General information about certificates

- 2021-05-10 - Comments (0) - Lasernet Developer FAQs

Lasernet can use certificates for the following purposes:

- Signing PDF files
- Signing emails (S/MIME)
- Encryption for secure data connections (SSL/TLS)
- Client authentication

Signing PDF files

PDF is the only file/document format that Lasernet can sign. Signing PDF files is done using the PDF Security modifier.

We recommend using a CDS certificate (Certified Document Services). CDS certificates are certified by Adobe and are automatically recognized as trusted parties when opening the signed PDF in Adobe Acrobat/Acrobat Reader.

A list of Adobe certified CDS certificate providers can be found in the Adobe knowledge base.

In order to use a CDS certificate with Lasernet, the certificate must be a server-based certificate for bulk signing (typically a company certificate). Certificates for individuals or desktop-based certificates normally require a PIN code for each signature and are therefore

not suited for use in Lasernet. The CDS certificate requires access to a Hardware Security Module (HSM) for storing the private key. An HSM device can either be acquired by the customer or possibly leased by a certificate provider.

Alternatively, any certificate designed for signing data can be used with Lasernet to sign PDF files. The drawback of using a non-CDS certificate is that it will not automatically be accepted as a trusted source, when the PDF is opened in Acrobat. The certificate must be a server-based certificate for bulk signing (typically a company certificate).

Signing emails (S/MIME)

Lasernet supports the signing of SMTP emails. To sign emails, you need a S/MIME certificate. These certificates are sometimes referred to as Secure Email Certificates. These are available from any respected certificate provider.

Encryption of secure data connection (SSL/TLS)

Lasernet supports encrypted connections in a number of scenarios, such as connections to and from HTTP, FTP and SMTP servers. Connection encryption is the most common use for certificates.

These certificates are normally referred to as SSL certificates and are available from any respected certificate provider.

Client authentication

Lasernet can use certificates for client authentication in the HTTP input and output ports.

Client certificates are typically used instead of the traditional username/password combination for authenticating against a service. When using a client certificate to connect to a remote server, you must use the certificate provided by the owner of the remote server.

Additional Information

Certificates intended for individuals or desktop-based certificates usually require the user to enter a PIN code for each signature/use and are therefore not suited for use in Lasernet. Certificates for use in Lasernet must be designed for server solutions. These kinds of certificates are often referred to as **Enterprise**, **Server-based,** or **Bulk** certificates.