API Mechanism", RFC 1964, June 1996, http://www.rfc-editor.org/rfc/rfc1964.txt

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997, http://www.rfc-editor.org/rfc/rfc2119.txt

[RFC2315] Kaliski, B., "PKCS #7: Cryptographic Message Syntax Version 1.5", RFC 2315, March 1998, http://www.ietf.org/rfc/rfc2315.txt

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000, http://www.rfc-editor.org/rfc/rfc2743.txt

[RFC3370] Housley, R., "Cryptographic Message Syntax (CMS) Algorithms", RFC 3370, August 2002, http://www.ietf.org/rfc/rfc3370.txt

[RFC3852] Housley, R., "Cryptographic Message Syntax (CMS)", RFC 3852, July 2004, http://www.ietf.org/rfc/rfc3852.txt

[RFC4120] Neuman, C., Yu, T., Hartman, S., and Raeburn, K., "The Kerberos Network Authentication Service (V5)", RFC 4120, July 2005, https://www.rfc-editor.org/rfc/rfc4120.txt

[RFC4556] Zhu, L., and Tung, B., "Public Key Cryptography for Initial Authentication in Kerberos", RFC 4556, June 2006, http://www.ietf.org/rfc/rfc4556.txt

[RFC5349] Zhu, L., Jaganathan, K., and Lauter, K., "Elliptic Curve Cryptography (ECC) Support for Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)", RFC 5349, September 2008, http://www.ietf.org/rfc/rfc5349.txt

[RFC8070] Moore, S., Miller, P., and Short, M., Ed., "Public Key Cryptography for Initial Authentication in Kerberos (PKINIT)", https://tools.ietf.org/html/rfc8070

[X509] ITU-T, "Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks", Recommendation X.509, August 2005, http://www.itu.int/rec/T-REC-X.509/en

1.2.2 Informative References

None.

1.3 Overview

The PKINIT protocol is a security protocol that authenticates entities on a network using public key cryptography. Kerberos is a security protocol that mutually authenticates entities on a network and can provide user credential delegation after authentication is complete. Kerberos is specified in [RFC4120] and [MS-KILE], and PKINIT is specified in [RFC4556]. [RFC5349] specifies the use of elliptic curve cryptography (ECC) within the framework of PKINIT. PKINIT is a pre-authentication extension that extends the Kerberos Protocol to use public key cryptography and ticket-granting ticket (TGT) data signing during the initial AS exchange.

This specification describes the extensions to PKINIT that enable the use of public key cryptography in the initial authentication exchanges of the Kerberos protocol (Authentication Service (AS) exchange) [RFC4120].

1.4 Relationship to Other Protocols

PKCA is defined as a Kerberos pre-authentication extension ([RFC4120] section 3.1.1). This extension is used in the Kerberos AS exchange [RFC4556], and therefore PKCA relies on a working Kerberos infrastructure and a certificate authority (CA) for issuing [X509] certificates. PKCA includes the use of elliptic curve cryptography (ECC). ECC support [RFC5349] relies upon a CA issuing ECC certificates. Applications already using Kerberos can use PKCA without modifications.

In order to support NTLM authentication [MS-NLMP] for applications connecting to network services that do not support Kerberos authentication, when PKCA is used, the KDC returns the user's NTLM one-way function (OWF) in the privilege attribute certificate (PAC) PAC_CREDENTIAL_INFO buffer ([MS-PAC] section 2.6.1).

1.5 Prerequisites/Preconditions

PKCA assumes the following, in addition to any assumptions specified in [MS-KILE]:

1. The key distribution center (KDC) has an X.509 public key certificate [X509], issued by a certificate authority (CA) and trusted by the clients in the Kerberos realm. For ECC support, the KDC has an ECC public key certificate issued by a CA and trusted by clients in the Kerberos realm. The issuing of these [X509] certificates is not addressed in this protocol specification.

2. A cryptographic-strength random-number generator is available for generating keys and other cryptographically sensitive information.<1>

3. Each user has an [X509] certificate suitable for use with PKINIT. Details about such a certificate are specified in [RFC4556] Appendix C.

Details about general Kerberos assumptions are specified in [RFC4120] section 1.6.

1.6 Applicability Statement

PKCA is used only in environments that use Kerberos, and it requires the deployment of a Public Key Infrastructure (PKI) for issuing [X509] certificates.

1.7 Versioning and Capability Negotiation

PKCA does not have explicit versioning; it is tied to the Kerberos protocol [MS-KILE] versioning mechanisms, as specified in [RFC4120] section 7.5.6. Capability negotiation is as specified in [RFC4556] sections 3.3 and 3.4.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

There are no standards assignments in PKCA beyond what is specified in [RFC4556] and [RFC5349].

2 Messages

2.1 Transport

Messages are carried in the Kerberos AS exchange as pre-authentication data, as specified in [RFC4120] section 5.2.7.

2.2 Message Syntax

The message syntax SHOULD<2> be as specified in [RFC4556] section 3.2.

PKCA MAY<3> support these variations based on an earlier draft of [RFC4556] for interoperability.

An earlier draft of [RFC4556] supported a different pre-authentication data identifier:

- PA-PK-AS-REP_OLD 15

The algorithm identifier in Cryptographic Message Syntax (CMS) messages, as specified in [RFC2315] and [RFC3852], is md5WithRSAEncryption instead of md5 ([RFC3370] sections 3.2 and 2.2).<4> SHA-1WithRSAEncryption [RFC3370] SHOULD<5> be supported. ecdsa-with-Sha1, ecdsa-with-Sha256, ecdsa-with-Sha384, and ecdsa-with-Sha512 ([RFC5349] section 3) SHOULD<6> be supported.

The following ECC curves ([RFC5349] section 5) SHOULD<7> be supported:

- ECPRGF256Random | groupP-256 | secp256r1
- ECPRGF384Random | groupP-384 | secp384r1
- ECPRGF521Random | groupP-521 | secp521r1

2.2.1 PA-PK-AS-REP_OLD 1

The data for the PA-PK-AS-REP_OLD pre-authentication data identifiers is based on an earlier draft of [RFC4556]; therefore, there are some differences in the message format. The ASN.1 [ITUX680] description of the message that SHOULD<8> be used in place of the message format specified in [RFC4556] section 3.2.1 follows.

```
PKINIT DEFINITIONS EXPLICIT TAGS ::=
BEGIN
--EXPORTS ALL--
IMPORTS
KerberosTime, PrincipalName, Realm, EncryptionKey
FROM KerberosV5Spec2
{ iso(1) identified-organization(3) dod(6) internet(1) security(5)
         kerberosV5(2) }
-- Different from [RFC4556] Appendix A
ContentInfo, EnvelopedData, SignedData, IssuerAndSerialNumber
FROM CryptographicMessageSyntax2004
{ iso(1) member-body(2) us(840) rsadsi(113549)
pkcs(1) pkcs-9(9) smime(16) modules(0) cms-
2004(24) }
-- Same as defined in [RFC3852]
AlgorithmIdentifier
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] (Same as defined in [RFC4556] Appendix A)
--
-- PKINT data types
```

```
--
PA-PK-AS-REQ ::= SEQUENCE {
-- PA TYPE 15
signedAuthPack [0] IMPLICIT OCTET STRING
}


AuthPack::= SEQUENCE {
    pkAuthenticator  [0] PKAuthenticator
}


--
-- PK-AUTHENTICATOR - Different from [RFC4556]
-- Appendix A, PKAuthenticator.
--
PKAuthenticator::= SEQUENCE {
    kdc-name   [0] PRINCIPAL-NAME,
    kdc-realm  [1] REALM,
-- name and realm of the KDC issuing the ticket
    cusec      [2] INTEGER,
    ctime      [3] KerberosTime,
    nonce      [4] INTEGER
}
END
```

PA-PK-AS-REQ field:

- signedAuthPack: Contains content identical to the content of the signedAuthPack field, as specified in [RFC4556] section 3.2.1.

AuthPack field:

- pkAuthenticator: Contains a PKAuthenticator structure, as defined in this document. This variation of the AuthPack structure is different from the one specified in [RFC4556].

PKAuthenticator fields:

- kdc-name: Contains the name portion of the ticket-granting service (TGS) name of the KDC that will service the request, as specified in [RFC4120] section 7.3.
- kdc-realm: Contains the realm portion of the TGS name of the KDC that will service the request, as specified in [RFC4120] section 7.3.
- cusec: Contains the same content of the corresponding, identically named field in the type PKAuthenticator, as specified in [RFC4556] section 3.2.1.
- ctime: Contains the same content of the corresponding, identically named field in the type PKAuthenticator, as specified in [RFC4556] section 3.2.1.
- nonce: Contains the same content of the corresponding, identically named field in the type PKAuthenticator, as specified in [RFC4556] section 3.2.1.

2.2.2 PA-PK-AS-REP_OLD 2

The data for the PA-PK-AS-REP_OLD pre-authentication data identifiers is based on an earlier draft of [RFC4556]; therefore, there are some differences in the message format. The ASN.1 [ITUX680] description of the message that SHOULD<9> be used in place of the message format specified in [RFC4556] section 3.2.3 follows.

```
--
-- KERB-REPLY-KEY-PACKAGE - Different from [RFC4556]
```

```
-- Appendix A, ReplyKeyPack
--
KERB-REPLY-KEY-PACKAGE ::= SEQUENCE {
    replyKey [0] EncryptionKey,
-- Contains the session key used to encrypt the enc-part
-- field in the AS-REP, for example, the AS reply key.


nonce [1] INTEGER,
-- binds response to the request; must be same as the nonce
-- passed in the PK-AUTHENTICATOR.
    ...
} --#public-
```

KERB-REPLY-KEY-PACKAGE fields:

- replyKey: Contains the same content of the identically named field in the type ReplyKeyPack, as specified in [RFC4556] section 3.2.3.2.
- nonce: Contains the nonce from the PKAuthenticator structure in the PA-PK-AS-REQ request.

However, if the AS-REQ message contains a padata of type KRB5-PADATA-AS-CHECKSUM(132) with no corresponding data field (padata-value is an empty OCTET STRING), then the PA-PK-AS-REP_OLD pre-authentication data contains the same data as specified in [RFC4556] section 3.2.3.2.

2.2.3 PA-PK-AS-REQ

The PA-PK-AS-REQ message format is specified in [RFC4556] section 3.2.1.<10>

2.2.4 PA-PK-AS-REP

The PA-PK-AS-REP message format is specified in [RFC4556] section 3.2.3.<11> The returned ticket does not include the AD-INITIAL-VERIFIED-CAS type in the authorization data. The content of the SignedData field in the content of EnvelopedData is encoded, as specified in [RFC2315] section 7, not as specified in [RFC3852]. Therefore, the data is not wrapped in OCTET STRING; rather, it is wrapped in an ANY DEFINED BY content specific type, as specified in [RFC2315] section 7.

3 Protocol Details

3.1 Common Details

3.1.1 (Updated Section) Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

The abstract data model follows what is specified in [RFC4556].

3.1.2 Timers

None.

3.1.3 Initialization

During initialization, the [FIPS140]-compliant random-number generator for keys and nonces is initialized.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

In addition to the required ([RFC4556] section 3.1.1) and recommended ([RFC4556] section 3.1.2) algorithms, PKCA supports the rc2-cbc ([RFC4556] section 3.1.4) algorithm. An implementer SHOULD<12> specify des-ede3-cbc ([RFC4556] section 3.1.2) as the default algorithm.

PKCA does not implement the id-pkinit-san algorithm ([RFC4556] section 3.2.2).

PKCA SHOULD<13> support the PKINIT Freshness Extension [RFC8070].

3.1.5.1 Client

The Kerberos client SHOULD<14><15> send only a PA-PK-AS-REQ pre-authentication data identifier.

Kerberos clients can process either the PA-PK-AS-REP_OLD or the PA-PK-AS-REP pre-authentication data identifier in the reply, but not both.<16>

For computer AS-REQ, PKCA clients SHOULD<17> fail unless all of the following conditions are met.

- The computer certificate contains:
  - subjectAltName (SAN) DNSName field: <computer name>.<DNS domain name> where <computer name> matches the computer name and <DNS domain name> matches the computer's DNS domain name.
  - Enhance Key Usage (EKU): id-pkinit-KPClientAuth (1.3.6.1.5.2.3.4) or TLS/SSL Client Authentication (1.3.6.1.5.5.7.3.2).

- The KDC certificate contains:
  - SAN DNSName field: the DNS name of the domain
  - EKU: id-pkinit-KPkdc (1.3.6.1.5.2.3.5)

3.1.5.2 KDC

If the KDC receives both a PA-PK-AS-REQ and PA-PK-AS-REQ_OLD, the KDC must return KRB_ERROR_GENERIC.

The KDC SHOULD<18> process the PA-PK-AS-REQ pre-authentication data identifier. The KDC SHOULD<19> respond with PA-PK-AS-REP.

The KDC MUST return the user's unicodePwd attribute ([MS-ADA3] section 2.332) in the NTLM_SUPPLEMENTAL_CREDENTIAL buffer ([MS-PAC] section 2.6.4).

3.1.5.2.1 Certificate Mapping

The KDC SHOULD look up the account using the cname. If the account is not found and the cname name-type is NT-X500-PRINCIPAL, the KDC locates the account in the account database using the explicit mapping fields. Implementations of PKCA KDCs which use Active Directory for the account database when the userAccountControl attribute ([MS-ADA3] section 2.342) bit WT or ST ([MS-ADTS] section 2.2.16) is:

- TRUE: validate certificate mapping using the SAN **DNSName** field.<20>
- Both FALSE: validate certificate mapping using the SAN **UPNName** field first, then try explicit mapping.

If the account is not found, the KDC returns KDC_ERR_C_PRINCIPAL_UNKNOWN.

3.1.5.2.1.1 SAN DNSName field

The KDC MUST confirm that the name of the account found matches the computer name in the **DNSName** field of the certificate terminated with "$" and that the DNS domain name in the **DNSName** field of the certificate matches the DNS domain name of the realm. Implementations of PKCA KDCs which use Active Directory for the account database MUST use the **sAMAccountName** attribute ([MS-ADA3] section 2.222) for the computer name. If they do not match, the KDC SHOULD return KDC_ERR_CLIENT_NAME_MISMATCH.

3.1.5.2.1.2 SAN UPN field

The KDC MUST confirm that the account found matches that the account found when using the UPN in the **UPN** field of the certificate. If they do not match, the KDC SHOULD return KDC_ERR_CLIENT_NAME_MISMATCH.

3.1.5.2.1.3 Explicit Mapping

The KDC MUST confirm the explicit mapping of the account to a certificate. Implementations of PKCA KDCs which use Active Directory for the account database MUST confirm that the **altSecurityIdentities** attribute ([MS-ADA1] section 2.61) contains the string created by concatenating the following information from the certificate in the order shown:

1. Subject and Issuer Name fields: "X509:<I>" + Issuer Name field with "\r" and "\n" replaced with "," + "<S>" + Subject field with "\r" and "\n" replaced with ",".
2. Subject field: "X509:<S>" + Subject field with "\r" and "\n" replaced with ",".

3. Issuer and Serial Number fields: "X509:<I>" + Issuer Name field with "\r" and "\n" replaced with "," + "<SR>" + Serial Number field.

4. Subject Key Identifier field: "X509:<SKI>" + Subject Key Identifier field.

5. SHA1 hash of public key: "X509:<SHA1-PUKEY>" + SHA1 hash of public key.

6. 822 field: "X509: <RFC822>" + 822 Name field.

If they do not match, the KDC SHOULD return KDC_ERR_CLIENT_NAME_MISMATCH.

3.1.5.2.1.4 Key Trust

The KDC SHOULD<21> look the account up using the public key. If an account is found with the public key that is trusted for the account, then the KDC SHOULD:

- If the account was also found using the cname but the accounts do not match, return KDC_ERR_CLIENT_NAME_MISMATCH.
- Ignore any certificate chain validation errors.

Implementations of PKCA KDCs that use Active Directory for the account database MUST confirm that the msDS-KeyMaterial attribute ([MS-ADA2] section 2.350) contains the same public key.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

There are no local events other than what is specified in [RFC4556].

4 Protocol Examples

The following sections describe three common scenarios to illustrate the function of the KILE.

4.1 Interactive Logon Using Smart Cards

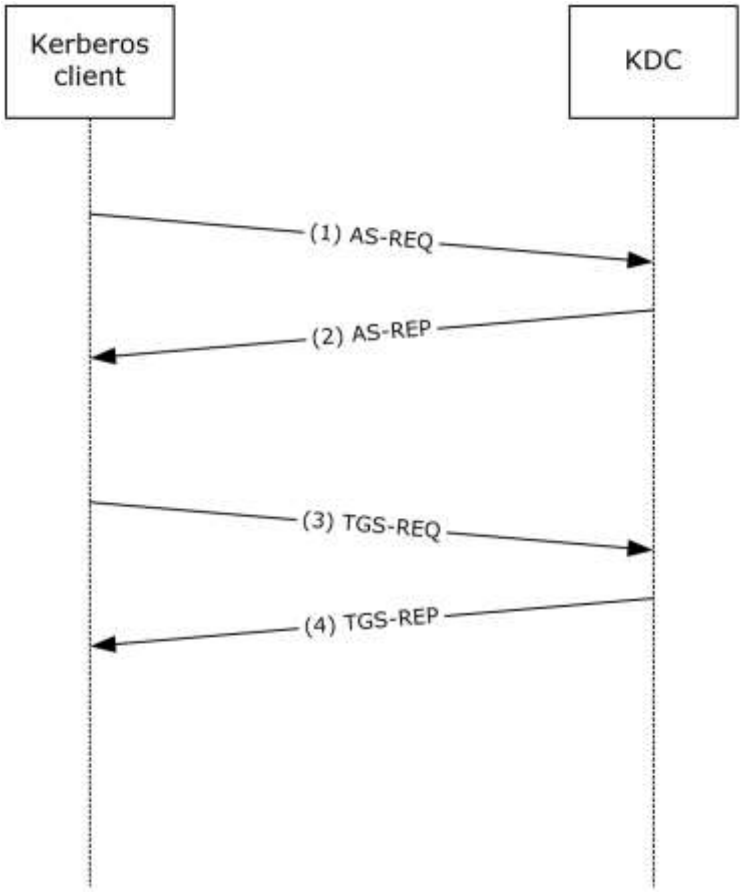

Figure 1: Interactive logon

Step 1: A user attempts to log on to a client. At the logon screen, the user selects the certificate and types the PIN. Using the PIN to unlock the smart card, the client generates an AS-REQ with PA-PK-AS-REQ pre-authentication data ([RFC4556] section 3.2.1) and sends the request to the KDC.

Step 2: The KDC validates the AS-REQ ([RFC4120] section 3.1.2), including verifying the user's signature and validating certificate ([RFC4556] section 3.2.2). If the AS-REQ is valid, the KDC generates an AS-REP ([RFC4556] section 3.2.3), with a PAC ([MS-KILE] section 3.3.5.3.2) in the authorization_data field of the TGT, and sends the reply to the client.

Step 3: The client validates the AS-REP ([RFC4556] section 3.2.4). For interactive logons, the client runtime requests authentication to host/hostname.domain, where hostname is the actual name of the client machine, and domain is the domain or realm of the client machine. If the AS-REP is valid, the client generates a TGS-REQ based on the TGT that is obtained in step 2 to obtain a service ticket for host/hostname.domain ([RFC4120] section 3.3.1) and sends the request to the KDC.

Step 4: The KDC validates the TGS-REQ ([RFC4120] section 3.3.2) ([MS-KILE] section 3.3.5.7.1). If the TGS-REQ is valid, the KDC adds Domain Local Groups to the PAC ([MS-KILE] section 3.3.5.7.3), generates a TGS-REP ([RFC4120] section 3.3.3), and sends the reply to the client.

The client validates the TGS-REP ([MS-KILE] section 3.3.4). If the TGS-REP is valid, the service ticket is then interpreted by the Kerberos runtime within the local workstation.

The following fields from the KERB_VALIDATION_INFO field of the PAC ([MS-PAC] Section 2.5) are required by the interactive logon client runtime to authorize the user for local interactive logon, and to establish the necessary management profile for the user:

- LogonTime
- LogoffTime
- KickOffTime
- PasswordLastSet
- PasswordCanChange
- EffectiveName
- FullName
- LogonScript
- ProfilePath
- HomeDirectory
- HomeDirectoryDrive
- LogonCount
- BadPasswordCount
- LogonServer
- LogonDomainName
- UserAccountControl

4.2 Network Logon Using Smart Cards

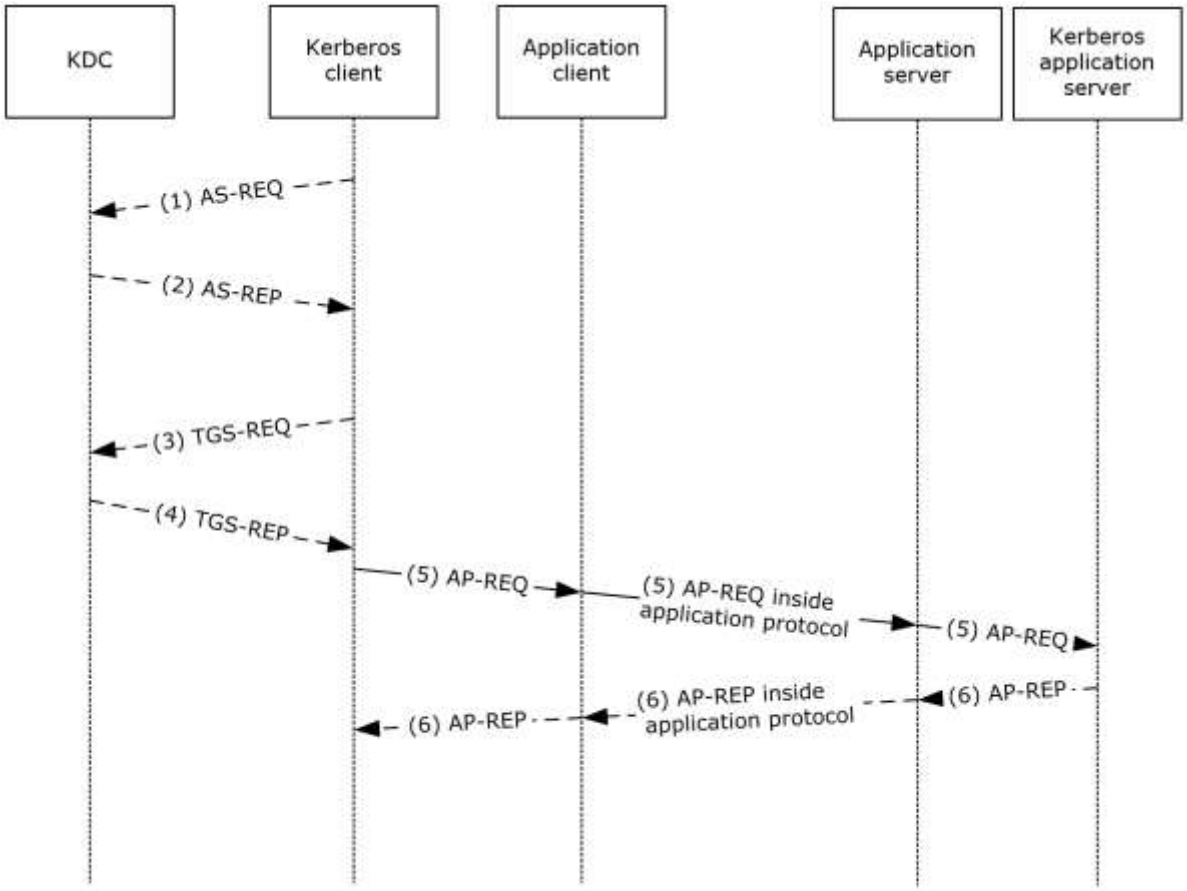

Figure 2: Network logon

When an application wants authentication, it calls GSS_Init_sec_context ([RFC2743] section 2.2.1) to either invoke KILE [MS-KILE] directly, or SPNEGO [MS-SPNG] which can invoke Kerberos.

Step 0: The application client calls GSS_Init_sec_context ([RFC2743] section 2.2.1).

When the client does not have a TGT, steps 1 through 2, as described in section 4.1, are performed.

When the client does not have a service ticket for the application server, steps 3 and 4, as described in section 4.1, are performed.

Step 5: The Kerberos client generates a GSS-API initial token ([RFC1964] section 1.1.1) containing an AP-REQ ([RFC4120] section 3.2.2) and returns it to the application.

Step 6: The application server calls GSS_Accept_sec_context ([RFC2743] section 2.2.2). The Kerberos application server validates the AP-REQ ([RFC4120] section 3.2.3). If the AP-REQ is valid and the client requested mutual authentication, the Kerberos application server generates a GSS-API response token ([RFC1964] section 1.1.2) containing an AP-REP ([RFC4120] section 3.2.4) and returns it to the application server. The Kerberos application server provides the authorization data from the ticket to the operating system, which creates an object called an access token that provides authorization functions.

If mutual authentication was requested, the application client calls GSS_Init_sec_context ([RFC2743] section 2.2.1). The Kerberos client validates the AP-REP ([RFC4120] section 3.2.5). If the AP-REP is valid, the Kerberos client returns GSS_S_COMPLETE ([RFC2743] section 2.2.1).

4.3 Non-RFC Kerberos Clients during AS-REQ

PKCA clients developed prior to finalizing RFC 4556 support a PKInit pre-authentication data based on an earlier draft of [RFC4556].

Step 1: A user attempts to log on to a client. At the logon screen, the user selects the certificate and types the PIN. Using the PIN to unlock the smart card, the client generates an AS-REQ with PA-PK-AS-REP_OLD pre-authentication data (section 2.2.1) and sends the request to the KDC.

Step 2: The KDC validates the AS-REQ ([RFC4120] section 3.1.2) including verifying the user's signature and validating certificate ([RFC4556] section 3.2.2). Since the PA-PK-AS-REP_OLD version of the pre-authentication data does not contain a paChecksum, the KDC does not return a KRB-ERROR with the code KDC_ERR_PA_CHECKSUM_MUST_BE_INCLUDED ([RFC4556] section 3.2.3). If the AS-REQ is valid, with the exception of the paChecksum checks, the KDC generates an AS-REP ([RFC4556] section 3.2.3) using the PA-PK-AS-REP_OLD, instead of the PA-PK-AS-REP with a PAC ([MS-KILE] section 3.3.5.6.4) in the authorization_data field of the TGT, and sends the reply to the client.

5 Security

5.1 Security Considerations for Implementers

PKCA security considerations are specified in [RFC4556]. PA-PK-AS-REP_OLD is the earlier version of PA-PK-AS-REQ and PA-PK-AS-REP, and has the same security considerations.

5.2 Index of Security Parameters

PKCA security parameters are specified in [RFC4556].

Security parameter	Section
PKAuthenticator	2.2.1
KERB-REPLY-KEY-PACKAGE	2.2.2

6 (Updated Section) Appendix A: Product Behavior

The information in this specification is applicable to the following Microsoft products or supplemental software. References to product versions include updates to those products.

- Windows 2000 operating system
- Windows XP operating system
- Windows Server 2003 operating system
- Windows Vista operating system
- Windows Server 2008 operating system
- Windows 7 operating system
- Windows Server 2008 R2 operating system
- Windows 8 operating system
- Windows Server 2012 operating system
- Windows 8.1 operating system
- Windows Server 2012 R2 operating system
- Windows 10 operating system
- Windows Server 2016 operating system
- Windows Server operating system
- Windows Server 2019 operating system
- Windows Server 2022 operating system

Exceptions, if any, are noted in this section. If an update version, service pack or Knowledge Base (KB) number appears with a product name, the behavior changed in that update. The new behavior also applies to subsequent updates unless otherwise specified. If a product edition appears with the product version, behavior is different in that product edition.

Unless otherwise specified, any statement of optional behavior in this specification that is prescribed using the terms "SHOULD" or "SHOULD NOT" implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term "MAY" implies that the product does not follow the prescription.

<1> Section 1.5: Windows contains a FIPS-140-validated random-number generator, as specified in [FIPS140].

<2> Section 2.2: [RFC4556] message syntax is not supported in Windows 2000, Windows XP, and Windows Server 2003.

<3> Section 2.2: Windows 2000, Windows XP, and Windows Server 2003 sent PA-PK-AS-REP_OLD where [RFC4120] would have them send PA-PK-AS-REQ or PA-PK-AS-REP.

<4> Section 2.2: Supported by Windows 2000, Windows XP operating system Service Pack 2 (SP2), and Windows Server 2003 operating system with Service Pack 1 (SP1). In Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2, the object identifier (OID) has been updated

to match CMS algorithms, as specified in [RFC3370] sections 3.2 and 2.2. Windows 2000, Windows XP, Windows XP operating system Service Pack 1 (SP1), and Windows Server 2003 do not accept the correct OID.

<5> Section 2.2: Not supported by Windows 2000, Windows XP, and Windows Server 2003.

<6> Section 2.2: **ECC** is not supported by Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008.

<7> Section 2.2: ECC is not supported by Windows 2000, Windows XP, Windows Server 2003, Windows Vista, or Windows Server 2008.

<8> Section 2.2.1: In Windows 2000, Windows XP SP2, and Windows Server 2003 with SP1, SignedData is encoded as specified in [RFC2315] section 9, not as specified in [RFC3852] section 5. Therefore, the data is not wrapped in OCTET STRING; it is wrapped in an ANY, as specified in [RFC2315] section 7.

Except in Windows 2000, Windows XP, and Windows Server 2003, SignedData is encoded as specified in [RFC3852].

Only Windows XP prior to Windows XP SP2, and Windows Server 2003 prior to Windows Server 2003 with SP1, do not accept the SignedData, as specified in [RFC3852].

In Windows 2000, Windows XP SP2, and Windows Server 2003 with SP1, the DHRepInfo form is not implemented; the Public Key Encryption style is used, as specified in [RFC4556] section 3.2.3.2.

The Diffie-Hellman key delivery method, as specified in [RFC4556] section 3.2.3.1, is not supported in Windows 2000, Windows XP, and Windows Server 2003.

In Windows 2000, Windows XP SP2, and Windows Server 2003 with SP1, the content-type field of the SignedData in PA-PK-AS-REQ is id-data, as specified in [RFC3852] section 4, instead of id-pkinit-authData.

Except in Windows 2000, Windows XP, and Windows Server 2003, the content-type field of the SignedData is id-pkinit-authData, as specified in [RFC4556] section 3.2.3.2.

Only Windows XP prior to Windows XP SP2, and Windows Server 2003 prior to Windows Server 2003 with SP1, do not accept id-data in the PA-PK-AS-REQ_OLD pre-authentication data.

<9> Section 2.2.2: In Windows 2000, Windows XP SP2, and Windows Server 2003 with SP1, the content-type field of the SignedData type inside the EnvelopedData type in the PA-PK-AS-REP_OLD pre-authentication data is id-data, as defined in [RFC3852] section 4, instead of id-pkinit-rkeyData, as defined in [RFC4556]. In all other Windows releases, the content-type field is id-pkinit-rkeyData, as specified in [RFC4556].

Except in Windows XP prior to Windows XP SP2 and Windows Server 2003 prior to Windows Server 2003 with SP1, Windows accepts id-data in the **SignedData** contained in the PA-PK-AS-REP_OLD pre-authentication data.

Windows does not process id-pkinit-san in the client's [X509] certificate, if present, as specified in [RFC4556] section 3.2.4.

<10> Section 2.2.3: The PA-PK-AS-REQ message format is not supported in Windows 2000, Windows XP, and Windows Server 2003.

<11> Section 2.2.4~~<11> Section 2.2.4:~~: The RFC version of PA-PK-AS-REP is not supported in Windows 2000, Windows XP, and Windows Server 2003.

<12> Section 3.1.5: In Windows with PKCA, the KDC supports both des-ede3-cbc and rc2-cbc. If both des-ede3-cbc and rc2-cbc are present, the KDC uses des-ede3-cbc.

<13> Section 3.1.5: [RFC8070] is not supported in Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows Server 2012, Windows 8.1, or Windows Server 2012 R2.

<14> Section 3.1.5.1: Except in Windows 2000, Windows XP, and Windows Server 2003, the PKINIT pre-authentication data identifiers have been updated to match what is specified in [RFC4556], with one addition (KRB5-PADATA-AS-CHECKSUM) as noted below. However, for backward-compatibility, if the client detects that the KDC is running Windows 2000, Windows XP, Windows Server 2003, or Windows Vista, it sends both.

Except in Windows 2000, Windows XP, and Windows Server 2003, the client sends additional padata (KRB5-PADATA-AS-CHECKSUM) besides what is specified in [RFC4556]. This padata contains no data.

```
#define KRB5_PADATA_AS_CHECKSUM         132 /* AS checksum */
```

Clients running Windows XP and Windows 2000 also send this additional padata type.

<15> Section 3.1.5.1: Windows 2000, Windows XP, and Windows Server 2003 clients send a PA-PK-AS-REP_OLD pre-authentication data identifier. Windows Vista, Windows Server 2008, Windows 7, and Windows Server 2008 R2 clients send a PA-PK-AS-REP_OLD pre-authentication data identifier when all of the following are true:

- The user certificate has a smart card logon EKU.
- The user certificate has a UPN in Subject Alternative Name.

<16> Section 3.1.5.1: Windows 2000 and Windows XP SP2 Kerberos clients only process PA-PK-AS-REP-WINDOWS-OLD.

<17> Section 3.1.5.1: Computer logon is not supported by Windows 2000, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7 and Windows Server 2008 R2.

<18> Section 3.1.5.2: Windows 2000 and Windows Server 2003 KDCs always discard the PA-PK-AS-REQ data identifier and process the PA-PK-AS-REP_OLD data identifier, if present.

<19> Section 3.1.5.2: Windows 2000 and Windows Server 2003 KDCs respond with PA-PK-AS-REP_OLD.

<20> Section 3.1.5.2.1: SAN **DNSName** field is not supported by Windows 2000, Windows Server 2003, Windows Server 2008 and Windows Server 2008 R2.

<21> Section 3.1.5.2.1.4: Public key lookup is not supported by Windows 2000, Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, or Windows Server 2012 R2 KDCs.

7 Change Tracking

This section identifies changes that were made to this document since the last release. Changes are classified as Major, Minor, or None.

The revision class **Major** means that the technical content in the document was significantly revised. Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements.
- A document revision that captures changes to protocol functionality.

The revision class **Minor** means that the meaning of the technical content was clarified. Minor changes do not affect protocol interoperability or implementation. Examples of minor changes are updates to clarify ambiguity at the sentence, paragraph, or table level.

The revision class **None** means that no new technical changes were introduced. Minor editorial and formatting changes may have been made, but the relevant technical content is identical to the last released version.

The changes made to this document are listed in the following table. For more information, please contact dochelp@microsoft.com.

Section	Description	Revision class
6 Appendix A: Product Behavior	Updated for this version of Windows Server.	Major

8 Index