NSW Zertifikats-Management

Stefan Bröhl / 14. Sitzung der NSW Technical Working Group – Februar 2021

NSW Zertifikats-Management

KISTERS

Überblick

Unser Ziel: Daten und Systeme vor unbefugten Zugriffen bestmöglich absichern

Wie erreichen wir das?

1. Einsatz eines Verschlüsselungsprotokolls (SSL/TLS) für eine **sichere Datenübertragung**
   - Abgesicherte Ende-zu-Ende-Kommunikation => **Transportverschlüsselung**
   - Workflow
     - Client authentisiert sich am Server & Server authentifiziert den Client
   - Inhalte eines SSL-Zertifikats
     - Inhaber, Aussteller, Ablaufdatum, öffentlicher Schlüssel und Prüfsummen/Signaturen

NSW Zertifikats-Management

KISTERS

Überblick

2. Doppelte Absicherung durch die Verschlüsselung von ein- und ausgehenden Requests
   - Zertifikate zur Signierung der Meldungen / Nachrichten
   - Workflow
     - SSP verschlüsselt (signiert) die ausgehenden Meldungen
     - NSW Schnittstelle entschlüsselt und überprüft die eingehenden Meldungen

     - NSW Schnittstelle verschlüsselt (signiert) ausgehende Nachrichten
     - SSP entschlüsselt und überprüft die eingehenden Nachrichten (Nachrichteneingang)

NSW Zertifikats-Management

KISTERS

Was ändert sich

1. **Transportsicherung** – nur noch ein SSL-Zertifikat für alle Systeme
   SSL-Clientzertifikate werden von KISTERS über den DFN-PKI Dienst[1] erstellt
   KISTERS benötigt keine Zertifikatsanfrage mehr!
   - Der SSP erhält von KISTERS eine passwortgeschützte p12-Datei per ZIP und das Passwort als PrivateBin[2] Link
   - Das öffentliche Zertifikat der CA kann vom DFN heruntergeladen werden
     https://www.pki.dfn.de/wurzelzertifikate/globalroot2/
2. **Signierung der Meldungen und Nachrichten** – ein Zertifikat für Staging (Training/Referenz) und ein Zertifikat für Produktiv.
   Der weitere Ablauf bleibt unverändert
   - Meldungen: Der SSP erstellt ein Zertifikat (Schlüsselpaar) und schickt Kisters das öffentliche Zertifikat. KISTERS importiert das öffentliche Zertifikat in die NSW Schnittstelle
   - Nachrichten: KISTERS erstellt ein Zertifikat (Schlüsselpaar) und schicket dem SSP das öffentliche Zertifikat. Der SSP importiert das öffentliche Zertifikat in sein Meldesystem

[1] https://www.pki.dfn.de/ueberblick-dfn-pki/ [2] https://privatebin.info/

NSW Zertifikats-Management

KISTERS

Vereinheitlichung Ablaufdatum

1. **Transportsicherung**
   1 Jahr gültig *(Vorläufiges Ablaufdatum immer am ersten Dienstag im März)*
   KISTERS erstellt SSL-Clientzertifikat über DFN-PKI Dienst
   1 Woche vor Ablauf erhält der SSP von KISTERS das neue SSL-Clientzertifikat
2. **Signierung der Meldungen/Nachrichten**
   3 Jahre gültig *(Vorläufiges Ablaufdatum immer am ersten Dienstag im Oktober)*
   Der SSP und KISTERS erstellen ein neues Zertifikat (Schlüsselpaar) zur Signierung der Meldungen/Nachrichten.
   2 Wochen vor Ablauf liegen dem SSP und KISTERS jeweils das öffentliche Zertifikat des Anderen vor
   Das öffentliche Zertifikat und die Signierungszertifikate des SSP und KISTERS werden zu einem festen Termin veröffentlicht. *(Vorläufig am letzten Dienstag im September)*

Für die konkreten Zeitpunkte verweisen wir auf die aktuelle Version des SLA.