designing e-health

Erläuterungen zur Verwendung von Software-Zertifikaten

Wien, November 2023

ecard

SVG

Inhaltsverzeichnis

1 Allgemeine Informationen

Software-Zertifikate können von berechtigen 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 Krankenanstaltenverbünden

- In Verbünden 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).

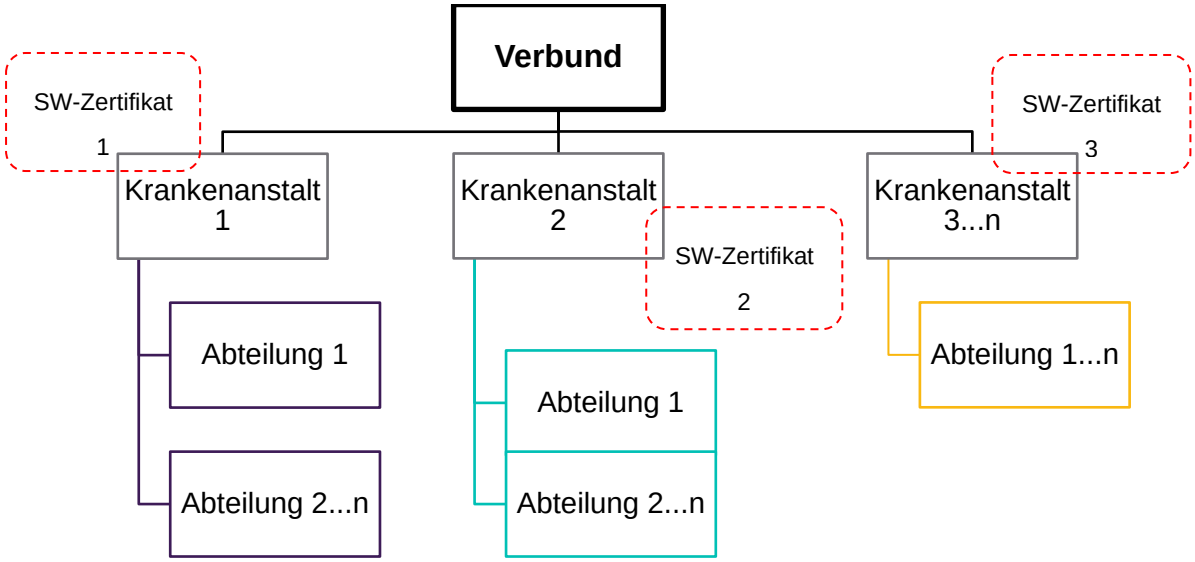


Abbildung 1: Darstellung der Verwendung von Software-Zertifikate in Krankenanstaltenverbünden mit mehreren Häusern.

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

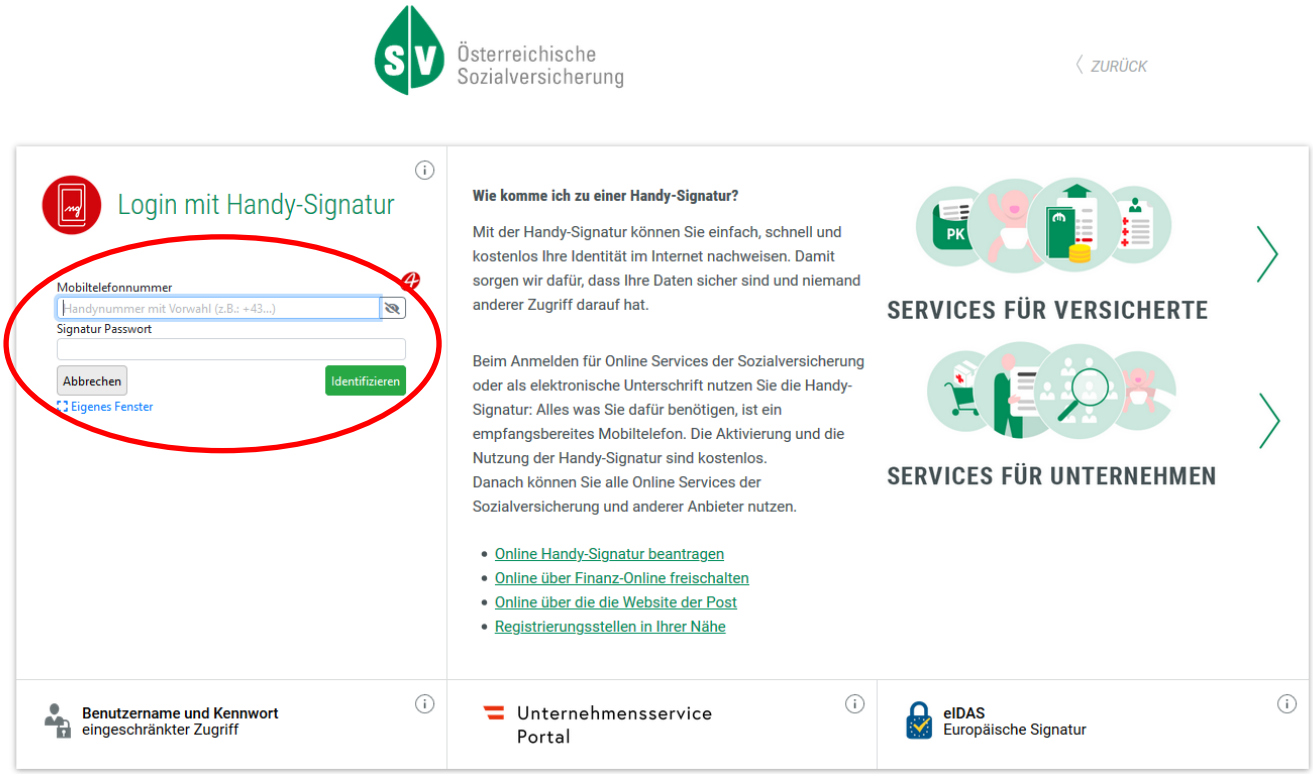
Eine Hilfestellung zur Erstellung selbstsignierter SW-Zertifikate ist auf www.chipkarte.at im Abschnitt „Erstellung selbstsignierter SW-Zertifikate“ unter folgendem Link zu finden.

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:

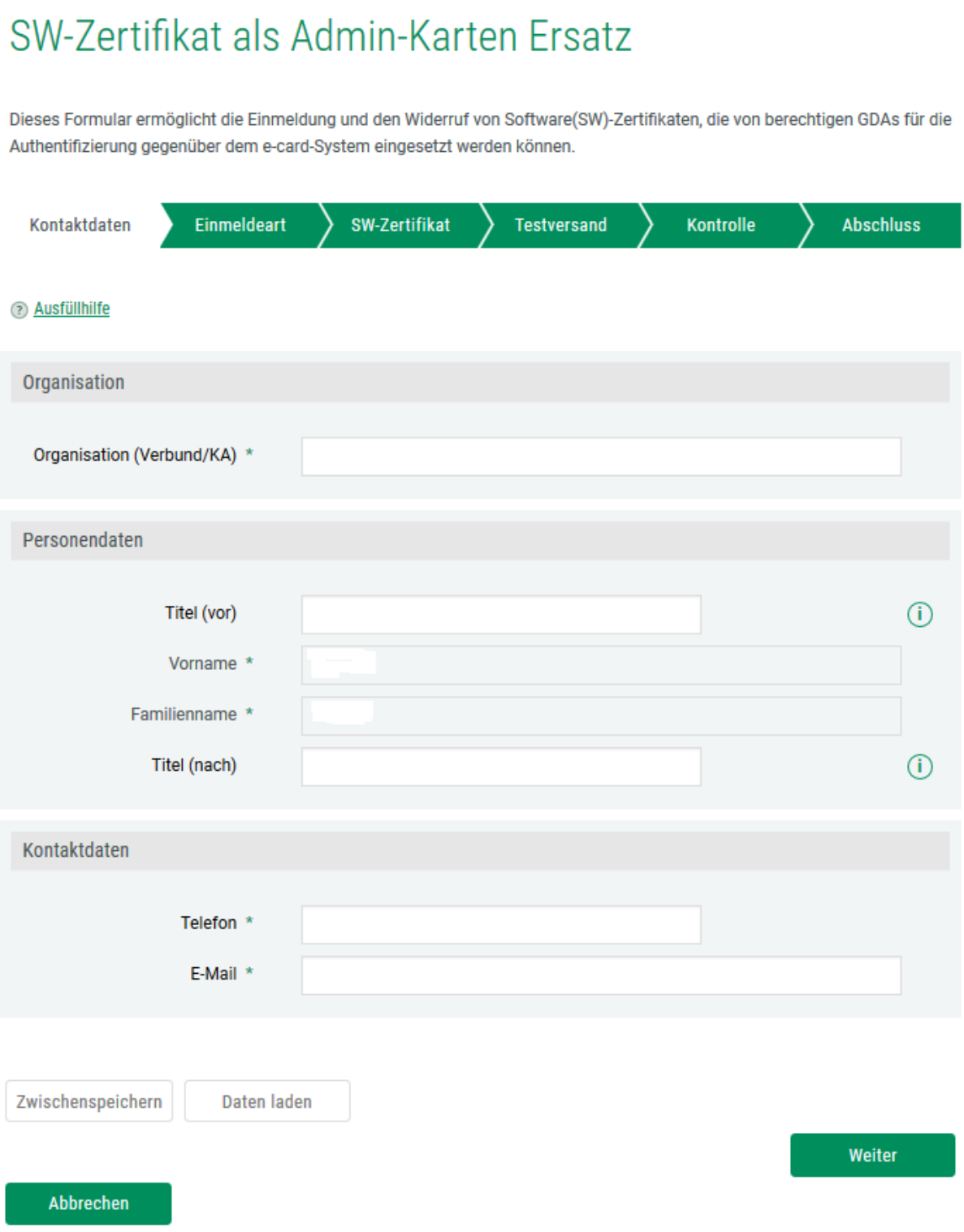
Schritt 1:



Schritt 2:

Befüllung der Pflichtfelder (*)

Hilfestellungen zur Befüllung erhalten Sie unter ⓘ



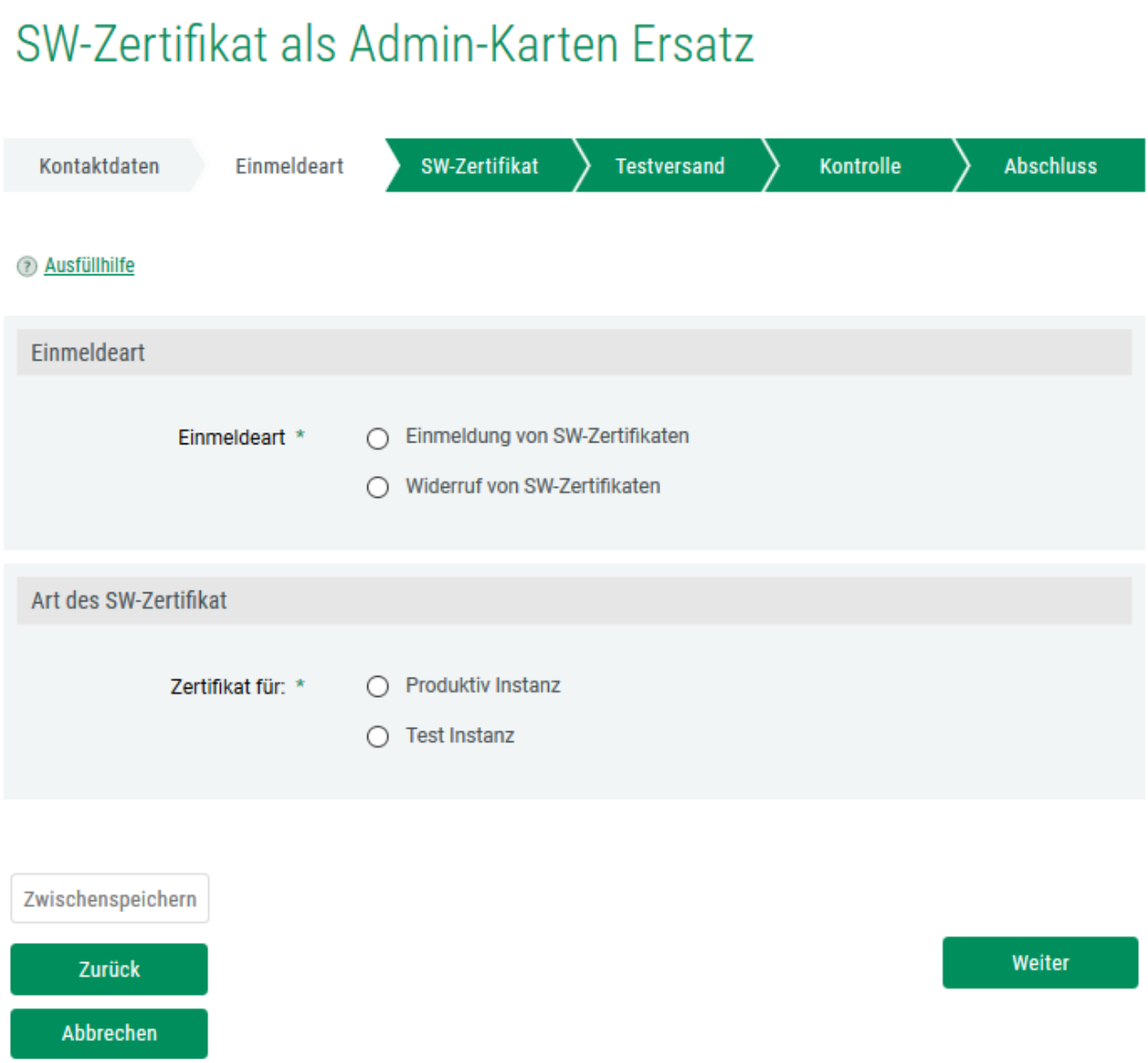
Befüllung der Pflichtfelder (*)

Auswahl, ob

- Einmeldung oder Widerruf
- für Produktiv oder Test Instanz

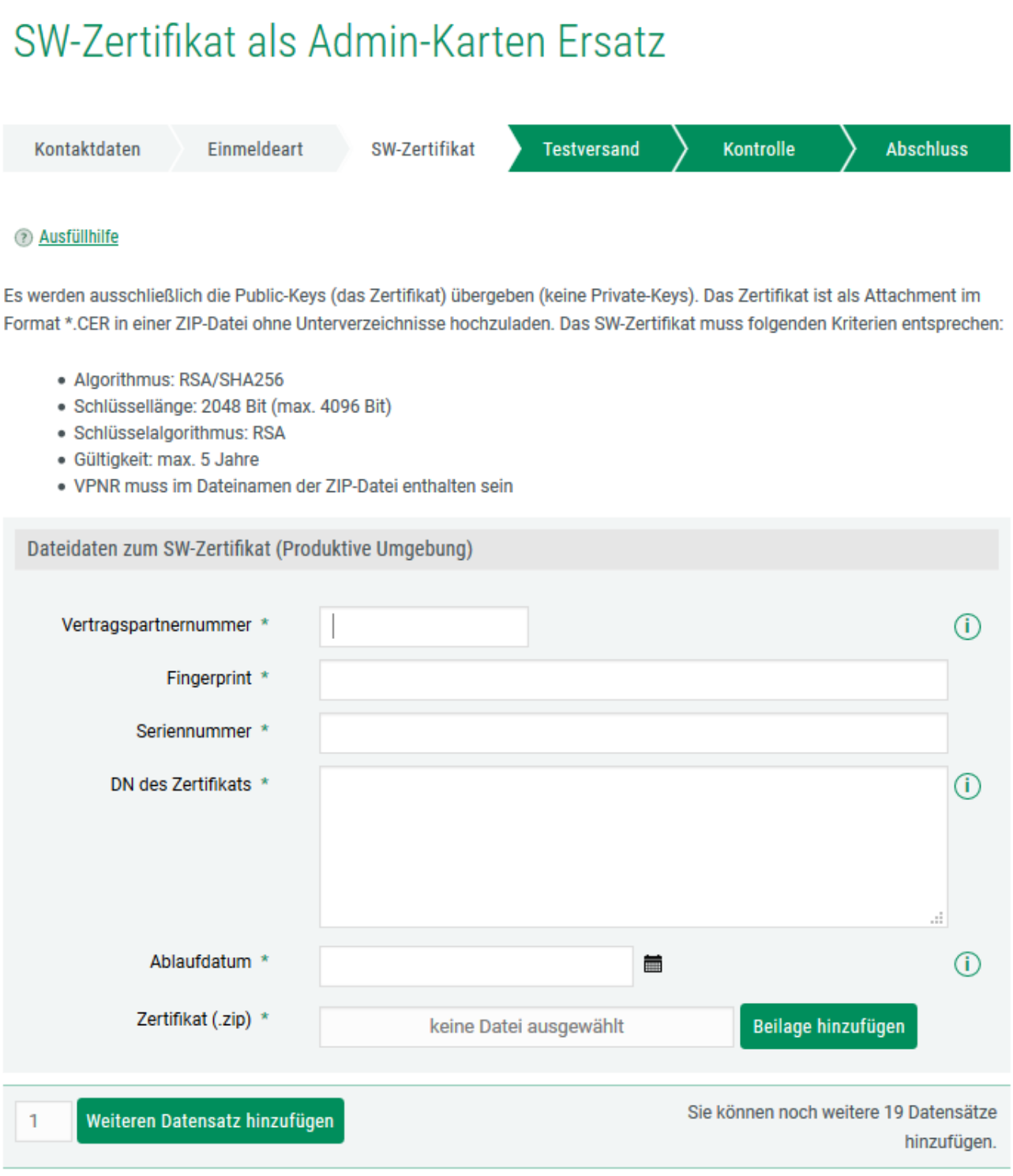
Pro Antrag dürfen entweder nur Einmeldungen oder nur Widerrufe durchgeführt werden.
Ein Antrag kann jeweils entweder nur die Produktiv- oder nur für die Testinstanz betreffen.

Hilfestellungen zur Befüllung erhalten Sie unter 



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

Hilfestellungen zur Befüllung erhalten Sie unter ⓘ .



Kontrollseite als letzter Überblick vor dem Absenden

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