Encryption and certificates for NGDX

Datenblatt | 27.03.2020

Encryption and certificates for NGDX

Motivation

Wherever business critical or sensitive data is exchanged digitally, security concerns are high and legal requirements are strict. Modern document exchange should therefore be encrypted and authenticated. In this way, sender and recipient are clearly verified and the documents cannot be tapped or changed during transmission.

Certificate handling often cumbersome

A glance at the key management for encrypted and authenticated e-mails reveals that this requires a high degree of knowledge on the part of the users in addition to the high effort involved in setting it up. The barriers to entry are therefore very high and the acceptance dwindles right at the beginning.

Encrypt the transport route, but how far does it go?

For a secure transmission of information it is often sufficient to encrypt the transport route. In telephony, however, the encryption is broken at each session border controller of the telephony provider and it is not clear whether it continues encrypted or unencrypted afterwards.

Authenticity of documents

During the transmission of information and documents, it is often not apparent whether the transmitted data has been manipulated, regardless of the encryption. Normally there is no complete check at the end of the transmission.

Document character and legal certainty

If a document is to be transmitted as such and not unformatted text and the sender has a clear proof of sending, the number of possible transmission variants is very small.

How is encryption done on NGDX?

NGDX uses both transport encryption (SRTP) and end-to-end content encryption (AES encryption of T.434 content).

The key exchange for transport encryption is done via TLS secured SIP messages. The key exchange for content encryption is based on asymmetric encryption and X.509 certificates.

An X.509 certificate with Tel URIs in a SAN extension (Subject Alternative Name) is used to authenticate the fax counterpart. This certificate can be signed by a certification authority.

If the software on the sending side detects Binary File Transfer (BFT), Error Correction Mode (ECM), polling and encryption by means of the receiving station's capabilities offered in the T.30-DIS message, an NGDX-capable receiving device is required and a document is first retrieved in the same telephone connection (fax polling). This document is a T.434 stream containing the X.509 certificate of the receiver's public key.

The certificate is checked according to adjustable rules (if the certification authority is trusted, the caller's telephone number matches). If the public key of the X.509 certificate is trusted, the generated session key is encrypted asymmetrically (RSA) for symmetric encryption with the public key.

Each document sent is cryptographically signed with the own private key. The documents are encrypted symmetrically (AES) with the session key. The cipher (ciphertext) of the documents and a JSON file with the cipher of the symmetric key, the signatures of the documents and the X.509 certificate of the own public key is sent in the T.434 transmission stream.

The receiving device can then check the certificate of the sending device. If it trusts the certificate, it can use its own private key to recover the AES session key and decrypt the documents. And it can verify the signature of the documents.

The certificate authority that signs NGDX X.509 certificates must verify that the organization requesting the certificate really has the phone numbers listed in the certificate. This is done, for example, by requesting a secret sent by fax to this number.

The procedure is secure as long as RSA and AES are secure, the certification authority is secure and verification calls from the certification authority to the applicant for the certificate cannot be diverted in the telephone network.

Certification Authority (CA)

NGDX uses X.509 certificates. Certificates are trusted if they are signed by a trusted certificate authority (CA).

However, NGDX is not based on domains but on telephone numbers. It must therefore be ensured that the telephone numbers used actually belong to the respective subscribers. For SAN certificates that contain a telephone URI, there are no processes at the known root CAs, because they mainly issue TLS certificates. So what can be done?

1. Use of self-signed certificates

These offer protection against eavesdropping or eavesdropping, as the data is encrypted. They do not protect against call forwarding attacks (a man-in-the-middle can decrypt) and do not provide verification of the identity of the remote peer.

2. Have telephone URI SAN certificates issued by the root CA of Ferrari electronic AG

Die Ferrari electronic AG hat Prozesse implementiert, um als Root-CA für Tel-URI-SAN-Zertifikate zu fungieren. Eine Root-CA zu sein, ist sehr anspruchsvoll und die Ferrari electronic ist nicht in der Lage, alle Standards und Industrievorschriften zu erfüllen, die für Zertifizierungsstellen gelten (siehe cabforum.org). Abhängig vom Schutz der privaten Schlüssel bietet diese Methode jedoch Schutz vor Lauschangriffen und Man-in-the-Middle-/Rufumleitungs-Angriffen und authentifiziert sowohl den Sender als auch den Empfänger.

3. Find a suitable root CA for signing telephone URI SAN certificates

If a public certification authority is willing to verify Tel-URIs, it can also issue NGDX certificates.

4. Setting up your own root CA and using telephone URI SAN certificates

Implement a separate certification authority for your company, your authority and distribute their root certificate within a closed user group. Because who can you trust better than yourself?

Procedure of Ferrari electronic AG for the issue of a certificate

As described above, Ferrari electronic AG does **not** meet the requirements for a Root CA. The following is a description of the implemented processes to enable you to make a confidence assessment.

The private key of the root CA's root certificate is stored outside of a computer in a Vault. The private key of an intermediate certificate signed by the root certificate is used for the actual signing of the end certificates. This means that the intermediate certificate can be revoked if it is compromised.

The device used to process Certificate Signing Requests (CSRs) is never connected to a network. The process is performed by a closed user group. However, the security level of the building does not exceed that of a normal office building. The certificate database is located on a computer with a permanently active network connection. In this way delivery and revocation lists can be implemented. Certificate revocation is performed using the CA database and the Online Certificate Status Protocol (OCSP).

Certificate request

- Install OfficeMaster Suite and connect SIP trunk
- Switch NGDX configuration to encrypted
- Ferrari electronic delivers a root certificate, which should be registered under Root CA.
- In the interface you can create a Self-Signed NGDX certificate. You will be asked to enter a phone number, this can also contain a wildcard at the end. This is useful in case of number blocks. This creates a private key, a Certificate Signing Request/CSR and a Self-Signed certificate. These can now be used for encryption - but do not yet have a signature from the CA.
- Please send the generated CSR file to us:

  pmc@ferrari-electronic.de

- We check the legitimacy of using your requested phone numbers and create a trustworthy certificate as root CA for these numbers.

