Schnittstellenübergreifende Themen

Version 1.7

Zielsetzung und Inhalte des Info Dokumentes

Als Grundlage für die Entwicklung und den Betrieb der elektronischen Schnittstellen WBCI und S/PRI dienen die auf den Seiten des Arbeitskreises S&P die abgelegten Spezifikationen.

WBCI

https://ak-spri.de/informationen-zur-wbci/wbci-spezifikationen/

S/PRI

https://ak-spri.de/spri/spri-spezifikationen/

Neben den oben genannten Spezifikationen sind im Rahmen der Umsetzung und der Zertifizierung Themen zwingend zu beachten, welche einheitlich über alle Schnittstellen gelten. Dieses Dokument dient zur Regelung dieser Sachverhalte.

Für alle Dokumente und Spezifikationen im Arbeitskreis Schnittstellen & Prozesse wird ein zentrales Abkürzungsverzeichnis verwendet, welches unter folgenden Link zu finden ist:

https://ak-spri.de/arbeitskreis-und-arbeitsgruppen/glossar

Editoren:

André Rochlitzer-Marquier, Plusnet GmbH

Tel: +49 160 8837500

E-Mail: andre.rochlitzer-marquier@plusnet.de

Stephan Braune, 1&1

Tel: +49 721 91374 6638

E-Mail: stephan.braune@1und1.de

1. Beantragung eines ITU Carrier Codes (ICC)

Gemäß der technischen Spezifikation zu der WBCI- und S/PRI-Schnittstelle ist für die Kommunikation die Verwendung eines ITU Carrier Codes (ICC) zwingend notwendig. Der ICC dient dabei der eindeutigen Identifizierung des Schnittstellenkommunikationspartners.

Das Vorhandensein des Codes ist demnach auch eine Voraussetzung für den Konformitätstest.

Dieses Dokument dient als Information, wie ein solcher ICC zu beantragen ist. Die Beschreibung des ICC ist auf der Seite der ITU unter folgenden Link abrufbar:

http://www.itu.int/en/ITU-T/inr/forms/Pages/carrier.aspx

Die Liste der in Deutschland bereits vergebenen ICC ist unter folgenden Link abrufbar:

http://www.itu.int/oth/T020100004F/en

Um einen neunen ICC zu beantragen ist gemäß http://www.itu.int/oth/T0201 der folgende Prozess zu durchlaufen:

1. Ausfüllen des ITU Formblattes zur Beantragung des ICC

   https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/TechnischeNummern/ICC/ICC_Basepage.html

2. Das Formblatt ist beim Referat 118 der BNetzA einzureichen

   Bundesnetzagentur
   Referat 118 Nummernverwaltung
   Canisiusstr. 21
   55122 Mainz

   bzw.

   Bundesnetzagentur
   Referat 118 Nummernverwaltung
   Postfach 8001
   55003 Mainz

3. Die BNetzA leitet den Antrag (nach Prüfung) an die ITU weiter
4. Die Informationen über die Zuteilung erhält der Antragssteller im Anschluss von der ITU
5. Die Zuteilungen werden zusätzlich im „ITU-Newsletter" veröffentlicht/kommuniziert

Es wird empfohlen den ICC so früh wie möglich zu beantragen, da die Bearbeitungszeiten schwanken und einige Wochen bis zur Zuteilung vergehen können.

2. Signierung und Zertifikatsverwendung

Die Umsetzung der hier beschriebenen Anforderungen bezüglich der Sicherheit ist Voraussetzung für eine erfolgreiche Zertifizierung der entsprechenden Schnittstelle. Im Wirkbetrieb vereinfacht die dadurch erreichte Einheitlichkeit der Sicherheitsmaßnahmen, die Zusammenschaltung zwischen den Häusern signifikant.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) definiert folgenden Mindeststandard für die gesicherte B2B Kommunikation beim Einsatz elektronischer Schnittstellen:[1]

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.html

Für die Nutzung der vom Arbeitskreis Schnittstellen und Prozesse definierten elektronischen Schnittstellen, ergeben sich daraus folgende Anforderungen:

Die Vertraulichkeit der Kommunikation wird durch eine Verschlüsselung der Übertragung mittels HTTPS (TLS 1.2) abgesichert. Zunächst ist ausschließlich eine serverseitige Authentifizierung vorgesehen, das heißt, es müssen entsprechende X509-Serverzertifikate bei den Betreibern der Webservice- Schnittstelle installiert werden. Das SSL-Zertifikat muss vom Typ X509 Version 3, Algorithmus "SHA256 with RSA" sein, eine RSA-Key Schlüssellänge (öffentlicher Schlüssel) von mindestens 2048 Bit haben und von einem der auf der „Whitelist valider Zertifikate Anbieter“ aufgeführten Zertifizierungsdiensteanbieter ausgestellt worden sein. Das SSL-Zertifikat muss eine Gültigkeitsdauer von maximal 36 Monaten haben. Als zusätzliche Sicherheitsmaßnahme erfolgt eine Signierung des Inhaltes (body) und eventueller Attachments jeder SOAP-Message nach dem WS-Security-Standard auf der Basis eines X-509-konformen Zertifikates. Die beim Empfänger notwendigen X509- Version 3 konformen Zertifikate (Codierung DER (X.690)) zur Validierung der Signatur mit dem Algorithmus "SHA256 withRSA" dürfen selbstsigniert sein und können eine längere Laufzeit als 36 Monate haben. Der RSA-Key ist mit einer Schlüssellänge von mindestens 2048 Bit zu generieren.

Soweit technisch möglich (kein IP-Bezug) dürfen Zertifikate aus dem Konformitätstest auch für den Wirkbetrieb weiterverwendet werden sofern sie den genannten Anforderungen genügen. Zur Vermeidung von DoS-Attacken (Denial of Services) wird die Schnittstelle je Kunde nur für eine definierte IP-Adresse freigeschaltet.

Diese Vorgaben bilden den zurzeit aktuellen Sicherheitsstandard ab. Durch neue Entwicklungen, oder Angriffe auf die IT-Sicherheit kann es notwendig werden, auch kurzfristig den neusten Sicherheitsstandard auf die genannten Schnittstellen anzuwenden.

[1] Im Mai 2019 aktualisierte das BSI den Mindeststandard für den Einsatz des TLS Protokolls (Link) – Der empfohlene Einsatz von TLS 1.3 wird mit Stand Juni 2019, durch die noch geringe Verbreitung/Anwendung für elektronische Schnittstellen, vom Arbeitskreis Schnittstellen und Prozesse nicht vorgeschrieben.

Einsatz von Zertifikaten:

- Es wird empfohlen, dass für die SOAP und SSL Signierung getrennte Zertifikate genutzt werden („zwei Zertifikate Lösung“).
- Es werden Zertifikate, welche sowohl das SOAP als auch das SSL Protokoll signieren, ebenfalls unterstützt („ein Zertifikat Lösung“). Die Nutzung solcher Zertifikate wird nicht empfohlen.
- Die Nutzung von „Wildcard-Zertifikaten“ ist aufgrund von Sicherheitsbedenken nicht erlaubt.

Signierung der Zertifikate

- Für die SSL Verschlüsselung ist eine Selbstsignierung nicht zugelassen.
  Es ist ein Zertifizierungsdiensteanbieter gemäß Whitelist zu nutzen.
  Die Whitelist ist unter Ziffer 3 hinterlegt und gilt sowohl für WBCI und S/PRI als auch für die OSS und ESS Schnittstellen der WITA.

- Für die SOAP Signierung ist neben der Nutzung eines Zertifizierungsdiensteanbieters gemäß Whitelist auch eine Selbstsignierung zugelassen. Dieses gilt allerdings nur im Falle einer „zwei Zertifikate Lösung“. Darüber hinaus kann die SOAP Signierung auch mit dem SSL Zertifikat erfolgen (Siehe „ein Zertifikat Lösung“).

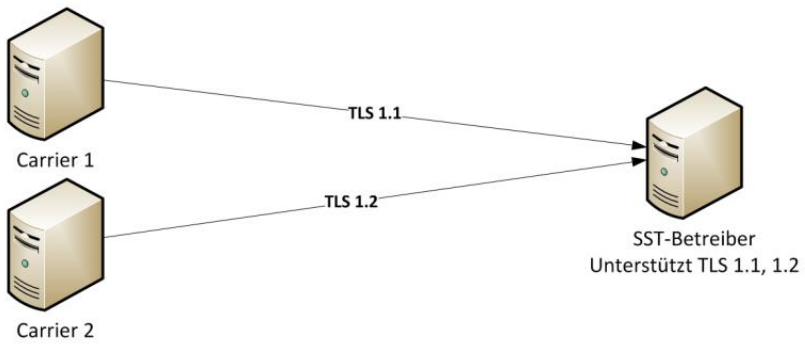
Migration und Umstellung

Im Falle von Migrationen oder Umstellungen, aufgrund ungenügender Sicherheitsmechanismen, wird der folgende Ablauf empfohlen (hier am Beispiel Umstellung von TLS 1.1 auf TLS 1.2):

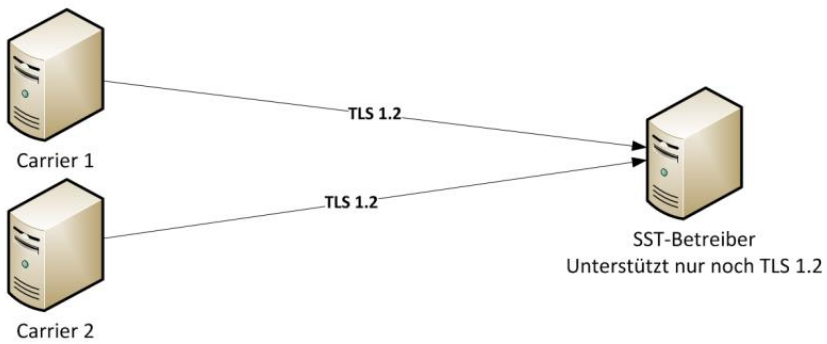
- SST-Betreiber muss die Unterstützung für ein neues Protokoll TLS 1.2 herstellen, ggf. sind dazu Software-Updates der Schnittstellen-Software und/oder des Betriebssystems notwendig.
- Die alte Protokollversion TLS 1.1 bleibt vorerst auf der Schnittstelle aktiv, ein Parallelbetrieb ist möglich, Client und Server handeln beim Verbindungsaufbau jeweils ein unterstütztes Protokoll aus.
- Alle Partner, die diese Schnittstelle nutzen, müssen auf die neue Protokollversion TLS 1.2 migriert werden.
- Nach Umstellung aller Partner wird auf der Schnittstellenseite das Protokoll TLS 1.1 deaktiviert.

Ablösung von Transportverschlüsselungsverfahren

IST:



SOLL:



3. Whitelist valider Zertifikate Anbieter

Stand Juli 2020

DigiCert	www.digicert.com
GeoTrust	www.geotrust.com DigiCert Gruppe
Thawte	www.thawte.com DigiCert Gruppe
RapidSSL	www.rapidssl.com DigiCert Gruppe
Sectigo	www.sectigo.com (ehemals Comodo)
Go Daddy	www.godaddy.com Go Daddy Gruppe
Starfieldt	www.starfieldtech.com Go Daddy Gruppe
GlobalSign	www.globalsign.com
SwissSign	www.swisssign.com
TeleSec	www.telesec.de
QuoVadis	www.quovadisglobal.de DigiCert Gruppe