[MS-RCMP]:
Remote Certificate Mapping Protocol Specification

Revision Summary

Date	Revision History	Revision Class	Comments
07/20/2007	0.1	Major	MCPP Milestone 5 Initial Availability
09/28/2007	0.1.1	Editorial	Revised and edited the technical content.
10/23/2007	0.1.2	Editorial	Revised and edited the technical content.
11/30/2007	0.1.3	Editorial	Revised and edited the technical content.
01/25/2008	0.1.4	Editorial	Revised and edited the technical content.

Table of Contents

1 Introduction

This document specifies the Remote Certificate Mapping Protocol. The Remote Certificate Mapping Protocol is a Microsoft-proprietary protocol and is used by servers that authenticate users via X.509 certificates, as specified in [X509]. This protocol allows the server to use a directory, database, or other technology to map the user's X.509 certificate to a **security principal**. This protocol returns the authorization information associated with the security principal in the form of a **privilege attribute certificate (PAC)**, as specified in [MS-PAC], that represents the user's identity and group memberships. Throughout this document, little-endian format applies unless otherwise stated.

1.1 Glossary

The following terms are defined in [MS-GLOS]:

Active Directory (AD)
Distinguished Name (DN)
Domain
Domain Controller (DC)
Domain Object
Issuer Name
Object Identifier (OID)
Principal
Privilege Attribute Certificate (PAC)
Remote Procedure Call (RPC)
RPC Transport
Security Principal
Service Principal Name (SPN)
Unicode
User Principal Name (UPN)

The following terms are specific to this document:

Object: An entity in **Active Directory (AD)** consisting of a set of attributes, each attribute with a set of associated values, as specified in [MS-ADTS].

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

1.2 References

1.2.1 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. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-ADTS] Microsoft Corporation, "Active Directory Technical Specification", June 2007.

[MS-ERREF] Microsoft Corporation, "Windows Error Codes", January 2007.

[MS-GLOS] Microsoft Corporation, "Windows Protocols Master Glossary", March 2007.

[MS-KILE] Microsoft Corporation, "Kerberos Protocol Extensions", January 2007.

[MS-NRPC] Microsoft Corporation, "Netlogon Remote Protocol Specification", March 2007.

[MS-PAC] Microsoft Corporation, "Privilege Attribute Certificate Data Structure", January 2007.

[MS-RPCE] Microsoft Corporation, "Remote Procedure Call Protocol Extensions", January 2007.

[MS-SECO] Microsoft Corporation, "Windows Security Overview", January 2007.

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

[RFC2246] Dierks, T. and Allen, C., "The TLS Protocol Version 1.0", RFC 2246, January 1999, http://www.ietf.org/rfc/rfc2246.txt

[RFC2716] Aboba, B. and Simon, D., "PPP EAP TLS Authentication Protocol", RFC 2716, October 1999, http://www.ietf.org/rfc/rfc2716.txt

[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

Note There is a charge to download the specification.

[X690] ITU-T, "Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", Recommendation X.690, July 2002, http://www.itu.int/rec/T-REC-X.690/en

Note There is a charge to download the specification.

1.2.2 Informative References

[GUTMANN] Gutmann, P., "X.509 Style Guide", October 2000, http://www.cs.auckland.ac.nz/~pgut001/pubs/x509guide.txt

1.3 Protocol Overview (Synopsis)

The Remote Certificate Mapping Protocol is used in deployments where users rely on X.509, as specified in [X509], certificates to gain access to resources. After a client authenticates itself to a server using an X.509 certificate, the server uses the Remote Certificate Mapping Protocol to contact a directory to determine the authorization information to use, such as group memberships. The Remote Certificate Mapping Protocol returns a privilege attribute certificate (PAC), as specified in [MS-PAC], that represents the user's identity and group memberships, suitable for making authorization decisions.

There are three methods by which a certificate can be associated with an account for the purposes of authorization. First, the **subjectAltName** field of the X.509 certificate should be treated as a **user principal name (UPN)** and used as the key, in the database sense, to locate the account record and corresponding authorization information. Second, the issuer and subject names should be taken together as a key, again in the database sense, to locate the account record. Third, the **issuer name** alone should be used as the lookup key when locating the account record.

The Remote Certificate Mapping Protocol itself consists of single request/reply message pair: SSL_CERT_LOGON_REQ (section 2.2.1) and SSL_CERT_LOGON_RESP (section 2.2.2). This request/response pair is transferred by using the generic pass-through capability of the Netlogon Remote Protocol, as specified in [MS-NRPC] section 3.2.4.1. The client creates an

SSL_CERT_LOGON_REQ message that contains the X.509 certificate for which the client wants to obtain the corresponding authorization information and specifies which (or all) of the methods described above should be applied. The Remote Certificate Mapping Protocol server uses attributes of this X.509 certificate and the indicated methods by the client to determine the authorization information. Assuming an account is found, the Remote Certificate Mapping Protocol server then creates and returns a PAC, as specified in [MS-PAC], that contains the authorization information in the SSL_CERT_LOGON_RESP message to the Remote Certificate Mapping Protocol client.

The Remote Certificate Mapping Protocol specification uses common fields from X.509, as specified in [X509], including **subjectName**, **subjectAltName**, and **issuerName**. An implementer of the Remote Certificate Mapping Protocol must be familiar with X.509 certificates, in particular the verification and parsing of the certificate to extract the fields listed above. For more information about X.509, see [GUTMANN].

1.4 Relationship to Other Protocols

Any protocol that authenticates clients based on public key certificates can make use of the Remote Certificate Mapping Protocol to obtain authorization information about the client. The Netlogon Remote Protocol serves as the transport for Remote Certificate Mapping Protocol messages.<1>

1.5 Prerequisites/Preconditions

The Remote Certificate Mapping Protocol requires that users have X.509 certificates available to them for authentication. The Remote Certificate Mapping Protocol also requires that a means exists to associate a certificate with a set of authorization data, commonly some form of an account database.<2>

1.6 Applicability Statement

The Remote Certificate Mapping Protocol is applicable in deployments where users have been issued X.509 certificates, as specified in [X509], and a common database for user and machine authorization information. In this type of environment, the Remote Certificate Mapping Protocol is used between the authentication step and authorization step. It enables the server that uses an authentication protocol using X.509 certificates to obtain a PAC, as specified in [MS-PAC], that represents the user's identity and group memberships, suitable for making authorization decisions.

1.7 Versioning and Capability Negotiation

The Remote Certificate Mapping Protocol does not have any versioning or capability negotiation.

1.8 Vendor-Extensible Fields

The Remote Certificate Mapping Protocol does not have any vendor-extensible fields.

1.9 Standards Assignments

There are no standards assignments in the Remote Certificate Mapping Protocol beyond the standards assignments as specified in [MS-NRPC].

2 Messages

The following sections specify how Remote Certificate Mapping Protocol messages are transported and Remote Certificate Mapping Protocol message syntax.

2.1 Transport

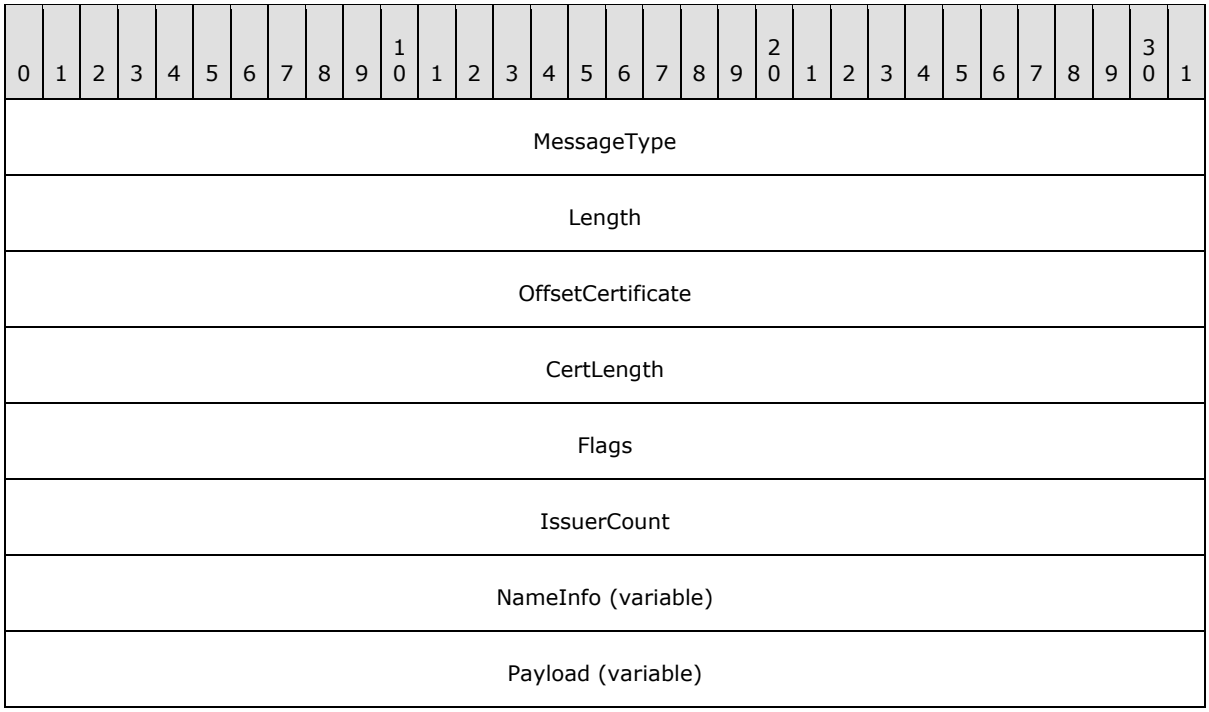
The Remote Certificate Mapping Protocol messages are embedded in Netlogon Remote Protocol messages in the logon interface. As a result, the Remote Certificate Mapping Protocol uses the Netlogon **RPC transport**, as specified in [MS-NRPC] section 2.1.

2.2 Message Syntax

Remote Certificate Mapping Protocol messages are encoded as opaque buffers and transported by the generic pass-through capability of the Netlogon Remote Protocol, as specified in [MS-NRPC] section 3.2.4.1.

2.2.1 SSL_CERT_LOGON_REQ Message

The SSL_CERT_LOGON_REQ structure defines a request to map a client certificate to a security principal for the purpose of retrieving the authorization information. All member fields MUST be encoded in little-endian format.



MessageType: A 32-bit unsigned integer that defines the Remote Certificate Mapping Protocol message type. This member MUST be 0x00000002.

Length: A 32-bit unsigned integer in little-endian format that defines the length, in bytes, of the SSL_CERT_LOGON_REQ request message, including the variable **NameInfo** and **Payload** sections.

OffsetCertificate: A 32-bit unsigned integer in little-endian format that defines the offset, in bytes, from the beginning of the SSL_CERT_LOGON_REQ request structure to the X.509 certificate, as specified in [X509], in the **Payload** member.

CertLength: A 32-bit unsigned integer in little-endian format that defines the length, in bytes, of the X.509 certificate in the **Payload** member.

Flags: A 32-bit unsigned integer that defines mapping behaviors. The value of this member is any combination of the flags as specified below.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	D	C	B	A	0	0	0	0

A (REQ_UPN_MAPPING): When set, this indicates that the Remote Certificate Mapping Protocol client requests the Remote Certificate Mapping Protocol server to use the **subjectAltName** from the X.509 certificate in the **Payload** member to locate the authorization information, as specified in section 3.5. If not set, the **subjectAltName** SHOULD NOT be used during the lookup operation.

B (REQ_SUBJECT_MAPPING): When set, the Remote Certificate Mapping Protocol client requests the Remote Certificate Mapping Protocol server to use the **issuer** and **subject** names from the X.509 certificate in the **Payload** member together to locate the authorization information, as specified in section 3.5. If not set, the **issuer** and **subject** fields SHOULD NOT be used during the lookup operation.

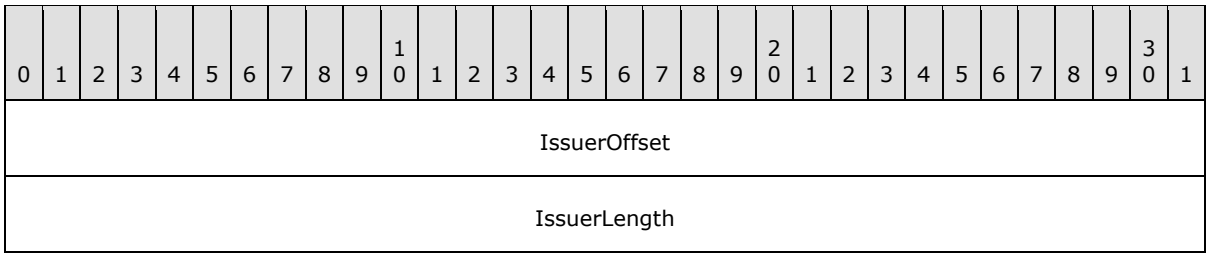
C (REQ_ISSUER_MAPPING): When set, the Remote Certificate Mapping Protocol client requests the Remote Certificate Mapping Protocol server to use the **issuer** from the X.509 certificate in the **Payload** member to locate the authorization information, as specified in section 3.5. If not set, the issuer name SHOULD NOT be used during the lookup operation.

D (REQ_ISSUER_CHAIN_MAPPING): When set, the Remote Certificate Mapping Protocol client requests the Remote Certificate Mapping Protocol server to use the chain of issuing authorities for the X.509 certificate in the **Payload** member to locate the authorization information, as specified in section 3.5. If not set, the chain of issuers SHOULD NOT be used during the lookup operation.

All other bits MUST be set to 0 by the Remote Certificate Mapping Protocol client and ignored on receipt.

IssuerCount: A 32-bit unsigned integer in little-endian format that defines the number of **NameInfo** elements.

NameInfo: An array of **IssuerOffset** and **IssuerLength** pairs, as defined below. The issuers MUST be in the same order as the chain of issuing authorities for the X.509 certificate in the **Payload** section. That is, if the certificate was issued by A, and certificate authority A was in turn issued by B, the order would be A B.



IssuerOffset: A 32-bit unsigned integer that defines the byte offset from start of packet to an **IssuerName** in the **Payload** member.

IssuerLength: A 32-bit unsigned integer that defines the length, in bytes, of an **IssuerName** in the **Payload** member.

Payload: A byte-array that contains the data referred to by the **OffsetCertificate** and **IssuerOffset** members. The data in the **Payload** section has no guaranteed order; order is defined by the **NameInfo** array listed above. Thus, the data may be packed into the buffer as "Issuer1, Issuer3, Certificate, Issuer2" but the **NameInfo** array above would list them as "Issuer1, Issuer2, Issuer3." The actual order is specified in section 3.5.1. The number of issuer names encoded into the **Payload** section is determined by the **IssuerCount** member. Each **IssuerName** MUST be 2-byte aligned and there MAY be variable length padding between each member of **Payload**.

Certificate: The client's BER-encoded X.509 certificate referred to by the **OffsetCertificate** member. The format of an X.509 certificate is specified in ASN.1 per the X.509 standard, as specified in [X509]. BER encoding is specified in [X690].

IssuerName: The BER-encoded certificate issuer name referred to by an **IssuerOffset**. Each **IssuerName** corresponds to the **issuerName** member of an X.509 certificate in the certificate chain, as specified in [X509]. Only the issuer name is present, not the complete issuer certificate.

2.2.2 SSL_CERT_LOGON_RESP Message

The SSL_CERT_LOGON_RESP structure defines a successful response to a SSL_CERT_LOGON_REQ request. It contains the PAC that is returned to the caller. All member fields MUST be encoded in little-endian order.

0	1	2	3	4	5	6	7	8	9	10	1	2	3	4	5	6	7	8	9	20	1	2	3	4	5	6	7	8	9	30	1
MessageType																															
Length																															
OffsetAuthData																															
AuthDataLength																															
Flags																															
OffsetDomain																															
DomainLength																															
Align																															
Payload (variable)																															

MessageType: A 32-bit unsigned integer that defines the Remote Certificate Mapping Protocol message type. This member MUST be 0x00000002, matching SSL_CERT_LOGON_REQ above.

Length: A 32-bit unsigned integer that defines the length, in bytes, of the SSL_CERT_LOGON_RESP response structure, including the variable **Payload** section.

OffsetAuthData: A 32-bit unsigned integer that defines the offset, in bytes, from the beginning of the SSL_CERT_LOGON_RESP response structure to the PAC, as specified in [MS-PAC], contained in the **Payload** field. This MUST be aligned to an 8-byte boundary.

AuthDataLength: A 32-bit unsigned integer that defines the length, in bytes, of the PAC, as specified in [MS-PAC], contained in the **Payload** field.

Flags: A 32-bit unsigned integer that MUST be 0, and ignored upon receipt. This field was intended for future expansion but was not used.

OffsetDomain: A 32-bit unsigned integer that defines the offset, in bytes, from the beginning of the SSL_CERT_LOGON_RESP request structure to a string of 16-bit **Unicode** characters comprising the name of the **domain** used for retrieving the authorization information. The domain name MUST be the fully qualified Domain Name System (DNS) name of the domain.

DomainLength: A 32-bit unsigned integer that defines the length, in bytes, of the domain name referred to by **OffsetDomain**. The length does not include any trailing NULL character; because the string is counted, there need not be a trailing NULL.

Align: A 32-bit unsigned integer used to maintain 64-bit alignment. This member MUST be 0x00000000.

Payload: This field contains the PAC, as specified in [MS-PAC], referred to by the **OffsetAuthData** field, and the domain name referred to by the **OffsetDomain** field.

2.3 Constants

The following constants are used in this specification.

Symbolic name	Value	Definition
STATUS_LOGON_FAILURE	0xC000006D	A logon failure occurred.

3 Protocol Details

The Remote Certificate Mapping Protocol utilizes the generic pass-through mechanism, as specified in [MS-NRPC] section 3.2.4.1, using Microsoft Unified Security Protocol Provider. The exchanged messages are SSL_CERT_LOGON_REQ and SSL_CERT_LOGON_RESP. When the account is found, the associated authorization data (for example, group memberships) is encoded as a PAC, as specified in [MS-PAC], and sent back to the Remote Certificate Mapping Protocol client. If no matching account is found, an error is returned to the client, as specified in section 3.5.2.

<3>

3.1 Abstract Data Model

The Remote Certificate Mapping Protocol requires that the server have available to it a database or directory of accounts with authorization information and associated name strings that will be used to query the database. The server will issue queries against this database based on strings extracted from the X.509 certificate.

It should be noted that a degenerate, but legal, server could map any certificate to a single set of authorization data. Or, all certificates could map to a small set of authorization data. For example, a Web server could have three levels of service (bronze, silver, and gold) managed by three certificate issuers; the Remote Certificate Mapping Protocol server would then merely map the certificates based on the issuer to one of three possible authorization levels and dispense with a full database.

3.2 Timers

There are no timers for the Remote Certificate Mapping Protocol.

3.3 Initialization

There is no initialization that is specific to the Remote Certificate Mapping Protocol.

3.4 Higher-Layer Triggered Events

The Remote Certificate Mapping Protocol message exchange is triggered by a Remote Certificate Mapping Protocol client that requires user authentication via an X.509 certificate. After this authentication takes place, the Remote Certificate Mapping Protocol client sends the SSL_CERT_LOGON_REQ message to the Remote Certificate Mapping Protocol server to obtain authorization information.

3.5 Message Processing Events and Sequencing Rules

The Remote Certificate Mapping Protocol in itself is a stateless protocol with request/response semantics. The general model is:

- The Remote Certificate Mapping Protocol client MUST determine the validity of the certificate by whatever means appropriate to the Remote Certificate Mapping Protocol client when the Remote Certificate Mapping Protocol is used to obtain a **principal's** authorization information on the basis of which access control is performed. The Remote Certificate Mapping Protocol server has three mechanisms, as specified in section 3.5.1, section 3.5.2, and section 3.5.3, for determining the authorization information.
- After the Remote Certificate Mapping Protocol client sends the SSL_CERT_LOGON_REQ message, the Remote Certificate Mapping Protocol server MAY send either an SSL_CERT_LOGON_RESP

message or return an error status in the Netlogon generic passthrough function, as specified in [MS-NRPC] section 3.2.4.1.

- Upon receiving the SSL_CERT_LOGON_REQ message and mapping the user's X.509 certificate to a particular account and authorization information, the Remote Certificate Mapping Protocol server sends a SSL_CERT_LOGON_RESP message to the Remote Certificate Mapping Protocol client.

3.5.1 Client Generation of SSL_CERT_LOGON_REQ Message

The client constructs the SSL_CERT_LOGON_REQ message by setting the user's X.509 certificate, the mapping method by which the server looks up the user's account (expressed via flags as specified in section 2.2.1) and by issuing authorities for the X.509 certificate. The issuing authorities are set in anchor last order. Anchor last order is defined as the leaf certification authority that issued the client's X.509 certificate is first, followed by the next certification authority in the certificate chain, and the next certification authority, and so on. The name of the root certification authority MUST NOT be included in the SSL_CERT_LOGON_REQ message.

The Remote Certificate Mapping Protocol client request, SSL_CERT_LOGON_REQ, is packed as a contiguous buffer and the encoded data is sent in the **LogonData** field in the NETLOGON_GENERIC_INFO structure, as specified in [MS-NRPC] section 2.2.1.4.2, via the generic passthrough capability of Netlogon, as specified in [MS-NRPC] section 3.2.4.1. The **PackageName** field in the NETLOGON_GENERIC_INFO structure, as specified in [MS-NRPC], MUST be a **UNICODE_STRING** structure with the string value being "Microsoft Unified Security Protocol Provider".<4>

3.5.2 Server Processing of SSL_CERT_LOGON_REQ Message

Upon receipt of the SSL_CERT_LOGON_REQ message at the server, the server decodes the request. The server must examine the requested flags from the client for the **REQ_UPN_MAPPING**, **REQ_SUBJECT_MAPPING**, and **REQ_ISSUER_MAPPING** flags. These correspond to the following methods described below:

- Method 1: Mapping via the **userPrincipalName** attribute. The Remote Certificate Mapping Protocol client requests this mapping scheme from the Remote Certificate Mapping Protocol server by setting the **REQ_UPN_MAPPING** flag in the SSL_CERT_LOGON_REQ message. If this mapping scheme is allowed by the Remote Certificate Mapping Protocol server's local policy, the Remote Certificate Mapping Protocol server looks up the authorization information by using the **subjectAltName** field, as specified in [X509], contained in the X.509 certificate in the request. If successful, the Remote Certificate Mapping Protocol RCMP server constructs a PAC, as specified in [MS-PAC], containing the authorization data.<5>

- Method 2: Mapping via certificate's subject and issuer **distinguished names**. The Remote Certificate Mapping Protocol client requests this mapping scheme from the Remote Certificate Mapping Protocol server, by setting the **REQ_SUBJECT_MAPPING** flag in the SSL_CERT_LOGON_REQ message. If this mapping scheme is allowed by the Remote Certificate Mapping Protocol server's local policy, the Remote Certificate Mapping Protocol server looks up the authorization information by using the subject name and issuer name contained in the X.509 certificate in the request. If successful, the Remote Certificate Mapping Protocol server constructs a PAC, as specified in [MS-PAC], containing the authorization information.<6>

- Method 3: Mapping via certificate's issuer DN. The Remote Certificate Mapping Protocol client requests this mapping scheme from the Remote Certificate Mapping Protocol server, by setting the **REQ_ISSUER_MAPPING** flag in the SSL_CERT_LOGON_REQ message. If this mapping scheme is allowed by the Remote Certificate Mapping Protocol server's local policy, the Remote

Certificate Mapping Protocol server looks up the account by using the issuer name that is contained in the X.509 certificate in the request. If the additional **REQ_ISSUER_CHAIN_MAPPING** flag is set, the other issuer names from the SSL_CERT_LOGON_REQ message are also used for the search. Each name from the chain of issuers should be used as the lookup key until a match is found, in the order from the SSL_CERT_LOGON_REQ message. If successful, the Remote Certificate Mapping Protocol server constructs a PAC, as specified in [MS-PAC], containing the authorization information.<7>

- The order that the server chooses to try these methods is not defined; a client MUST not rely on a particular order. If none of the methods specified as acceptable by the client can determine the appropriate account to use, the mapping request cannot be satisfied. In this event, there is no SSL_CERT_LOGON_RESP message constructed, and the Netlogon generic passthrough method, as specified in [MS-NRPC] section 3.2.4.1, MUST return STATUS_LOGON_FAILURE, as specified in [MS-ERREF], indicating this failure condition. There is no specific error frame or status code in the SSL_CERT_LOGON_RESP message.<8>

If none of the requested methods are successful, the server does not generate a SSL_CERT_LOGON_RESP message, and instead only returns the error code STATUS_LOGON_FAILURE (0xC000006D) to the client via the return code of the Netlogon generic pass-through, as specified in [MS-NRPC] section 3.2.4.1.

3.5.3 Server Generation of the SSL_CERT_LOGON_RESP Message

The SSL_CERT_LOGON_RESP message is constructed by the server in the event that the certificate was associated successfully with an account, and authorization information can be retrieved. The Remote Certificate Mapping Protocol server constructs a PAC, as specified in [MS-PAC], containing the authorization data. The Remote Certificate Mapping Protocol server also supplies the name of the domain that contained the account used as the source of the authorization data.

The response, SSL_CERT_LOGON_RESP (section 2.2.2), is packed as a contiguous buffer and the encoded data is sent in the **LogonData** field in the NETLOGON_GENERIC_INFO structure, as specified in [MS-NRPC] section 2.2.1.4.2.<9>

3.6 Timer Events

There are no timer events for the Remote Certificate Mapping Protocol. All associated timer events are specified in the Netlogon Remote Protocol, which serves as the transport for Remote Certificate Mapping Protocol messages.

3.7 Other Local Events

There are no other local events that affect the operation of this protocol.

4 Protocol Examples

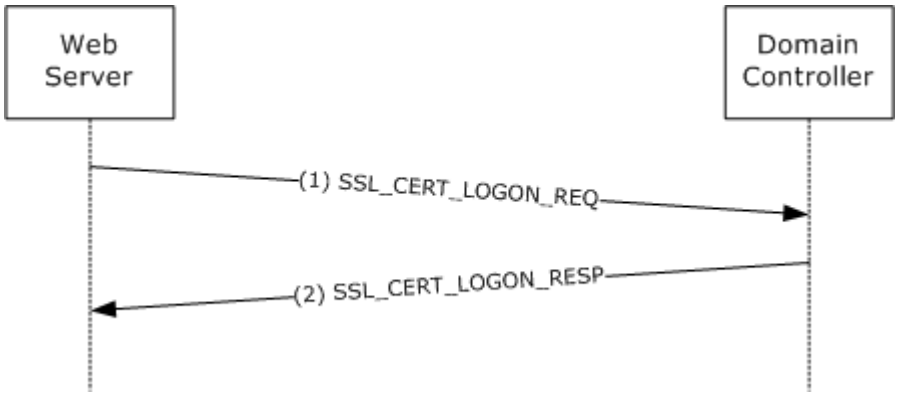


Figure 1: Obtaining a PAC that corresponds to an X.509 certificate

1. A Web server requires clients to authenticate via an X.509 certificate. During the Transport Layer Security (TLS) handshake, the client sends the user's X.509 certificate to the server and proves knowledge of the corresponding private key. On completing the handshake, the server side of the TLS implementation builds the SSL_CERT_LOGON_REQ message (which contains the user's X.509 certificate) and sends it to the Remote Certificate Mapping Protocol server, in this example, located on a **domain controller**.

2. The Remote Certificate Mapping Protocol server on the domain controller parses the incoming request and uses the X.509 certificate attributes to look up the user's account in **Active Directory**. On a successful lookup, the domain controller generates the SSL_CERT_LOGON_RESP message, which includes the user's PAC, as specified in [MS-PAC], and sends the message back via the Netlogon Remote Protocol. On receiving this message, the server will generate an NT access token, as specified in [MS-SECO], for the client, which it can then use to access resources on the user's behalf.

5 Security

The following sections specify security considerations for implementers of the Remote Certificate Mapping Protocol and an index of security parameters.

5.1 Security Considerations for Implementers

The Remote Certificate Mapping Protocol enables a user with an X.509 certificate and corresponding private key to gain access to resources based on group information associated with a given Active Directory account. Prior to performing the Remote Certificate Mapping Protocol, the Remote Certificate Mapping Protocol client must first authenticate the user using the X.509 certificate because the authorization information returned by the Remote Certificate Mapping Protocol server enables the user to gain access to various resources.

The Remote Certificate Mapping Protocol itself does not have any built-in security mechanisms to provide authentication and assure the confidentiality and integrity of the Remote Certificate Mapping Protocol client/Remote Certificate Mapping Protocol server message exchange. Instead, it relies on security mechanisms, as specified in [MS-RPCE], used to protect Netlogon **RPC**, as specified in [MS-NRPC], that transport Remote Certificate Mapping Protocol request/reply messages.

5.2 Index of Security Parameters

There are no security parameters for the Remote Certificate Mapping Protocol. All associated security parameters are specified in the Netlogon Remote Protocol, which provides all security for Remote Certificate Mapping Protocol messages.

6 Appendix A: Windows Behavior

The information in this specification is applicable to the following versions of Windows:

- Windows Server 2008
- Windows Vista
- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT

Exceptions, if any, are noted below. Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies Windows behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that Windows does not follow the prescription.

<1> Section 1.4: The Remote Certificate Mapping Protocol is used by Microsoft to implement the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol, as specified in [RFC2246], and EAP-TLS protocol, as specified in [RFC2716], when client authentication by means of an X.509 certificate is selected as part of the TLS handshake. In the SSL/TLS, authentication of client is optional and is only done when requested by the SSL/TLS server. If the client authentication option is chosen, the SSL/TLS client authenticates itself to the SSL/TLS server using an X.509 certificate.

<2> Section 1.5: Windows 2000 and later uses the Active Directory as the database for the authorization. Active Directory uses the distinguished name (DN) of the security principal**object** and the **userPrincipalName** and **altSecurityIdentities** attributes on the security principalobjects for establishing the relationship between the certificates and the authorization information, as specified in [MS-ADTS].

<3> Section 3: The Remote Certificate Mapping Protocol server is always a domain controller, and the Remote Certificate Mapping Protocol client can either be a member server of a domain or another domain controller in the same forest. The mapped account is searched within the forest of the domain controller. The domain controller can also contact another domain controller in the same forest using the SSL_CERT_LOGON_REQ and SSL_CERT_LOGON_RESP exchange if the user's account is located on a different domain than that of the domain controller that receives the request.

<4> Section 3.5.1: All four flags that are specified in section 2.2.1 are set in the SSL_CERT_LOGON_REQ message.

<5> Section 3.5.2: To look up an account, the Windows 2000 and later domain controller performs the following based on the type of certificates in the request. For machine account certificates that contain the DNS name in the dNSName Subject Alternative Extension **subjectAltName** field of the client's X.509 certificate, the domain controller prefixes the DNS host name with "host/" to form the **SPN** name form "host/machinename" and searches within the forest directory for an account that contains this SPN in the SPN attribute. For user account certificates that contain the UPN **subjectAltName** field in the X.509 certificates, the domain controller searches within the forest directory for an account containing the UPN. The matching rules in the search are the diacritical folding matching rules, as specified in [MS-KILE]. In X.509 certificates, the UPN is encoded in the subject alternative name extension with **OID** 1.3.6.1.4.1.311.20.2.3. The character encoding is in UTF8 format if the characters are not U.S. ASCII characters. Details are specified in [MS-ADTS].

<6> Section 3.5.2: The Windows 2000 and later domain controller extracts the issuer DN and the subject DN from the X.509 certificate, and constructs the following string "<I>[value of issuer]<S>[value of the subject DN]". The resulting string is evaluated against the **altSecurityIdentities** attribute of all user and machine account objects, and the scope of this evaluation is the entire forest. The matching rules are the diacritical folding rules, as specified in [MS-KILE]. The **altSecurityIdentities** attribute is a multiple-value attribute.

<7> Section 3.5.2: The Windows 2000 and later domain controller extracts the issuer DN from the X.509 certificate, and constructs the following string "<I>[value of issuer]". The resulting string is evaluated against the **altSecurityIdentities** attribute of all user and machine account objects and the scope of this evaluation is the entire forest. Note that the **altSecurityIdentities** attribute is a multiple-value attribute.

<8> Section 3.5.2: Server uses the following order to look up the user's account: First it attempts method 1; if the lookup fails, it proceeds to method 2; lastly, if method 2 fails, it attempts method 3.

<9> Section 3.5.3: If the user's account does not belong to the domain controller, then it uses Remote Certificate Mapping Protocol to contact other domain controllers. After looking up the user's account based on the algorithm described in section 3.5.2, the domain controller that the user's account belongs to constructs the PAC, as specified in [MS-PAC], that contains the domain global and domain universal groups. The SSL_CERT_LOGON_RESP (section 2.2.2) message is then passed to the domain controller that the Remote Certificate Mapping Protocol client's machine account belongs to (if the domain with the user information was different than the domain of the Remote Certificate Mapping Protocol client). This domain controller decodes the PAC and expands the group membership to include domain local groups. It then constructs a new PAC and includes it in a SSL_CERT_LOGON_RESP (section 2.2.2) message and sends it back to the Remote Certificate Mapping Protocol client.

7 Index