



Erläuterungen zur Verwendung von Software-Zertifikaten

Wien, November 2023

Inhaltsverzeichnis

1	Allgemeine Informationen	3
2	Anforderungen an Software-Zertifikate	4
2.1.1	Zuordnung Software-Zertifikate zu einer Vertragspartnernummer.....	4
2.1.1.1	Produktivsystem	4
2.1.1.2	Testumgebung (VPSWH)	4
2.1.2	Technische Vorgaben.....	5
3	Zulieferung von Software-Zertifikaten	6
3.1.1	Produktivumgebung (PROD)	6
3.1.2	Testumgebung (VPSWH)	6
4	Dokumentationen.....	6
5	Erläuterungen zum Online-Formular	7

1 Allgemeine Informationen

Software-Zertifikate können von berechtigten GDA bzw. SW-Hersteller für die Authentifizierung gegenüber dem e-card System eingesetzt werden.

SW-Zertifikate können nur nach Freigabe durch die SVC verwendet werden. Es sind spezielle Security-Vorgaben zu erfüllen. Weitere Informationen erhalten Sie unter krankenanstalten@svc.co.at.

SW-Zertifikate können entweder anstatt der Admin-Karte oder auch in Kombination mit dieser verwendet werden. Die dem Zertifikat zugeordneten Admin-Karten behalten auch nach der Aktivierung von SW-Zertifikaten die volle Funktionsfähigkeit und können somit parallel zu den Zertifikaten verwendet werden.

Vor der Freigabe und Übermittlung von SW-Zertifikaten ist das Berechtigungsschreiben ausgefüllt und unterschrieben an krankenanstalten@svc.co.at zu senden.

Abgelaufene Zertifikate werden vom e-card System automatisch als ungültig vermerkt und können in Folge nicht mehr verwendet werden. Die Verantwortung zur Überprüfung des Ablaufdatums und das rechtzeitige Einmelden neuer, gültiger Zertifikate obliegt dem Aussteller!

Abgelaufene bzw. nicht mehr verwendete Zertifikate müssen widerrufen werden.

2 Anforderungen an Software-Zertifikate

2.1.1 Zuordnung Software-Zertifikate zu einer Vertragspartnernummer

2.1.1.1 Produktivsystem

Einem Software-Zertifikat kann genau eine Vertragspartnernummer (VPNR) zugeordnet werden. Es ist die Haupt-Vertragspartnernummer, für die das Zertifikat gelten soll, anzugeben. Es werden automatisch alle Bezugs-VPNR (z.B. für Abteilungen, Stationen, Ambulanzen usw.) – wenn vorhanden – diesem Zertifikat zugeteilt.

Aus dem Filenamen des Zertifikats muss erkennbar sein, für welche VPNR es ausgestellt wurde.

Software-Zertifikate in Krankenanstaltenverbänden

- In Verbänden mit mehreren Häusern muss pro Haupt-VPNR (pro Haus) ein Zertifikat angemeldet werden.
- Das KIS muss alle SW-Zertifikate verwalten.
- Ein SW-Zertifikat pro Haus ist ausreichend, auch wenn die Abteilung (Bezugs-VPNR) bei der Applikation angegeben werden muss (Verwaltung durch KIS).

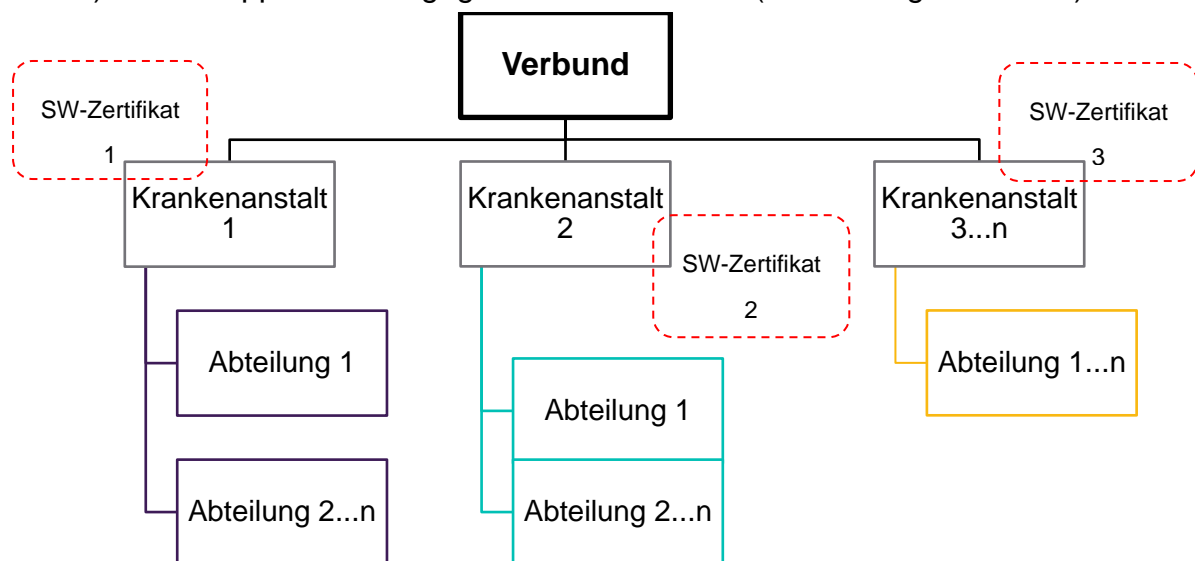


Abbildung 1: Darstellung der Verwendung von Software-Zertifikate in Krankenanstaltenverbänden mit mehreren Häusern.

2.1.1.2 Testumgebung (VPSWH)

Ein Zertifikat für die Testumgebung (VPSWH) muss einer VPNR der gelieferten Pseudo-Admin-Karte zugeordnet werden. Es dürfen keine produktiven VPNR verwendet werden. Aus dem Filenamen des Zertifikats muss erkennbar sein, für welche VPNR es ausgestellt wurde.

In der Testumgebung gibt es keine hierarchische Struktur, jedes Zertifikat gilt für eine bestimmte VPNR.

2.1.2 Technische Vorgaben

Es gelten (sowohl für PROD, als auch VPSWH) Vorgaben hinsichtlich folgender Parameter:

- **VPNR** (Vertragspartnernummer)
 - PROD: Es ist die Haupt-VPNR einzutragen. Damit werden alle Bezugs-VPNR automatisch für dieses Zertifikat freigegeben. Aus dem Filenamen des Zertifikats muss erkennbar sein, für welche VPNR es ausgestellt wurde.
 - VPSWH: In der Testumgebung gibt es keine hierarchische Struktur; jedes Zertifikat gilt für eine bestimmte VPNR. Aus dem Filenamen des Zertifikats muss erkennbar sein, für welche VPNR es ausgestellt wurde.

- **Algorithmus**

Es sind die folgend angeführten Parameter einzuhalten.

Parameter	Wert
Zertifikats-Signaturalgorithmus	SHA224/RSA, SHA256/RSA, SHA384/RSA, SHA512/RSA
Zertifikats-Schlüsseltyp	RSA
Schlüssellänge Min.	2048
Schlüssellänge Max.	4096
Anwendungs-Signatur	vgl. Zertifikats-Signaturalgorithmus
Anwendungs-Digest	SHA224, SHA256, SHA384, SHA512

- **Antragsteller**

Aus den Parametern für den Antragsteller muss erkennbar sein, für welche Organisation/Krankenanstalt und für welche Haupt-VPNR das Zertifikat ausgestellt wurde.

Hinweis: Es dürfen keine Sonderzeichen und Umlaute verwendet werden.

- **Gültigkeitsdauer**

Ein SW-Zertifikat darf maximal 5 Jahre gültig sein.

- **Zertifikat Antragsteller - DN**

Aus den Parametern für den Antragsteller muss erkennbar sein, für welche Organisation/Krankenanstalt und für welche Haupt-VPNR das Zertifikat ausgestellt wurde.

Aus dem Filenamen des Zertifikats muss erkennbar sein, für welche VPNR es ausgestellt wurde.

Die im Zertifikat verwendeten Distinguished Names (Subject, Issuer) dürfen nur folgende, in RFC 1779 (A String Representation of Distinguished Names) definierten RDNs enthalten:

Key	Attribute (X.520 keys)
CN	CommonName
L	LocalityName
ST	StateOrProvinceName
O	OrganizationName
OU	OrganizationalUnitName
C	CountryName
STREET	StreetAddress

Hinweis: Die Verwendung einer E-Mail-Adresse beim Antragsteller oder Aussteller des Zertifikats mit dem X.520 Attribute E ist nicht erlaubt.

Es dürfen keine Sonderzeichen und Umlaute verwendet werden.

3 Zulieferung von Software-Zertifikaten

3.1.1 Produktivumgebung (PROD)

Das Einmelden bzw. der Widerruf von Software-Zertifikaten erfolgt **durch die Organisation/Krankenanstalt über das Web-Formular**. An die SVC müssen die **Public-Keys** (das Zertifikat) zur Registrierung übergeben werden. Das Zertifikat muss digital im Format *.CER als zip-File über das Web-Formular gesendet werden.

Hinweis: Es werden nur Zertifikate von dafür berechtigten Personen in das e-card System eingespielt. Zur Bestätigung der einmeldeberechtigten Personen muss das Berechtigungsschreiben ausgefüllt und unterschrieben an krankenanstalten@svc.co.at übermittelt werden.

3.1.2 Testumgebung (VPSWH)

Bei Zertifikaten für die Testumgebung erfolgt die Registrierung durch den Softwarehersteller oder durch die testende Organisation/Krankenanstalt.

Die Bedingungen sind ident zu denen für das Produktivsystem.

4 Dokumentationen

Eine Hilfestellung zur Erstellung selbstsignierter SW-Zertifikate ist auf www.chipkarte.at im Abschnitt „Erstellung selbstsignierter SW-Zertifikate“ unter folgendem [Link](#) zu finden.

5 Erläuterungen zum Online-Formular

Voraussetzung für die Einmeldung bzw. den Widerruf von SW-Zertifikaten ist **eine Handy-Signatur**. Die einmeldeberechtigte Person, welche im Berechtigungsschreiben angegeben wurde, muss sich mit der Handy-Signatur authentifizieren.

Nachfolgend eine Erklärung zur Befüllung des Formulars:

Schritt 1:

< ZURÜCK

<div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; align-items: center;"> <h3 style="margin: 0;">Login mit Handy-Signatur</h3> </div> <div style="margin-top: 10px;"> <p>Mobiltelefonnummer</p> <input style="width: 90%; border: 1px solid #ccc;" type="text" value="Handynummer mit Vorwahl (z.B.: +43...)"/> </div> <div style="margin-top: 5px;"> <input style="width: 90%; border: 1px solid #ccc;" type="password" value="Signatur Passwort"/> </div> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> Abbrechen Identifizieren </div> <div style="margin-top: 5px;"> Eigenes Fenster </div> </div>	<p>Wie komme ich zu einer Handy-Signatur?</p> <p>Mit der Handy-Signatur können Sie einfach, schnell und kostenlos Ihre Identität im Internet nachweisen. Damit sorgen wir dafür, dass Ihre Daten sicher sind und niemand anderer Zugriff darauf hat.</p> <p>Beim Anmelden für Online Services der Sozialversicherung oder als elektronische Unterschrift nutzen Sie die Handy-Signatur: Alles was Sie dafür benötigen, ist ein empfangsbereites Mobiltelefon. Die Aktivierung und die Nutzung der Handy-Signatur sind kostenlos. Danach können Sie alle Online Services der Sozialversicherung und anderer Anbieter nutzen.</p> <ul style="list-style-type: none"> Online Handy-Signatur beantragen Online über Finanz-Online freischalten Online über die Website der Post Registrierungsstellen in Ihrer Nähe 	<div style="text-align: center; margin-bottom: 20px;"> <p>SERVICES FÜR VERSICHERTE</p> </div> <div style="text-align: center;"> <p>SERVICES FÜR UNTERNEHMEN</p> </div>
<div style="display: flex; align-items: center;"> <p>Benutzername und Kennwort eingeschränkter Zugriff</p> </div>	<div style="display: flex; align-items: center;"> <p>Unternehmensservice Portal</p> </div>	<div style="display: flex; align-items: center;"> <p>eIDAS Europäische Signatur</p> </div>

Schritt 2:

Befüllung der Pflichtfelder (*)

Hilfestellungen zur Befüllung erhalten Sie unter

SW-Zertifikat als Admin-Karten Ersatz

Dieses Formular ermöglicht die Einmeldung und den Widerruf von Software(SW)-Zertifikaten, die von berechtigten GDAs für die Authentifizierung gegenüber dem e-card-System eingesetzt werden können.



[Ausfüllhilfe](#)

Organisation

Organisation (Verbund/KA) *

Personendaten

Titel (vor)
 Vorname *
 Familienname *
 Titel (nach)

Kontaktdaten

Telefon *
 E-Mail *

Zwischenspeichern

Daten laden

Weiter

Abbrechen

Befüllung der Pflichtfelder (*)

Auswahl, ob

- Einmeldung oder Widerruf
- für Produktiv oder Test Instanz

Pro Antrag dürfen entweder nur Einmeldungen oder nur Widerrufe durchgeführt werden.

Ein Antrag kann jeweils entweder nur die Produktiv- oder nur für die Testinstanz betreffen.

Hilfestellungen zur Befüllung erhalten Sie unter 

SW-Zertifikat als Admin-Karten Ersatz



 [Ausfüllhilfe](#)

Einmeldeart

Einmeldeart *

Einmeldung von SW-Zertifikaten

Widerruf von SW-Zertifikaten

Art des SW-Zertifikat

Zertifikat für: *

Produktiv Instanz

Test Instanz

Zwischenspeichern

Zurück

Abbrechen

Weiter

Befüllung der Pflichtfelder (*) inkl. Hinzufügen des/der Zertifikats/e (max. 20 Stück)

Hilfestellungen zur Befüllung erhalten Sie unter .

SW-Zertifikat als Admin-Karten Ersatz



[Ausfüllhilfe](#)

Es werden ausschließlich die Public-Keys (das Zertifikat) übergeben (keine Private-Keys). Das Zertifikat ist als Attachment im Format *.CER in einer ZIP-Datei ohne Unterverzeichnisse hochzuladen. Das SW-Zertifikat muss folgenden Kriterien entsprechen:

- Algorithmus: RSA/SHA256
- Schlüssellänge: 2048 Bit (max. 4096 Bit)
- Schlüsselalgorithmus: RSA
- Gültigkeit: max. 5 Jahre
- VPNR muss im Dateinamen der ZIP-Datei enthalten sein

Dateidaten zum SW-Zertifikat (Produktive Umgebung)

Vertragspartnernummer *	<input type="text"/>	
Fingerprint *	<input type="text"/>	
Seriennummer *	<input type="text"/>	
DN des Zertifikats *	<input style="height: 80px;" type="text"/>	
Ablaufdatum *	<input type="text"/>	
Zertifikat (.zip) *	<input type="text" value="keine Datei ausgewählt"/> Beilage hinzufügen	

1

Weiteren Datensatz hinzufügen

Sie können noch weitere 19 Datensätze hinzufügen.

Kontrollseite als letzter Überblick vor dem Absenden

Kontrollseite

Bitte überprüfen Sie nun nochmals die unten stehenden Angaben. Sollten Korrekturen notwendig sein, können Sie mit "Zurück" wieder zurückblättern. Wenn Ihre Angaben korrekt und vollständig sind, können Sie die Antragsdaten mit "Senden" absenden.

Kontaktdaten
Einmeldeart
SW-Zertifikat
Testversand
Kontrolle
Abschluss

Identifikation

PEID 3577020982

Organisation

Organisation (Verbund/KA) Krankenhaus

Personendaten

Vorname Max
 Familienname Mustermann

Kontaktdaten

Telefon 01/723025/2589
 E-Mail krankenanstalt@ka.at

Einmeldeart

Einmeldeart Einmeldung von SW-Zertifikaten

Art des SW-Zertifikat

Zertifikat für: Produktiv Instanz

Dateidaten zum SW-Zertifikat (Produktive Umgebung)

Vertragspartnernummer 123456
 Fingerprint b585858a4394949b39393c393939
 Seriennummer 407f11158795213347810324
 DN des Zertifikats CN = Krankenhaus OU = 123456 O = Verbund L = Stadt S = Bundesland C = AT
 Ablaufdatum 09.08.2023
 Zertifikat (.zip) g1_Beilage001.zip

Zwischenspeichern

Zurück

PDF-Ansicht

Senden

Abbrechen

Abgelaufene Zertifikate werden vom e-card System automatisch als ungültig vermerkt und können in Folge nicht mehr verwendet werden. Die Verantwortung zur Überprüfung des Ablaufdatums und das rechtzeitige Einmelden neuer, gültiger Zertifikate obliegt dem Aussteller!

Abgelaufene bzw. nicht mehr verwendete Zertifikate müssen widerrufen werden.