

Certificates and Secure Message Delivery

Overview

The *ATS 5822—2010 — E-Health Secure Message Delivery* (SMD) specification requires certificates for several different purposes.

There are many different types of certificates and they cannot all be used in the same way. Different purposes require different features in the certificate.

Some certificates, such as the existing *Medicare Location Certificates*, can be used for some of these purposes but they are not suitable for other purposes that SMD requires. The *NASH HPI-O Process Certificates* are designed to support all the purposes required by SMD. Until these NASH certificates are available, a mixture of different certificates will need to be used to completely support all modes of SMD.

This article describes what types of certificates SMD requires and where existing *Medicare Location Certificates* can and cannot be used.

What are certificates?

Certificates are credentials used in *Public Key Infrastructure* (PKI) to associate an identity with a public key.

Certificates are usually issued by a *Certificate Authority* (CA), who is a trusted third party. The Registration Authority checks the identity of the certificate owner before issuing the certificate to them. The user of the certificate trusts the Certificate Authority and hence will trust the certificates issued by them.

A certificate is represented by a file that contains: information to identify the certificate owner, additional information about the certificate owner, technical information about the certificate, and the owner's public key.

What types of certificates are there?

There are different types of certificates and they cannot be used interchangeably. The PKI certificates are defined by X.509v3 and related specifications, but the X.509v3 specification allows for many variations.

For the purposes of SMD, several significant technical differences need to be highlighted:

- What are the technical policies restricting the certificate's use? Can it be used for performing signing and/or encrypting?

- What additional information is available in the certificate? For example, domain names are needed for Transport Layer Security (TLS) server certificates.
- How is the certificate owner identified in the certificate? For example, does it contain a healthcare identifier?

These are the significant technical differences, but there are also other technical and non-technical differences between different types of certificates.

What does SMD use certificates for?

The Secure Message Delivery (SMD) specification requires certificates for its digital signing and encrypting operations. An implementation of SMD uses certificates for five different purposes:

- Signing the sealed payload.
Certificates need to be capable of digital signing.
- Encrypting the sealed payload.
Certificates need to be capable of key encipherment.
- TLS server authentication and session establishment.
Certificates should be capable of key encipherment and contain the server's domain name in the certificate.
- TLS client authentication.
Certificates must be capable of digital signing.
- WS-Security signing and encryption.
Certificates must be capable of both digital signing and key encipherment.

Types of certificates

Medicare Location Certificates

Current Medicare Location Certificates are issued as dual certificates: one certificate is for signing and a second certificate is for encryption.

The *signing certificate* is capable of digital signing, but cannot be used for encrypting. So it can be used for signing the sealed payload and for TLS client authentication; but cannot be used for any of the other three purposes.

The *encryption certificate* is capable of key encipherment, but cannot be used for digital signing and does not contain the server's domain name in it. So it can be used for encrypting the sealed payload; but cannot be used for any of the other four purposes.

Therefore, Medicare Location Certificates can be used for certain purposes in SMD, but they cannot be used for TLS server authentication nor for WS-Security signing and encryption. Different types of certificates would be required for those purposes.

Medicare Location Certificates identify the owner using their name and a Medicare issued "RA number". The Medicare RA number is a Medicare internal identifier, and is not suitable for use as a healthcare organization identifier.

The above has looked at only some of the technical constraints. It should be noted that Medicare Australia's policy currently do not support the use of those certificates for any purpose other than for communication with Medicare for the purposes of claiming.

Commercial certificates

Certificates can be purchased from a number of commercial vendors. They are usually sold as TLS certificates for securing Web pages, but they can also be used with SMD.

These certificates usually support digital signing and key encipherment. They contain the server's domain name in the certificate.

Commercial certificates could be used for all five purposes required by SMD, but there are disadvantages.

The disadvantage of commercial certificates is that they are provided by many different Certificate Authorities. Users will not know which ones to trust. Their issuing policies might not be up to the standard required for healthcare applications. They can also contain different additional information (i.e. they follow different certificate profiles), which means it is necessary to choose a suitable certificate vendor and ensure that implementations do not depend on any vendor specific information in the certificate. They can also be relatively expensive to purchase.

Commercial certificates identify the owner using a name. There is no reliable mechanism in the certificate for mapping those names into a healthcare provider organization.

NASH HPI-O Process Certificates

The NASH HPI-O Process Certificates will be a single certificate that supports both signing and key encipherment. It will also contain the

server's domain name in the certificate along with the owner's HPI-O number.

Therefore, the NASH HPI-O Process Certificate can be used for all five purposes required by SMD.

The NASH HPI-O Process Certificates identify the healthcare provider organization using their HPI-O number.

Conclusion

	Medicare signing	Medicare encrypting	Commercial certificate	NASH HPI-O Process
Payload sign	•		•	•
Payload encrypt		•	•	•
TLS client	•		•	•
TLS server			•	•
WS-Security			•	•
Single trusted issuer	•	•		•
Single profile	•	•		•
No/low cost	•	•		•
Healthcare ID				•

SMD has a range of different requirements for the certificates it uses.

The NASH HPI-O Process Certificates will meet all these requirements from SMD. When they become available, it will be possible to use a single certificate with SMD.

In the interim, SMD can be deployed using other certificates (or a combination of several other certificates). Deployments will need to address the deficiencies of these interim certificates: they will need to establish an agreement about which issuers are mutually trusted, how healthcare organizations are identified and how that identifier relates to the certificate.