

Zielsetzung und Inhalt des 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 abgelegten Spezifikationen.

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

S/PRI -> <https://ak-spri.de/spri/spri-spezifikationen/>

Neben den 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>

Inhalt

1. Beantragung eines ITU Carrier Codes (ICC)	2
2. Realisierung der sicheren Zusammenschaltung.....	3
2.1. Motivation	3
2.2. Geltungsbereich	3
2.3. Übertragungsweg	3
2.4. Sicherung der Übertragung	3
2.5. Sicherung der Inhalte nur für das SOAP-Protokoll	5
2.6. Einschränkung des Angriffsvektors	5
3. Migration und Umstellung	6
4. Whitelist valider Zertifikate Anbieter	7

Editoren:

André Rochlitzer-Marquier, Plusnet GmbH Tel.: +49 160 8837500 E-Mail: andre.rochlitzer-marquier@plusnet.de	Stephan Braune, 1&1 Telecommunication SE 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 neuen 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/Fachthemen/Telekommunikation/Nummerierung/ICC/start.html>

2. Das Formblatt ist beim Referat 114 der BNetzA einzureichen

Bundesnetzagentur
Referat 121 Nummernverwaltung
Canisiusstr. 21
55122 Mainz

bzw.

Bundesnetzagentur
Referat 121 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. Realisierung der sicheren Zusammenschaltung

2.1. Motivation

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

Die nachfolgend beschriebenen Vorgaben bilden den aktuellen Sicherheitsstandard ab und werden durch den Arbeitskreis in regelmäßigen Abständen überprüft und aktualisiert. Durch neue Entwicklungen oder Angriffe auf die IT-Sicherheit kann es notwendig werden, auch kurzfristig den neuesten Sicherheitsstandard auf die genannten Schnittstellen anzuwenden.

2.2. Geltungsbereich

Die nachfolgend beschriebenen Vorgaben sowie die unter Kapitel 4 referenzierte Whitelist gelten für alle im Arbeitskreis definierten Schnittstellen.

2.3. Übertragungsweg

Die Übertragung der Daten erfolgt über das Internet. Für die Kommunikation zwischen den Netzwerken mit verschiedener Hardwarearchitektur und Betriebssystemen wird das weitverbreitete Standardprotokoll TCP/IP verwendet.

2.4. Sicherung der Übertragung

Der Versand von Nachrichten und Inhalten **muss** mithilfe einer Transportverschlüsselung abgesichert werden. Zu diesem Zweck findet das Kommunikationsprotokoll HTTPS unter Einsatz von TLS-Zertifikaten Anwendung.

Der Arbeitskreis verweist hierbei auf das Bundesamt für Sicherheit in der Informationstechnik (BSI), welches den nachfolgenden Mindeststandard für die gesicherte B2B Kommunikation beim Einsatz elektronischer Schnittstellen definiert.

https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

Aus dem Arbeitskreis Schnittstellen und Prozesse ergeben sich folgende obligatorische Vorgaben an die Transportverschlüsselung:

Sicherheitsvorgaben Transportverschlüsselung	
Transportsicherheit	<ul style="list-style-type: none">• HTTPS (Mindestens TLS 1.2)• Port 443 (unbelegte Alternativen zulässig)
Zertifikatsvorgaben	<ul style="list-style-type: none">• Typ X.509• Version 3• Algorithmus "SHA256 with RSA"
Schlüssellänge	<ul style="list-style-type: none">• RSA-Key<ul style="list-style-type: none">○ Mindestens 3072 Bit○ bestehende Zertifikate mit 2048 Bit sind bis Laufzeitende gültig oder <ul style="list-style-type: none">• ECC-Key<ul style="list-style-type: none">○ Mindestens 256 Bit
Gültigkeitsdauer	<ul style="list-style-type: none">• Vorgabe durch CA geplant:<ul style="list-style-type: none">○ 2026 auf 200 Tage○ 2027 auf 100 Tage○ 2029 auf 47 Tage
Zertifikatsaussteller	<ul style="list-style-type: none">• Nutzung offizieller CAs aus unten ausgeführter Whitelist• selbstsignierte Zertifikate unzulässig

Auf Grund der reduzierten Gültigkeitsdauern durch die Zertifikatsaussteller (CA) wird empfohlen, dass Zertifikat Pinning nicht mehr anzuwenden. Stattdessen sollte nur den ausstellenden Root CAs vertraut werden. Somit ist für einen Wechsel des TLS-Zertifikates keine Anzeige gegenüber den Schnittstellenpartnern notwendig. Bei einem Wechsel des Zertifikatsanbieters empfiehlt es sich die Schnittstellenpartner vorab zu informieren.

2.5. Sicherung der Inhalte nur für das SOAP-Protokoll

Als zusätzliche Sicherheitsmaßnahme **muss** eine Authentifizierung durch Signierung des Inhaltes (Body) sowie eventueller Attachments jeder SOAP-Message gemäß WS-Security-Standard erfolgen. Basis hierfür ist ein X-509-konformes Zertifikat unter folgenden vom Arbeitskreis definierten Vorgaben:

Sicherheitsvorgaben Authentifizierung (Signierung)	
Signatursicherheit	<ul style="list-style-type: none">• WS-Security-Standard
Zertifikatsvorgaben	<ul style="list-style-type: none">• Typ X.509• Version 3• Algorithmus "SHA256 with RSA"
RSA-Key Schlüssellänge	<ul style="list-style-type: none">• Mindestens 3072 Bit• bestehende Zertifikate mit 2048 Bit sind bis Laufzeitende gültig
Gültigkeitsdauer	<ul style="list-style-type: none">• unbeschränkt
Zertifikatsaussteller	<ul style="list-style-type: none">• unbeschränkt (selbstsignierte Zertifikate zulässig)

Die **Empfehlung** lautet, zwei unabhängige Zertifikate gemäß der Sicherheitsvorgaben zu verwenden.

Die Nutzung von Wildcard-Zertifikaten ist technisch **zulässig**, wird aufgrund von Sicherheitsbedenken jedoch **nicht empfohlen**.

Soweit technisch möglich (kein IP-Bezug), **dürfen** Zertifikate aus dem Konformitätstest auch für den Wirkbetrieb weiterverwendet werden, sofern sie den zuvor genannten Anforderungen genügen.

2.6. Einschränkung des Angriffsvektors

Zur Vermeidung von DDoS-Attacken (Distributed Denial of Services) wird die Schnittstelle je Kunde nur für definierte Outbound-IP-Adressen freigeschaltet.

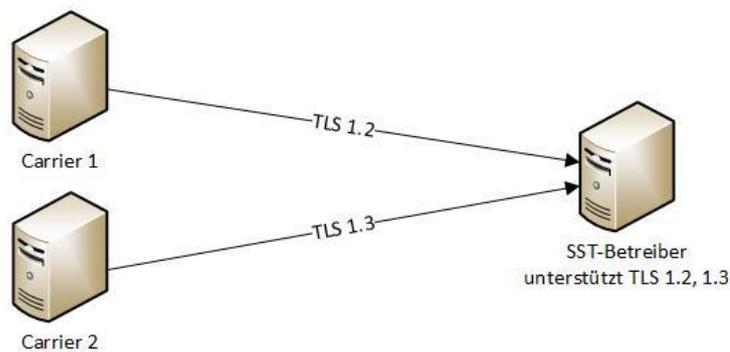
3. Migration und Umstellung

Im Falle von Migrationen oder Umstellungen, aufgrund ungenügender Sicherheitsmechanismen, wird der folgende Ablauf empfohlen (hier am Beispiel Umstellung von TLS 1.2 auf TLS 1.3):

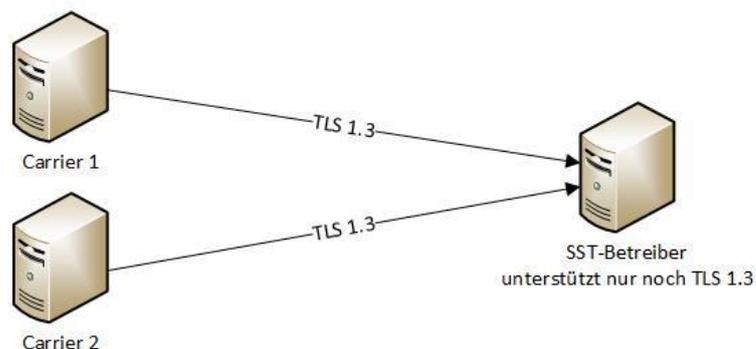
- SST-Betreiber muss die Unterstützung für ein neues Protokoll TLS 1.3 herstellen, ggf. sind dazu Software-Updates der Schnittstellen-Software und/oder des Betriebssystems notwendig.
- Die alte Protokollversion TLS 1.2 bleibt vorerst auf der Schnittstelle aktiv, ein Parallelbetrieb ist möglich, Client und Server handeln beim Verbindungsaufbau jeweils ein unterstütztes Protokoll aus.
- Alle Partner, die diese Schnittstelle nutzen, müssen auf die neue Protokollversion TLS 1.3 migriert werden.
- Nach Umstellung aller Partner wird auf der Schnittstellenseite das Protokoll TLS 1.2 deaktiviert.

Ablösung von Transportverschlüsselungsverfahren

IST:



SOLL:



4. Whitelist valider Zertifikate Anbieter

Stand Oktober 2025

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
Amazon	www.aws.com
Let's Encrypt	www.letsencrypt.org