

# Bestellung einer SwissSign Managed Public Key Infrastructure **MPKI-EV**

## Kunde



Gemäss (Handels-)Registereintrag aus dem staatlichen Register des jeweiligen Landes

## Verrechnungsadresse

Verrechnungsadresse von Kunde übernehmen

# Produktbestellung: Die Preise verstehen sich in

pro Jahr exklusiv MwSt.

 Bitte beachten Sie, dass für die MPKI EV Bestellung ein **Mindestbetrag von EUR 1'000.– pro Jahr** in Rechnung gestellt wird.

	Anzahl	Einzelpreis	EUR
<b>DV</b>	<b>SSL Silver</b> domainvalidiert   optional www	<input type="text"/>	<input type="text"/>
	<b>SSL Silver Wildcard</b> domainvalidiert   für alle Subdomains	<input type="text"/>	<input type="text"/>
	<b>E-Mail ID Silver</b> E-Mail domainvalidiert   Haftung bis max. EUR 10'000.–	<input type="text"/>	<input type="text"/>
<b>OV</b>	<b>SSL Gold</b> organisationsvalidiert   optional www	<input type="text"/>	<input type="text"/>
	<b>SSL Gold Wildcard</b> organisationsvalidiert   inkl. Subdomains	<input type="text"/>	<input type="text"/>
	<b>SSL Gold Multi-Domain (20)</b> organisationsvalidiert   max. 20 SAN (Subject Alternative Name) Einträge   mit/ohne www	<input type="text"/>	<input type="text"/>
	<b>E-Mail ID Gold</b> E-Mail- und organisationsvalidiert   Name   Vorname   E-Mail   Organisation   Ort   auch zur Authentisierung geeignet   Haftung bis max. EUR 100'000.–	<input type="text"/>	<input type="text"/>
	<b>E-Mail ID Gold ohne Authentisierung</b> E-Mail- und organisationsvalidiert   Name   Vorname   E-Mail   Organisation   Ort   Haftung bis max. EUR 100'000.–	<input type="text"/>	<input type="text"/>
	<b>E-Mail ID Gold (RSASSA-PSS)</b> E-Mail- und organisationsvalidiert   Name   Vorname   E-Mail   Organisation   Ort   auch zur Authentisierung geeignet   Haftung bis max. EUR 100'000.–	<input type="text"/>	<input type="text"/>
<b>EV</b>	<b>SSL Gold EV</b> Extended Validation, optional www	<input type="text"/>	<input type="text"/>
	<b>SSL Gold Multi-domain EV (20)</b> Extended Validation, max. 20 SAN Einträge, mit/ohne www	<input type="text"/>	<input type="text"/>
Zertifikatspreise			<input type="text"/>
Volumenrabatt		<input type="text"/>	<input type="text"/>
Zuschlag Mindestbetrag	Mindestbetrag EV EUR 1'000.–	<input type="text"/>	<input type="text"/>
<b>Total Jahrespreis (Netto)</b>			<input type="text"/>

# 1. Allgemein

SwissSign ist in der Schweiz eine nach dem Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur, ZertES) anerkannte Anbieterin von Zertifizierungsdiensten sowie vertrauenswürdige Zertifizierungsstelle resp. Certification Authority («CA») bei den relevanten Software- und Betriebssystemherstellern.

Zertifizierungsstellen haben unter anderem die Aufgabe, eine Identifikation der Antragsteller für Zertifikate durchzuführen.

Gemäss anwendbaren nationalen gesetzlichen Regelungen und internationalen Regularien, wie z.B. Bundesgesetz über die elektronische Signatur, ZertES; eIDAS – Verordnung der EU, ETSI – Normen oder CA/ Browser Forum Richtlinien können die anerkannten Zertifizierungsstellen ihre Aufgabe zur Identifikation eines Antragstellers an Dritte delegieren.

SwissSign will im Rahmen der Ausstellung von Zertifikaten die Identifikation der Antragsteller durch Registrierungsstellen im Sinne der o.g. Rechtsprechung und Regularien bei sorgfältig ausgewählten und kontrollierten Organisationen zulassen und erwartet im Rahmen dieser Bestellung die Zustimmung zu den aufgeführten Verpflichtungen.

Der Kunde nimmt mit dieser MPKI Bestellung die Rolle einer eingeschränkten oder vollumfänglichen Registrierungsstelle für Zertifikatsanfragen und Genehmigungen ein.

## 2. Mitgeltende Unterlagen

Integrierende Bestandteile dieser Bestellung sind nachrangig und in nachstehender, hierarchisch absteigender Rangfolge:

- vorliegend ausgefüllte und rechtsgültig unterzeichnete Bestellung
- Allgemeine Geschäftsbedingungen (AG) Managed PKI Services (MPKI\_GTC): <https://www.swisssign.com/managed-pki/managed-pki-service.html>
- anwendbare SwissSign AG AGB: <https://www.swisssign.com/agb-swisssign.html>

Verhaltensrichtlinien (jeweils aktuelle Version dieser Dokumente ist unter <https://repository.swisssign.com> zu finden)

- PDS; PKI Disclosure Statement Certificate Services
- Teilnehmervereinbarung (EUA); Subscriber-Agreement
- RPA; Relying Party Agreement
- RA-Policy; Richtlinie für die Delegation der Registrierungsstellentätigkeit

**Zum Zeitpunkt der Zertifikatsausstellung gelten zudem die jeweils aktuellen Versionen der folgenden Dokumente** (Diese SwissSign Dokumente sind unter <https://repository.swisssign.com> veröffentlicht. Neue Versionen dieser Dokumente werden am Tag der Inkraftsetzung veröffentlicht und über folgende Systemstatusseite kommuniziert: <https://www.swisssign.com/support/systemstatus.html>);

### Für alle Zertifikate


- Trust Services Practice Statement (TSPS) (SwissSign-TSPS.pdf)

### Für alle TLS Zertifikate gelten zusätzlich

- Certificate Practice Statement for TLS certificates (CPS TLS) (SwissSign-CPS-TLS.pdf)
- Certificate, CRL and OCSP Profiles for TLS certificates (CPR TLS) (SwissSign-CPR-TLS.pdf)

### Für Domain Validated TLS Zertifikate gelten zusätzlich

- SwissSign DV CP – Certificate Policy for Domain Validated certificates (DVCP) (SwissSign-CP-DV.pdf)

 Bitte beachten Sie, dass für eine gültige Bestellung das vorliegende Dokument wie folgt auszufüllen und zu unterzeichnen ist:

- Zeichnungsberechtigte Personen des Kunden Seite 11, Ziffer 9
- Zugangsverantwortliche der MPKI Seite 5, Ziffer 3
- Allgemeine E-Mail-Adresse, Benachrichtigungen und Veröffentlichung der Zertifikate Seite 6

Zusätzlich muss zu allen getätigten Unterschriften eine gültige Ausweiskopie (ID oder Pass, Vorder- und Rückseite), welche vom jeweiligen Inhaber handschriftlich datiert und unterschrieben ist, der Bestellung beigelegt werden.

#### **Für Organization Validated TLS Zertifikate gelten zusätzlich**

- SwissSign OV CP – Certificate Policy for Organization Validated certificates (OVCP)  
(SwissSign-CP-OV.pdf)

#### **Für Extended Validation TLS Zertifikate gelten zusätzlich**

- SwissSign EV CP – Certificate Policy for Extended Validation certificates (EVCP)  
(SwissSign-CP-EV.pdf)

#### **Für alle S/MIME Zertifikate gelten zusätzlich**

- Certificate Practice Statement for S/MIME certificates (CPS S/MIME)  
(SwissSign-CPS-SMIME.pdf)
- Certificate, CRL and OCSP Profiles for S/MIME certificates (CPR S/MIME)  
(SwissSign-CPR-SMIME.pdf)

#### **Für Domain Validation LCP S/MIME Zertifikate gelten zusätzlich**

- Certificate Policy according to Lightweight Certificate Policy (LCP)  
(SwissSign-CP-LCP.pdf)

#### **Für Organizational Validation NCP S/MIME Zertifikate gelten zusätzlich**

- Certificate Policy according to Normalized Certificate Policy (NCP)  
(SwissSign-CP-NCP.pdf)

#### **Für Organizational Validation NCP S/MIME Zertifikat mit speziellen EKU gelten zusätzlich**

- Certificate Policy according to Normalized Certificate Policy (NCP) with extended EKU  
(SwissSign-CP-NCP-extended.pdf)

Beziehungsweise:

- **CP/CPS von SwissSign Silver CA Tree;** SwissSign Silver CP/CPS (neuste Version)  
Gilt nur im Falle des Bezugs von Silberzertifikaten
- **CP/CPS von SwissSign Gold CA Tree;** SwissSign Gold CP/CPS (neuste Version)  
Gilt nur im Falle des Bezugs von Gold- und Gold EV Zertifikaten.

Diese Dokumente unterstehen der Aufsicht der Auditoren von SwissSign und können inhaltlich nicht geändert werden. Sie müssen und werden laufend den Regularien und Normen für Zertifizierungsstellen angepasst. Änderungsmeldungen bezüglich des Inhaltes der Systemstatusseite können dort abonniert werden. Sie gelten als genehmigt, sofern der Kunde nicht innert Monatsfrist nach Aufschaltung schriftlich widerspricht. Ein Widerspruch gilt als ordentliche Kündigung der zugehörigen Verträge und hat eventuell die Revozierung von Zertifikaten mit Ausgabedatum nach der Änderung zur Folge. Eine neue Version der Richtlinie für die Delegation der Registrierungsstellentätigkeit muss immer schriftlich im Rahmen einer Erneuerung dieser Annahmeerklärung genehmigt und akzeptiert werden.

Allgemeine Geschäftsbedingungen des Kunden sind wegbedungen.

### **3. Ernennung der Zugangsverantwortlichen für die Registrierungsstellentätigkeit und Benachrichtigungen**

Die im Rahmen der Zertifikatsbeantragung, -genehmigung und -verwaltung notwendigen Aufgaben kann der Kunde durch die nachfolgend unterzeichnenden Personen wahrnehmen lassen, denen sie hiermit beschränkt darauf eine Handlungsvollmacht für die Registrierungsstellentätigkeit erteilt. Zur weiteren Vertretung, insbesondere auch zur Änderung dieses Vertrages, sind diese **nicht** befugt. Für die Registrierungsstellentätigkeit erhalten diese Personen einen Zugang zur Genehmigung von Zertifikatsanträgen. Die benannten Personen sind je einzeln zeichnungsberechtigt und zur Freigabe von Zertifikaten gemäss Registrierungsprozess (Ziffer 4) befugt.



Es sind mindestens zwei Zugangsverantwortliche als Bevollmächtigte für die Registrierungsstellentätigkeit zu ernennen.



Gültige Ausweiskopie (ID oder Pass, Vorder- und Rückseite) muss vom Zugangsverantwortlichen handschriftlich datiert und unterschrieben und der Bestellung beigelegt werden.

### Zugangsverantwortliche/r 1

Vorname, Nachname

Position

Firma

Kanton/Bundesland der Firma

Land der Firma

E-Mail-Adresse

Telefon

Unterschrift

### Zugangsverantwortliche/r 2

Vorname, Nachname

Position

Firma

Kanton/Bundesland der Firma

Land der Firma

E-Mail-Adresse

Telefon

Unterschrift

### Zugangsverantwortliche/r 3

Vorname, Nachname

Position

Firma

Kanton/Bundesland der Firma

Land der Firma

E-Mail-Adresse

Telefon

Unterschrift

### Zugangsverantwortliche/r 4

Vorname, Nachname

Position

Firma

Kanton/Bundesland der Firma

Land der Firma

E-Mail-Adresse

Telefon

Unterschrift

### Zugangsverantwortliche


oder bereits durch die SwissSign AG validierte Zugangsverantwortliche der MPKI-Installation für die folgende Firma:

Genauere Bezeichnung der Firma mit bereits bestehender MPKI Installation:

## Allgemeine E-Mail-Adresse für Mitteilungen an den Kunden und die CMC Schnittstelle

Im Rahmen der Tätigkeit als Registrierungsstelle erhalten die Zugangsverantwortlichen E-Mails z.B. über den Ablauf der Zertifikate. Diese E-Mails sollen an folgende allgemeine E-Mail-Adresse des Kunden gesendet werden, z.B. [it-info@beispiel.com](mailto:it-info@beispiel.com)

E-Mail-Adresse für Mitteilungen und die CMC Schnittstelle:

 Sofern regulatorische Vorgaben weitere oder andere Benachrichtigungen erfordern, wird SwissSign diese erfüllen, unabhängig der getroffenen Auswahl.

### Benachrichtigungen über den Ablauf von Zertifikaten

Keine Benachrichtigung, da z.B. das eingesetzte System zum Auto-Enrollment oder Mailgateway die Benachrichtigungen oder Erneuerungen übernimmt

Benachrichtigung an die Zugangsverantwortlichen, aber keine Benachrichtigung an den Zertifikatsinhaber, 10 und 30 Tage vor Ablauf der Gültigkeit des Zertifikates

Benachrichtigung an den Zertifikatsinhaber und die Zugangsverantwortlichen, 10 und 30 Tage vor Ablauf der Gültigkeit des Zertifikates

Die Zugangsverantwortlichen werden immer über die im Konto des Kunden hinterlegte E-Mail-Adresse informiert.

### Veröffentlichung der Zertifikate durch SwissSign

Der Kunde möchte seine Zertifikate im allgemeinen Verzeichnis von [www.swisssign.net](http://www.swisssign.net) (LDAP) veröffentlichen, so dass sie für jeden ersichtlich sind und jeder mit ihm verschlüsselt kommunizieren kann.

Der Kunde möchte seine Zertifikate nicht veröffentlichen.

## 4. Einverständniserklärung zum Registrierungsprozess für öffentlich vertrauenswürdige Zertifikate

Für alle öffentlich vertrauenswürdigen Zertifikate verifiziert der Kunde die Identität und sofern gefordert die Organisationzugehörigkeit und weitere spezifische Attribute eines Zertifikats-Antragstellers. Folgende Bedingungen bilden die Basis für den Ausstellungsprozess der Zertifikate im Rahmen dieser Vereinbarung:

### A) Beschäftigte und Teilzeitbeschäftigte (im Fall von E-Mail-Zertifikaten)

Der Kunde garantiert, im Rahmen einer MPKI die Beschäftigten und Teilzeitbeschäftigten seiner Organisation mit folgenden Prüfungen eindeutig zu identifizieren bzw. identifizieren zu lassen:

- Arbeitsvertrag und
- Kopie eines Passes oder die Kopie der Vorder- und Rückseite einer gültigen Identitätskarte (CH, EU, EFTA) in lateinischer Schrift.

### B) Unterauftragnehmer und Berater (im Fall von E-Mail-Zertifikaten)

Der Kunde garantiert, im Rahmen einer MPKI die Unterauftragnehmer und Berater mit den folgenden Prüfungen eindeutig zu identifizieren bzw. identifizieren zu lassen:

- Vertragsvereinbarung zwischen dem Kunden und Unterauftragnehmer/Berater, welche explizit den Unterauftragnehmer oder Berater identifiziert (z.B. auch Geheimhaltungsvereinbarung) und
- Kopie eines Passes oder die Kopie der Vorder- und Rückseite einer gültigen Identitätskarte (CH, EU, EFTA) in lateinischer Schrift.

### **C) Maschinen, Geräte, (Web-)Server (im Falle von SSL Zertifikaten) möglich:**

- Domain Validierung

### **D) Andere:**

Der Kunde garantiert, alle anderen Personen wie folgt zu identifizieren bzw. identifizieren zu lassen, und mit diesen wie folgt zu verfahren:

- Zustandekommen eines Vertrages, welches die sorgfältige Nutzung der Zertifikate vorschreibt und in dem die Person die Pflichten und Mitwirkungsleistungen im Rahmen der Zertifikatsnutzung vollständig akzeptiert und
- Kopie eines Passes oder die Kopie der Vorder- und Rückseite einer gültigen Identitätskarte (CH, EU, EFTA) in lateinischer Schrift.

### **Offenlegungspflicht gegenüber SwissSign**

In allen Fällen garantiert der Kunde seine Fähigkeit:

- die Prüfung der Registrierung und aller zugehörigen Dokumente gemäss den obengenannten Regeln durchzuführen oder durchführen zu lassen
- insbesondere ist sichergestellt, dass für alle Personen, für welche Zertifikate ausgestellt werden (E-Mail Zertifikate mit einem Organisationseintrag), die Organisationszugehörigkeit geprüft wurde
- eine Evidenz zur Sicherstellung dieser Überprüfungen kann jederzeit auf Anfrage von SwissSign durch den Kunden vorgelegt werden

## **5. Auftragsdatenverarbeitung**

SwissSign erbringt für den Kunden im Rahmen des vorliegenden Vertrags Leistungen auf dem Gebiet der Datenverarbeitung. Dabei erhält SwissSign Zugriff auf personenbezogene Daten und verarbeitet diese ausschliesslich im Auftrag und nach Weisung des Kunden. Im Rahmen der Delegation der Registrierungsstellentätigkeit übernimmt der Kunde Aufgaben bei der Zertifikatsausstellung im Bereich Identifizierung, Registrierung und Archivierung. Gemäss den regulatorischen Vorgaben (u.a. ZertES, eIDAS, CA/Browser Forum Baseline Requirements) verbleibt die Verantwortung gegenüber dem Zertifikatsinhaber und den vertrauenden Dritten bei SwissSign.

### **5.1 Geltungsbereich**

Teil der Vertragsdurchführung ist die Verarbeitung personenbezogener Daten. Gegenstand, Dauer, Umfang und Zweck der Datenbearbeitung durch SwissSign ergeben sich ausschliesslich durch den vorliegenden Vertrag.

Die Parteien vereinbaren für die Bearbeitung von Personendaten (insbesondere Name, Vorname, Ausweistyp, Adresse, E-Mail-Adresse, Wohnsitz/Sitz), die jeweils anwendbaren gesetzlichen Rahmenbedingungen, insbesondere aber das Schweizerische Datenschutzgesetz (DSG) sowie die Europäische Datenschutzgrundverordnung (DSGVO), einzuhalten.

### **5.2 Personendaten**

Unter Personendaten werden alle Informationen verstanden, welche unter Art. 5 lit. a DSG resp. Art. 4 Ziff. 1 sowie Art. 9 DSGVO definiert werden.

### **5.3 Art und Zweck der Verarbeitung**

SwissSign hat die Personendaten nicht zu eigenen Zwecken und zu keinem anderen Zweck als dem im vorliegenden Vertrag erwähnten zu verwenden. Die Verarbeitung von Personendaten durch SwissSign dient dem Zweck der Identifizierung, Registrierung sowie der Ausstellung und Bewirtschaftung von Zertifikaten und ist folgender Art:

- Ausstellen von Zertifikaten
- Veröffentlichung der Zertifikatsstatusinformationen (Revocation Status Service)
- Identifizieren
- Registrieren
- Prüfen und freigeben
- Archivieren
- Revozieren
- Korrespondenz und Kontakt mit betroffenen Personen

## 5.4 Datenkategorien

Es werden folgende Datenkategorien durch SwissSign verarbeitet:

- Personenstammdaten (Name, Anrede, Titel/akademischer Grad, Geburtsdatum, Anschrift)
- Kontaktdaten (Adresse, E-Mail-Adresse, Telefonnummer)
- Vertragsdaten (Vertragsdetails, Leistungen, Produkt- bzw. Vertragsinteresse, Kundennummer)
- Kundenhistorie
- Vertragsabrechnungsdaten und Zahlungsinformationen (Rechnungsdetails, Bankverbindung, Kreditkarteninformationen)
- Protokoll Daten (Logfiles)
- Identitätsdaten
- Authentifizierungsdaten
- Systemdaten (Log-, Konfiguration und Auditdaten)
- Auskunftsangaben (z.B. öffentlichen Verzeichnissen)

## 5.5 Kategorien von betroffenen Personen

Von folgenden Kategorien betroffener Personen werden die obengenannten personenbezogenen Daten verarbeitet:

- Zertifikatsinhaber
- Kontaktpersonen/Ansprechpartner

## 5.6 Ort der Verarbeitung

Die Datenverarbeitung von SwissSign findet ausschliesslich in der Schweiz statt.

Eine Auslagerung der Datenverarbeitung in ein Drittland ausserhalb der EU /EFTA bedarf der vorgängigen, schriftlichen Zustimmung des Kunden.

## 5.7 Auftragsverarbeitung und Beizug Dritter

SwissSign bearbeitet Personendaten ausschliesslich im Auftrag und unter Weisung des Kunden (im Sinne von Art. 9 DSG resp. Art. 28 DSGVO). Die Tätigkeiten und Leistungsbeschreibungen ergeben sich aus dem vorliegenden Vertrag inklusive der erwähnten mitgeltenden Unterlagen. Änderungen der Leistungspflichten und Weisungen haben schriftlich zu erfolgen.

SwissSign führt für die vorliegende Auftragsverarbeitung ein Verarbeitungsverzeichnis nach Art. 12 DSG resp. Art. 30 DSGVO.

SwissSign gewährleistet, dass es den mit der Verarbeitung der Daten befassten Mitarbeitern und weiteren Hilfspersonen untersagt ist, die Daten ausserhalb der Weisung zu verarbeiten. Es wird gewährleistet, dass die vorgenannten Personen einer angemessenen Vertraulichkeits- und Verschwiegenheitspflicht unterliegen, welche auch nach Beendigung des Arbeits-, Auftragsverhältnisses etc. fortbesteht.

Zur Leistungserbringung beigezogene Dritte unterliegen in Bezug auf die Verarbeitung von Personendaten denselben Pflichten wie die Parteien. Die Parteien gewährleisten, ihre Pflichten allfälligen Dritten zu überbinden. Sie bleiben für die Einhaltung der Pflichten verantwortlich.

## 5.8 Technische und organisatorische Massnahmen

SwissSign verpflichtet sich, alle zumutbaren, erforderlichen, technischen und organisatorischen Massnahmen zum Schutz der Personendaten zu ergreifen, namentlich zur Verhinderung von unbefugten Zugriffen von Dritten, Verlust, Beschädigung, Löschung oder Vernichtung der Daten. Die ergriffenen Schutzmassnahmen haben mindestens den Anforderungen von Art. 7 DSG resp. Art. 32 DSGVO zu genügen.

Die technischen und organisatorischen Massnahmen haben die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen. Neben der digitalisierten Informations- und Datensicherheit sind die Räumlichkeiten, in welchen die Daten bearbeitet werden, Zutrittsgeschützt.



SwissSign setzt hier insbesondere die folgenden Massnahmen ein:

- Zugangskontrolle: Räumlichkeiten/IT-Systeme
- Weitergabekontrolle
- Bekanntgabekontrolle
- Speicherkontrolle
- Benutzerkontrolle
- Zugriffskontrolle
- Trennungskontrolle

### **5.9 Kontroll- und Auditrechte des Kunden**

SwissSign verpflichtet sich, dem Kunden auf dessen mündliche oder schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte und Nachweise zur Verfügung zu stellen, die zur Durchführung einer Kontrolle der vertragsgemässen Bearbeitung von Personendaten des Kunden durch SwissSign erforderlich sind.

Der Kunde hat das Recht, die Einhaltung der anwendbaren Datenschutzvorgaben im erforderlichen Umfang und auf eigene Kosten durch einen entsprechend qualifizierten externen Auditor, welcher der Geheimhaltungspflicht unterliegt, mit einer Überprüfung zu beauftragen. Dabei ist der Grundsatz der Verhältnismässigkeit einzuhalten sowie die schutzwürdigen Interessen von SwissSign (insbesondere auf Geheimhaltung) zu berücksichtigen. Kontrollen bei SwissSign haben ohne vermeidbare Störungen ihres Geschäftsbetriebs und nach angemessener Vorankündigung zu erfolgen.

### **5.10 Mitwirkungspflichten des Kunden**

Die Mitwirkungspflichten des Kunden aus der Registrierungsstellentätigkeit, insbesondere in Zusammenhang mit der Identifikation der Antragsteller, ergeben sich aus dem vorliegenden Vertrag und den mitgeltenden Unterlagen.

Der Kunde gewährleistet, dass alle notwendigen Rechtfertigungsgründe für die Datenbearbeitung (Einwilligung etc.) vorliegen.

### **5.11 Informations- und Unterstützungspflichten**

Beide Parteien informieren sich gegenseitig und angemessen frühzeitig über nicht-vertragskonforme Vorfälle in Bezug auf Datengovernance, Datenschutz und Informationssicherheit.

Die Parteien verpflichten sich zur gegenseitigen Unterstützung bei der Einhaltung der anwendbaren Datenschutzvorgaben unter diesem Vertrag sowie im Falle von behördlichen Anordnungen.

Die Parteien unterrichten sich gegenseitig und unverzüglich, wenn sie Verletzungen des Schutzes von Personendaten im Rahmen der vertraglichen Leistungserbringung feststellen. Die Parteien melden eine entsprechende Verletzung innert 72 Stunden auch der zuständigen Aufsichtsbehörde.

### **5.12 Betroffenenrechte**

Die Parteien verpflichten sich, die Betroffenenrechte zu wahren und zu gewährleisten.

Die betroffene Person hat namentlich das Recht auf Auskunft, Löschung, Korrektur, Sperrung sowie Portabilität der Daten (Art. 25 ff. DSG resp. Art. 12 ff. DSGVO).

Können Daten aufgrund gesetzlicher oder geschäftlicher Pflichten nicht gelöscht werden, werden sie blockiert. Ist die Richtigkeit oder Unrichtigkeit von Daten nicht beweisbar, werden sie mit einem Bestreitungsvermerk versehen.

Die Parteien verpflichten sich die Daten, welche die betroffene Person zur Bearbeitung zur Verfügung gestellt hat, in einem gängigen, maschinenlesebaren Format auf Anfrage der betroffenen Person herauszugeben.

Wendet sich eine betroffene Person an SwissSign, leitet diese die betroffene Person an den Kunden weiter und wartet dessen Weisungen ab. Die Parteien unterstützen einander soweit vereinbart bei der Bearbeitung der Betroffenenanfragen. SwissSign haftet nicht, wenn das Ersuchen der betroffenen Person vom Kunden nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

### 5.13 Datenschutzbeauftragte Person

SwissSign bestellt – soweit von den anwendbaren Datenschutzvorgaben vorgeschrieben – schriftlich eine datenschutzbeauftragte Person. Datenschutzbeauftragte Person der SwissSign ist:

General Counsel  
SwissSign AG  
Sägereistrasse 25  
CH-8152 Glattbrugg  
[privacy@swissign.com](mailto:privacy@swissign.com)

Über Änderungen der datenschutzbeauftragten Person und/oder von deren Kontaktdaten wird der Kunde unverzüglich schriftlich informiert.

### 5.14 Geheimhaltung

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmassnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

### 5.15 Aufbewahrungspflicht, Löschung und Rückgabe

Nach Beendigung dieses Vertrages hat SwissSign sämtliche in ihren Besitz gelangten Unterlagen und erstellten Verarbeitungs- oder Nutzungsergebnisse oder zur Leistungserfüllung hergestellten oder kopierten personenbezogenen oder sonstige vertrauliche Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, auf Aufforderung dem Kunden auszuhändigen oder in Abstimmung mit dem Kunden datenschutzgerecht zu vernichten oder sicher zu löschen, sofern nicht eine gesetzliche oder regulatorische Verpflichtung von SwissSign zur Speicherung besteht. Die Löschung ist in geeigneter Weise zu dokumentieren. Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben unberührt.

Zur Einhaltung der regulatorischen Vorgaben (u.a. ZertES, VZertES, CA/Browser Forum Baseline Requirements) müssen alle Unterlagen und Beweismittel, die für die Genehmigung von Zertifikatsanträgen relevant sind, elf (11) Jahre nach Ablauf der Gültigkeit des Zertifikates aufbewahrt werden. Der Kunde verpflichtet sich im Rahmen seiner Registrierungsstellentätigkeit, diese Unterlagen und Beweismittel während der vorgeschriebenen Dauer aufzubewahren.

Nach Erfüllung des Zwecks, jedenfalls aber nach Beendigung, Ablauf oder Kündigung des vorliegenden Vertrages, hat der Kunde alle Daten während der gesetzlich vorgeschriebenen Archivierungsfrist rechtsgenügend aufzubewahren und im Bedarfsfall SwissSign kostenlos zur Verfügung zu stellen.

## 6. Genehmigung im Rahmen MPKI

Die Handlungsvollmacht der Zugangsverantwortlichen für die Registrierungsstellentätigkeit gemäss Ziffer 3 umfasst darüber hinaus ohne weitere Einzelprüfung die Genehmigung der Registrierung und Veröffentlichung aller Zertifikate für die genannte Organisation, die gleichlautend dem Registereintrag oder Organisationsnachweis ist. Der Organisationsname kann dann auch im öffentlich vertrauenswürdigem Zertifikat publiziert werden, sofern das im Zertifikat vorgesehen ist. Vorbehalten ist die Genehmigung bestimmter weiterer Einträge im öffentlich vertrauenswürdigem Zertifikat, die nicht die Organisation betreffen (z.B. Domains, Personennamen) durch den Kunden.

Die Nutzung aller im Rahmen einer MPKI ausgestellten Zertifikate über das Ende des kommerziellen Vertrages mit SwissSign oder einem SwissSign-Partner hinaus ist nicht gestattet. Alle technisch noch gültigen Zertifikate müssen revoziert werden durch den Kunden oder gegen Gebühr durch SwissSign.

Im Kündigungsfall eines eines SwissSign-Partners ist SwissSign berechtigt, den MPKI Kunden über die Kündigung zu informieren sowie auf Wunsch die zur Weiterführung der Leistungserbringung geeigneten Schritte zu ergreifen.

## 7. Genehmigung und Annahmeerklärung

Der Kunde erklärt hiermit sein Einverständnis zu der Richtlinie für die Delegation der Registrierungsstellentätigkeit und den Teilnehmerbedingungen Zertifikatsdienstleistungen. Er anerkennt zudem, dass SwissSign die Ausstellung der Zertifikate auf Basis der von ihm genehmigten Zertifikatsanträge vornimmt.

Der Kunde wird SwissSign schriftlich mittels Änderungsformular über Änderungen bezüglich der Zugangsverantwortlichen informieren.

## 8. Vertragsabschluss, -laufzeit und Beendigung

Das Einsenden der unterzeichneten Bestellung gilt als verbindliche Bestellung einer zahlungspflichtigen Leistung.

Vertragslaufzeit und Verrechnungsperiode beginnen mit dem Datum der Bestellung.

Die Erstvertragslaufzeit beträgt ein Jahr und verlängert sich nach Ablauf der Erstvertragslaufzeit jeweils automatisch um ein weiteres Jahr.

Nach Ablauf der Erstvertragslaufzeit kann der Vertrag jeweils per Ende der Vertragslaufzeit und mit 3-monatiger Kündigungsfrist beendet werden.

## 9. Unterschriften

Für den Kunden unterschreiben die Zeichnungsberechtigten gemäss Handelsregister oder dem offiziellem Organisationsnachweis.

Mit seiner Unterschrift bestätigt der Kunde, den Kauf der MPKI mit der obengenannten Erstvertragslaufzeit sowie, die SwissSign AGB inklusive der für diesen Vertrag relevanten Anhänge gelesen, verstanden und akzeptiert haben.

### Zeichnungsberechtigte/r 1

Ort, Datum

E-Mail-Adresse

Telefonnummer

Name, Vorname, Funktion *in Druckschrift*

Unterschrift

### Zeichnungsberechtigte/r 2

Ort, Datum

E-Mail-Adresse

Telefonnummer

Name, Vorname, Funktion *in Druckschrift*

Unterschrift



Zusätzlich zu den Unterschriften in diesem Dokument ist pro unterzeichnende Person immer eine Kopie eines gültigen Ausweisdokumentes (ID oder Pass, Vorder- und Rückseite) beizulegen, welche von der entsprechenden Person handschriftlich datiert und unterschrieben werden muss.

Bitte beachten Sie, dass ohne die Ausweiskopien die MPKI nicht aufgesetzt werden kann und dass aufgrund regulatorischer Vorgaben in gewissen Zeitabständen eine Re-Validierung durchgeführt werden muss.

# Checkliste und Dokumentenversand



Haben alle Zugangsverantwortlichen unterzeichnet? (Ziffer 3)



Liegen von den Zugangsverantwortlichen persönlich datierte und unterzeichnete Ausweiskopie (ID oder Pass, Vorder- und Rückseite) derselben bei? (Ziffer 3)



Sind die Vertragsunterzeichner nachprüfbar über den Registerauszug zeichnungsbefugt? (Ziffer 9)



Liegen von den Vertragsunterzeichnern persönlich datierte und unterzeichnete Ausweiskopien (ID oder Pass, Vorder- und Rückseite) derselben bei? (Ziffer 9)



Senden Sie die Dokumente im Papieroriginal per Post an SwissSign.

**SwissSign AG**  
**Sales & Partner Management**  
**Sägereistrasse 25**  
**8152 Glattbrugg**  
**Schweiz**

Der Eingang der Bestellung wird von SwissSign per E-Mail bestätigt.

## Hinweise und Anmerkungen

Stellen Sie sicher, dass die Bestellung an SwissSign versendet wird.

Das Prüfverfahren kann nur durchgeführt werden, wenn alle erforderlichen Dokumente beiliegen. Achten Sie im Speziellen auf folgende Punkte:

- von allen Unterzeichnern dieser Bestellung ist eine durch den Unterzeichner datierte und unterschriebene Kopie der ID oder des Passes beigefügt
- dass nur Personen, welche im Handelsregister oder dem offiziellen Organisationsnachweis als zeichnungsberechtigt hinterlegt sind, dieses Formular unter Ziffer 9 «Unterschriften» unterzeichnen

Sofern nicht die im Handelsregister oder Organisationsnachweis eingetragenen Personen unterzeichnen, werden wir bezüglich der Zeichnungsvollmacht den Personalverantwortlichen oder Vertreter des Unternehmens gemäss Handelsregister oder Organisationsnachweis anrufen. Bitte rechnen Sie, je nach Erreichbarkeit der anzurufenden Personen, einige Tage oder Wochen zusätzliche Bearbeitungszeit hierfür ein.

Die Domainprüfung wird mittels automatisiertem SwissSign-Check-Verfahren durchgeführt.

Die vom CAB Browserforum bewilligten Verfahren sind jeweils auf der SwissSign Support Seite unter <https://www.swisssign.com/support/mpki-setup.html> beschrieben.



Abonnieren des RSS Benachrichtigungsfeeds über Systemstatusmeldungen (empfohlen)

<https://www.swisssign.com/support/systemstatus.html>