Certificate translation

Niklas Borselius and Chris Mitchell
Information Security Group,
Royal Holloway, University of London,
Egham, Surrey TW20 0EX, UK.
Niklas.Borselius@rhbnc.ac.uk, C.Mitchell@rhbnc.ac.uk

Abstract

As public key technology becomes more widely used, problems with incompatibility between digital certificates issued in different domains or by different CAs will become more apparent. In this paper we define and describe the concept of digital certificate translation, a concept that can be used to translate certificates of different types. Since it involves issuing new certificates the concept can also be used for other purposes such as delegating path validation and centralising trust and policy management. After describing the concept of certificate translation and some security concerns, we discuss what certificate translation can be used for and give two practical examples where the concept can prove beneficial. Finally, we look at where a protocol for certificate translation can be employed, either as an extension to existing protocols or as a stand-alone protocol.

Keywords: digital certificates, certificate translation, PKI

1 Background

The deployment and use of Public Key Infrastructures (PKIs) to facilitate secure communication has gained widespread popularity during the last few years. This trend is likely to continue for the foreseeable future. Digital certificates have a central role in any PKI. The traditional way to enable communication between entities in different PKIs is to utilise cross certification where a Certification Authority (CA) issues a certificate for a CA in another PKI. However, such certificates may not exist or may not be directly useable for various reasons.

Certificates used in different PKI implementations tend to have different structures and different information stored in them. This can make communication between entities of different PKIs tedious or even impossible. Although many PKIs make use of standard formats for certificates such as X.509 [8], this can still create problems since, as in the case of X.509, the standard supports extension fields that are not defined within the standard.

Wireless data communication is expected to take off within the next couple of years as a development of today's mobile phone systems, putting new requirements on existing networks, services, and protocols. Much effort is currently being put into standardising protocols to be used in this wireless environment. WTLS, the security protocol specified for WAP [9], has been specified to make use of digital certificates and it is assumed that digital certificates will also be used by other protocols in this new environment.

2 General concept

By electronically signing a public key along with an entity identifier and possibly various other attributes a certification authority provides assurance regarding the relationship between the public key and the included attributes. If any of these attributes are changed a new CA signature must be applied to the certificate.

In certain circumstances, such as where a certificate carries an incompatible certificate field or is of an incompatible type from that which the end user understands, it would be useful to make changes to existing certificates. Such changes can be achieved using certificate translation, a concept that forms the main focus of this paper. We now define the terms underlying this translation concept. A *translated certificate* is a certificate to which changes has been made since it was originally issued. Changes to a certificate's content as well as to its format (e.g. structure, coding) may have been made. The value of the public key is the only certificate field that may not be altered. A *certificate translation service* is able to accept a certificate and create a new (translated) certificate with a modified structure and/or content. A *certificate translation server* (CTS) is a server that offers a certificate translation service to clients. A certificate translation server would have to be trusted by its clients, the entities using the service, just like any traditional CA has to be trusted by its users.

If the CA who signed the original certificate is 'accessible' (and willing) it can issue a new certificate including the public key of the original certificate and any other attributes that apply. On other occasions the CA who issued the original certificate will not be available or able to issue a certain certificate. On such occasions a CA acting as a CTS, who is able to verify the original certificate, could issue a new certificate including the public key from the original certificate.

Another application of certificate translation is to translate a chain of certificates into a single certificate. This can in particular be useful in environments where CPU, memory, or bandwidth resources are constrained, and can also be used to centralise trust and policy management in an organisation.

3 Security considerations

3.1 Certificate content assurance

A certificate translation service will in practice act as a CA. A CA usually takes certain measures to ensure that the information it puts into a certificate is correct. This typically includes measures to ensure that a claimed identity actually belongs to the claimant and that an entity that supplies a public key to be included in a certificate is also in possession of the corresponding private key. The effort a CA puts into ensuring the correctness of this information is usually defined either implicitly or explicitly in a certificate practice statement. A certificate translation service would have to rely on measures taken by other CAs for the purposes of verifying identity and validating public keys. The signature of the certificate that is to be translated, as well as any intermediate certificates required to form a certificate chain to a trusted root, have to be validated. A certificate translation service would have to publish its own certificate practice statement specifying under what circumstances a translated certificate will be produced.

3.2 Revocation

By translating a certificate the translator is in practice issuing a new certificate and therefore acting as a CA. If the original certificate is revoked the translated certificate should also be revoked. In certain environments and applications this problem can be tackled through giving translated certificates a minimal validity period. Where this is not possible, revocation must be dealt with in a proper way, just as in any other PKI.

If clients are going to be able to validate the status of the original certificate even when only in possession of the translated version, enough information must be provided in the translated certificate (or along with it) to validate it against certificate revocation lists, or any other means used to advertise revocations for certificates issued by the original CA. In the case where X.509 v3 [8] is used in the translated certificate and the original certificate is X.509 v1, v2, or v3 the issuer name and certificate serial number can be stored in an extension of the translated certificate in order to allow traceability of the original certificate.

3.3 Liability

A certification authority may place limitations on the use of its certificates, in order to control the risk that it assumes as a result of issuing certificates. For instance, it may restrict the community of certificate users, the purpose for which they may use its certificates and/or the type and extent of damages that it is prepared to make good in the event of a failure on its part, or that of its end-entities. These matters can be defined in a certificate policy.

It is most likely that by translating a certificate any liabilities undertaken by the original CA will no longer apply. For certain applications, or where the certificate policy refers to the public key rather than to the certificate as such, liabilities undertaken by the CA originally issuing a certificate might still apply. If the translating service is prepared to do so, it can issue translated certificates under similar policies as the original certificate was issued; otherwise it can issue the certificate using a more appropriate policy for the situation.

4 Applications for certificate translation

4.1 Translating between incompatible certificate types

Many types of certificates exist today. A few examples are: X.509 [8], X9.68, OpenPGP certificates [2], SPKI certificates [3], EMV certificates [4], and WTLS certificates [10]. Applications designed to use one type of certificate usually do not work very well with a different type of certificate. In some cases certificates are very application oriented and using a different type of certificate does not make any sense. For other applications different types of certificates are used for the same purpose, possibly in different domains. Under such circumstances translation of certificates from one format into another would allow entities using different types of certificates to communicate using the advantages of public-key cryptography and digital certificates.

4.2 Translating incompatible certificate fields

Although many PKIs make use of standard formats for certificates such as X.509 [8], this can still create problems since, as in the case of X.509, the standard supports extension fields that are not defined within the standard. Two different CAs can be issuing certificates carrying extensions with the same purpose but with different names. It is also possible that different CAs are issuing certificates carrying extensions with the same name and syntax but with different purposes.

4.3 Delegating path validation

If a client does not have sufficient processing or networking resources to perform path validation for each certificate it receives, path validation can be delegated to a certificate translation server. The CTS validates the certificate chain and issues a new certificate carrying the public key of the last certificate in the chain.

4.4 Centralised trust and policy management

For organisations requiring a centrally imposed policy and management function, it is unacceptable to allow a client to manage its own set of trusted roots, or the policies that it accepts during path validation. A certificate translation server can enforce policy decisions while performing path validation. After validating a certificate chain the certificate translation server can, if appropriate, issue a translated version of the last certificate in the chain, at the same time imposing restrictions regulated through its policy.

5 Scenarios

5.1 WAP

5.1.1 Need for certificate translation in WAP

WAP (Wireless Application Protocol) [9] is considered here as a possible application for which certificate translation could prove to be of advantage.

In WTLS (Wireless Transport Layer Security), the security protocol designed for WAP, certificates are used for server authentication as well as for client authentication when so requested. Digital certificates can also be used in WAP for key agreement [10]. The WAP specification specifies three supported formats of certificates and allows additional certificate types to be added in the future. The currently specified certificate types are X.509v3 [8], X9.68, and a WTLS certificate which is a certificate optimised for size.

WAP is intended to be used in a wireless environment using handheld devices with limited storage, processing resources and transmission bandwidth. Security parameters are negotiated during the WTLS handshake. This negotiation may also require transmission of certificates between server and client and vice versa. When certificates are known in advance no certificates need to be transmitted between the two parties. When a certificate is transmitted the sender indicates the type of certificate that it supplies. However, there is no way for the receiving party to indicate which type of certificate it prefers or understands. It must be assumed that in order to be compatible with this version of WTLS an implementation must cope with the three specified certificate types. A certificate chain can be transmitted along with a certificate. In a certificate chain, all certificates must use algorithms appropriate for the negotiated key exchange suite. E.g. if RSA has been selected all certificates must carry RSA keys signed with RSA.

5.1.2 Certificate translation in WAP

Certificate translation could be used in WAP in order to minimise the processing and storage requirements of certificates as well as to provide compatibility with other types of certificates besides those defined within the current WTLS specification.

When a WAP client receives a certificate with an unknown type it can simply forward it to a server that offers a certificate translation service. The certificate translation server interprets the certificate, validates it, and rewrites it in a format that the client has requested, putting its own signature on it. However, WAP is designed to be used in an environment where large time delays exist, and it is possible that a connection would time out during the time it takes for the WAP client to establish a session with a server that offers the translation service and has the certificate translated. This should not however lead to any serious complications. The client can initiate a new WTLS session and during this handshake indicate that it already has the server certificate. The corresponding scenario where a WAP server does not understand the client certificate type would work in the same manner.

Certificate translation could also be used to reduce the load on a handheld device with limited CPU resources. Every certificate that needs to be verified requires some computing resources. Given that a certificate chain can contain quite a few certificates and that the processing power on some handheld devices will be very limited it may be desirable to let a CTS do the computations required. By doing this, resource requirements will be shifted from CPU resources (on the handheld device) to bandwidth requirements, assuming that CPU resources at the CTS is not a problem. The CTS would, after receiving a certificate chain, verify the certificates and if it leads to a trusted root certificate create a new certificate. This new certificate would, according to our definition, be a translation of the last certificate in the chain. After receiving the translated certificate the user could store the translated certificate for future use, if applicable.

5.2 MExE

5.2.1 Need for certificate translation in MExE

MExE is considered here as another application where a certificate translation service could be advantageous.

MExE (Mobile Station Application Execution Environment), specified by 3GPP, provides a standardised execution environment for mobile stations (typically a mobile phone with a smart card). MExE specifies three security domains [1]:

- MExE security operator domain (MExE executables authorised by the HPLMN (Home Public Land Mobile Network) operator, i.e the operator to whose network the user has a subscription).

- MExE security manufacturer domain (MExE executables authorised by the terminal manufacturer).

- MExE security third party domain (trusted MExE executables authorised by trusted third parties).

Untrusted MExE executables are not in a specific domain, and have very reduced privileges. For each domain a root public key is installed in the MS (mobile station). In order for an executable to run it has to carry a signature that can be validated using root public keys and digital certificates (certificate chains are supported). An optional mechanism, involving storing a hash of the executable along with its expiry date/time in a protected verified application list, is defined to avoid complete signature verification each time an executable is run.

The MExE specification [1] mentions WTLS certificates and X.509 certificates but does not rule out other types of certificates.

5.2.2 Certificate translation in MExE

Just as for WAP, certificate translation can be used in MExE in order to minimise the processing and storage requirements of certificates as well as to provide compatibility with various types of certificates.

Since no certificate type is mandated for MExE it is possible that problems with incompatible certificate types will arise. Certificate translation can, in a very similar way as described for WAP, be used to overcome such obstacles.

The problem with recurrent signature validation of previously executed code has been taken care of through the verified application list as mentioned above. However, in cases where several applets are downloaded and executed from the same site they are likely to share the same certificate chain. A translated certificate can be used to shorten such a certificate chain in order to preserve CPU and memory resources. It is likely that an MS aware of multiple instances of signed code from the same site could do such a verification even more efficiently in terms of CPU resources. A certificate translation approach however could be more general and would not require the terminal to store any intermediate states or results and therefore would require less memory resources.

6 Extension to SCVP

The Simple Certificate Validation Protocol (SCVP) is currently an IETF draft [5]. The protocol allows a client to offload certificate handling to a server. The server can give a variety of information about a certificate, such as whether or not a certificate is valid, a chain to a trusted certificate, and so on. SCVP has many purposes, including simplifying client implementations and allowing companies to centralise their trust and policy management.

SCVP allows a client to request the status of a certificate. This requires applications using the SCVP service to be aware of the protocol. Applications designed before SCVP is finalised, or which for some other reason do not support SCVP, will not easily be able to make use of the SCVP protocol. If a certificate translation server were used instead, standalone software able to communicate with a CTS would be able to interact with existing software without any changes to the certificate using software. The certificate using software would have to load the CTS certificate as a trusted root CA certificate and certificates signed by the CTS would be valid. Such a solution would allow a company to centralise their trust and policy management, requiring minimal changes to existing systems.

Another advantage with a certificate translation solution over the current SCVP protocol is that only a certificate would need to be stored by the client, as opposed to SCVP where a certificate and associated status information need to be stored by the client if required for future use.

Since many features of SCVP are required or useful in a certificate translation service, certificate translation could be implemented as an extension to, or in combination with, SCVP.

7 Outline of a certificate translation protocol

7.1 Protocol overview

In this section we will outline a protocol for certificate translation. The protocol described is a standalone protocol in order to show how certificate translation can be implemented. As described in section 6 the protocol could be incorporated into another protocol. However, for environments with restricted bandwidth, having a dedicated protocol for the purpose is likely to reduce unnecessary communication overhead.

This protocol uses a simple request response model. That is, a client creates a single request and sends it to the server; the server creates a single response and sends it to the client. The client is assumed to be in possession of the CTS' digital certificate prior to the protocol taking place.

Certificate translation is expected to be of particular importance in environments, such as wireless, with limited bandwidth and where clients have restricted processing and memory resources. Hence, in order to keep the data sent over the communication path to a minimum, the CTS can keep a database of its clients and their preferences. This will minimise the information that is sent in every translation request. The server can, for example, store the preferred certificate type, client certificate, and possibly certain certificate field information that might be specific to a client.

7.2 Request

A translation request is made up of the following information, of which some will not always be required:

- Client identification
- Original certificate (certificate to be translated)
- Original certificate type
- New certificate type
- New certificate content
- Certificates for path validation
- Client certificate
- Client signature

We now consider each of these information types in a little more detail.

7.2.1 Client identification

Client identification is used to identify the client requesting translation. Identification can be used for things such as accounting, locating the client's certificate (if not supplied in the request), or to find client's preferences in a database if such a database exists. In environments where this information is not required, such as in a protected private network where the translation service is available to all connected users, and there is no need for the server to keep a user database of any kind, this information may well be omitted.

7.2.2 Original certificate

This is the certificate for which translation is requested. The complete certificate or a certificate identifier must be supplied as part of a certificate translation request.

7.2.3 Original certificate type

If known by client, the type of the certificate that is submitted for translation is indicated here. Since one purpose of the protocol is to enable clients not aware of a certain type of certificate to have certificates of that type translated into a known type, it must be assumed that the client is not always aware of the type of the certificate that is submitted for translation. The translation server should therefore be able to analyse the supplied certificate and make qualified conclusions regarding the supplied certificate type. In many environments where the translation service will be used for the purpose of translating from certificate types unknown to the client, the translation server can be configured to know which types of certificates its clients are aware of, not aware of, and likely to be requesting translation for. The certificate type field is also, when applicable, used to indicate certificate encoding, such as BER [6] or PER [7], if known by the client.

7.2.4 New certificate type

This field indicates the type of certificate, and encoding if applicable, that the client expects to receive back from the translation server.

7.2.5 New certificate content

This part allows the client to describe any specific information that needs to be included in the new certificate. The client can include the content of any fields it wishes to have included or may only indicate which fields are to be included in the new certificate and let the translation server get the information from the translated certificate. Another approach would be for the client to indicate the intended usage for the new certificate. The detailed specification of this particular section requires further research to allow enough flexibility without requiring too much overhead.

7.2.6 Certificates for path verification

Many protocols utilising digital certificates let the communicating parties include a certificate chain when exchanging certificates in order for the other party to verify the certification path. If the client receives such a certificate chain it can forward it to the translation server.

7.2.7 Client certificate

When the server is not expected to already be in possession of the requesting client's public key or is not able to retrieve it by other means, the client should also supply its digital certificate in the request in order to enable the server to validate the signature (see section 7.2.8).

7.2.8 Client signature

When the translation service need to be restricted to pre-registered clients only, when the service is being charged for, or when clients need to be held accountable for their translation requests for other reasons, the client signs the complete request.

7.3 Response

The certificate translation response is sent back to the client in response to its request. If the requested certificate translation failed the server returns an error code indicating why the request was not fulfilled. If the request was processed successfully a new translated certificate is returned to the client. Since the certificate will carry the translation server's signature, no further message authentication will be required in many cases. However, on occasions when the client who requested the translation will not be the end user, it is possible that the client will not be able to verify the certificate signature, and another signature would be required in the response to ensure that the message originates from the certificate translation server and has not been tampered with.

8 Conclusions

We have described the concept of certificate translation and how it can be used for different purposes. Not only can the concept prove useful to convert certificates of different types but it can also be particularly useful in wireless environments in order to preserve bandwidth, memory, and CPU resources. A protocol for certificate translation can be implemented as a standalone protocol or as an extension to, or in combination with, existing adjacent protocols. SCVP is a good candidate of an existing protocol that can be extended to incorporate certificate translation. In other environments a standalone protocol is more suitable to keep communications overhead to a minimum.

Future work will include development of a detailed protocol for the certificate translation service, based on a detailed analysis of requirements emerging from the requirements of mobile communications.

References

[1] 3GPP, 3G TS 23.057, 3rd Generation Partnership Project; Technical Specification Group Terminals; Mobile Station Application Execution Environment (MExE); Functional description; Stage2 (Release 1999), March 2000.

[2] Callas J. et al., OpenPGP Message Format, IETF RFC 2440, November 1998.

[3] Ellison C. et al., SPKI Certificate Theory, IETF RFC 2693, September 1999.

[4] EMV 4.0 Book 2, EMV Integrated Curcuit Card Specification for Payment Systems - Book 2: Security & Key Management, Version 4.0, EMVCo, LLC, 2000.

[5] Malpani A., Hoffman P., Simple Certificate Validation Protocol, Internet draft, 12 June 2000.

[6] ISO/IEC 8825-1:1998 / ITU-T X.690, Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1998.

[7] ISO/IEC 8825-2:1998 / ITU-T X.691 (1997), Information Technology - ASN.1 Encoding Rules: Specification of Packed Encoding Rules (PER), 1998.

[8] ISO 9594-8 / ITU-T X.509, Information Technology - Open Systems Interconnection - The Directory: Authentication framework, August 1997.

[9] WAP Forum, Wireless Application Protocol, Architecture Specification, 30 April 1998.

[10] WAP Forum, Wireless Application Protocol, Wireless Transport Layer Security Specification, 5 Nov 1999.