Verschlüsselung und Zertifikate bei NGDX

Datenblatt | 27.03.2020

Verschlüsselung und Zertifikate bei NGDX

Motivation

Überall dort, wo unternehmenskritische oder sensible Daten digital ausgetauscht werden, sind die Sicherheitsbedenken groß und die gesetzlichen Vorgaben streng. Der moderne Dokumentenaustausch sollte deshalb verschlüsselt und authentisiert erfolgen. Damit werden Sender und Empfänger eindeutig verifiziert und die Dokumente können während der Übertragung nicht abgegriffen oder verändert werden.

Zertifikatshandling oft umständlich

Ein Blick auf das Schlüsselverwaltung bei verschlüsselten und authentisierten E-Mails verrät, dass dies neben dem hohen Aufwand bei der Einrichtung auch ein hohes Maß an Wissen bei den Anwendern erfordert. Die Einstiegshürden sind damit sehr hoch und die Akzeptanz schwin-det gleich zu Beginn.

Transportweg verschlüsseln, aber wie weit reicht das?

Für eine sichere Übertragung von Informationen ist es oft hinreichend, den Transportweg zu verschlüsseln. Bei der Telefonie wird die Ver-schlüsselung aber an jedem Session Border Controller der Telefonie-Provider aufgebrochen und es ist nicht klar, ob es anschließend verschlüsselt oder unverschlüsselt weitergeht.

Echtheit von Dokumenten

Bei der Übertragung von Informationen und Dokumenten, ist es unabhängig von der Verschlüsselung oft nicht ersichtlich, ob die übertragenen Daten manipuliert wurden. Es erfolgt im Normalfall keine vollständige Prüfung zum Abschluss der Übertragung.

Dokumentencharakter und Rechtssicherheit

Soll ein Dokument als solches und nicht unformatierter Text übertragen werden und der Absender einen eindeutigen Sendenachweis vorliegen haben, ist die Anzahl der möglichen Übertragungsvarianten sehr gering.

Wie wird bei NGDX verschlüsselt?

NGDX nutzt sowohl Transportverschlüsselung (SRTP) als auch eine Ende-zu-Ende Inhaltsverschlüsselung (AES-Verschlüsselung der T.434 Inhalte).

Der Schlüsselaustausch für die Transportverschlüsselung erfolgt über TLS-gesicherte SIP-Nachrichten. Der Schlüsselaustausch für die Inhaltsverschlüsselung basiert auf asymmetrischer Verschlüsselung und X.509 Zertifikaten.

Zur Authentisierung der Faxgegenstelle wird ein X.509-Zertifikat mit Tel-URIs in einer SAN-Erweiterung (Subject Alternative Name) genutzt. Dieses Zertifikat kann von einer Zertifizierungsstelle signiert sein.

Falls die Software auf Sendeseite anhand der in der T.30-DIS-Nachricht angebotenen Fähigkeiten der Empfangsstelle Binärdatenaustausch (BFT, Binary File Transfer), Fehlerkorrekturmode (ECM, Error Correction Mode), Polling und Verschlüsselung erkennt, wird ein NGDX-fähiges Empfangsgerät vorausgesetzt und in der gleichen Telefonverbindung zuerst ein Dokument abgerufen (Fax-Polling). Dieses Dokument ist ein T.434 Strom, welcher das X.509 Zertifikat des öffentlichen Schlüssels des Empfangsgerätes enthält.

Das Zertifikat wird nach einstellbaren Regeln geprüft (wird der Zertifizierungsstelle vertraut, passt Telefonnummer des Anrufers). Falls der öffentliche Schlüssel des X.509-Zertifikats vertrauenswürdig ist, wird der generierte Sitzungsschlüssel für die symmetrische Verschlüsselung mit dem öffentlichen Schlüssel asymmetrisch verschlüsselt (RSA).

Jedes gesendete Dokument wird kryptografisch mit dem eigenen privaten Schlüssel signiert. Die Dokumente werden mit dem Sitzungsschlüssel symmetrisch (AES) verschlüsselt. Die Chiffre (Ciphertext) der Dokumente und eine JSON-Datei mit der Chiffre des symmetrischen Schlüssels, den Signaturen der Dokumente und dem X.509 Zertifikat des eigenen öffentlichen Schlüssels wird im T.434 Sendestrom versandt.

Das Empfangsgerät kann dann das Zertifikat des Sendegeräts prüfen. Falls es dem Zertifikat vertraut, kann es mit dem eigenen privaten Schlüssel den AES-Sitzungsschlüssel wiederherstellen und die Dokumente entschlüsseln. Und es kann die Signatur der Dokumente prüfen.

Die Zertifizierungsstelle, welche die NGDX-X.509-Zertifikate signiert, muss überprüfen, ob die die Ausstellung des Zertifikats beantragende Organisation wirklich über die im Zertifikat genannten Rufnummern verfügt. Die geht z.B. über die Abfrage eines per Fax an diese Nummer gesandten Geheimnisses.

Das Verfahren ist sicher, solange RSA und AES sicher sind, die Zertifizierungsstelle sicher ist und Verifizierungsanrufe von der Zertifizierungsstelle an den Antragsteller des Zertifikates nicht im Telefonnetz umgelenkt werden können.

Zertifizierungsstelle (CA)

NGDX nutzt X.509 Zertifikate. Zertifikaten wird vertraut, wenn sie durch vertrauenswürdige Zertifizierungsstelle (certificate authority, CA) signiert sind.

NGDX basiert jedoch nicht auf Domains, sondern auf Telefonnummern. Es muss also sichergestellt werden, dass die verwendeten Telefonnummern den jeweiligen Teilnehmern auch wirklich gehören. Für SAN-Zertifikate, die einen Telefon-URI enthalten, existieren bei den bekannten Root CAs keine Prozesse, da diese hauptsächlich TLS-Zertifikate ausstellen. Was kann also getan werden?

1. Verwendung selbstsignierter Zertifikate

Diese bieten Schutz gegen Abhören oder Lauschen, da die Daten verschlüsselt sind. Sie schützen nicht vor Angriffen durch Anrufumleitung (ein Man-in-the-Middle kann entschlüsseln) und bietet keine Überprüfung der Identität der Gegenstelle.

2. Lassen Sie Telefon-URI-SAN-Zertifikate durch die Root CA der Ferrari electronic AG ausstellen

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. Finden Sie eine geeignete Root-CA zum Signieren von Telefon-URI-SAN-Zertifikaten

Falls eine öffentliche Zertifizierungsstelle bereit ist, Tel-URIs zu überprüfen, kann diese auch NGDX Zertifikate ausstellen.

4. Eigene Root-CA aufbauen und Telefon-URI-SAN-Zertifikate verwenden

Implementieren Sie für Ihr Unternehmen, Ihre Behörde eine eigene Zertifizierungsstelle und verteilen Sie deren Stammzertifikat innerhalb einer geschlossenen Benutzergruppe. Denn wem können Sie besser vertrauen als sich selbst?

Verfahren der Ferrari electronic AG zur Ausstellung eines Zertifikats

Wie zuvor beschrieben erfüllt die Ferrari electronic AG die Anforderungen an eine Root CA **nicht**. Es folgt eine Beschreibung der implementierten Prozesse, um Ihnen eine Vertrauenseinschätzung zu ermöglichen.

Der private Schlüssel des Stammzertifikats der Root CA wird außerhalb eines Computers in einem Tresor gespeichert. Der private Schlüssel eines vom Stammzertifikat signierten Zwischenzertifikats wird für die eigentliche Signierung der Endzertifikate verwendet. Das bedeutet, dass das Zwischenzertifikat widerrufen werden kann, wenn es kompromittiert wird.

Das Gerät, das zur Verarbeitung von CSRs (Certificate Signing Requests) verwendet wird, ist nie mit einem Netzwerk verbunden. Der Prozess wird von einer geschlossenen Benutzergruppe durchgeführt. Das Sicherheitsniveau des Gebäudes geht jedoch nicht über das eines normalen Bürogebäudes hinaus. Die Zertifikats-Datenbank befindet sich auf einem Computer mit einer ständig aktiven Netzwerkverbindung. So können Liefer- und Sperrlisten implementiert werden. Der Widerruf von Zertifikaten wird unter Verwendung der CA-Datenbank und des Online Certificate Status Protocol (OCSP) durchgeführt.

Zertifikatsanforderung

- OfficeMaster Suite installieren und SIP-Trunk anbinden
- NGDX-Konfiguration auf verschlüsselt umstellen
- Ferrari electronic liefert ein Stammzertifikat aus, welches unter Root CA eingetragen sein sollte.
- In der Oberfläche können Sie ein Self-Signed NGDX Zertifikat erstellen. Sie werden aufgefordert eine Rufnummer anzugeben, diese kann am Ende auch eine Wildcard enthalten. Dies ist im Falle von Rufnummernblöcken sinnvoll. Dabei entsteht ein Private Key, eine Zertifikat-Signierungsanforderung (Certificate Signing Request/CSR) und ein Self-Signed Zertifikat. Diese können ab sofort für Verschlüsselung genutzt werden – haben aber noch keine Signatur der CA.
- Das erzeugte CSR-File schicken Sie uns an:

  pmc@ferrari-electronic.de

- Wir überprüfen die Rechtmäßigkeit zur Verwendung Ihrer angefragten Rufnummern und erstellen als Root CA ein vertrauenswürdiges Zertifikat für diese Nummern.

