PKI Disclosure Statement Zeitstempelservice

(PKI Disclosure Statement TSA)

Version: 1.0
OID: 2.16.756.1.89.1.1.6.1.1

Dieses Dokument unterliegt dem Audit der SwissSign als akkreditierte Zertifizierungsstelle und darf weder abgeändert noch durch Nebenabreden entkräftet oder abgeändert werden.

SwissSign

Freigabe und Versionierung

Autor	Datum	Version	Kommentar
Ingolf Rauh	2017-07-14	1.0	Erstellung

Freigabe durch

Zeichnungsbefugte SwissSign	Digitale Signatur
Reinhard Dietrich (CISO) SwissSign AG	Reinhard Armand Dietrich Qualifiziert signiert durch Reinhard Armand Dietrich Swiss Post Solutions AG Glattbrugg, 7. September 2017
Markus Naef (CEO) SwissSign AG	Qualifiziert signiert durch Markus Naef SwissSign AG Glattbrugg, 11. September 2017

SwissSign

Inhalt

1. Geltungsbereich 4
2. CA Kontakt Info 4
3. Zertifikatstyp, Validierungsprozesse und Nutzung 4
3.1 Nutzungszweck 4
3.2 Validierungsprozesse 4
3.3 Einschränkungen 5
4. Vertrauensbeschränkungen 5
5. Pflichten des TEILNEHMERS 5
6. Pflichten der RELYING PARTY und Zertifikatsprüfung 5
7. Begrenzte Haftung 6
8. Mitgeltende Unterlagen 6
9. Datenschutz 7
10. Rückerstattungen 7
11. Anwendbares Recht und Beschwerden 7
11.1 Aussergerichtliche Streitbeilegung 7
11.2 Anwendbares Recht und Gerichtsstand 7
11.3 TSP und Repository Lizenzen, Vertrauenshinweise und Audit 7

1. Geltungsbereich

Mit der Antragstellung für einen Signaturservice und/oder Zeitstempeldienstleistung, stimmt der Teilnehmer eines Signaturservices und/oder Zeitstempeldienstleistung (nachfolgend: TEILNEHMER) der Teilnehmervereinbarung Signatur- und Zeitstempeldienstleistung (nachfolgend: TEILNEHMERVEREINBARUNG) zu.

Die TEILNEHMERVEREINBARUNG regelt das Vertragsverhältnis zwischen TEILNEHMER sowie der SwissSign AG, Sägereistrasse 25, 8152 Glattbrugg, Schweiz, (nachfolgend: SWISSSIGN) betreffend die Nutzung von Zeitstempeln von SWISSSIGN und Nutzung von Signaturen der von SWISSSIGN treuhänderisch verwalteten Zertifikaten oder auf SWISSSIGN lautenden Zertifikaten für den Signatureinsatz für Dritte (nachfolgend: „DIENSTLEISTUNGEN“).

Ein TEILNEHMER ist der Empfänger eines Zeitstempels und/oder einer Signatur. Er kann eine Organisation sein oder ein individueller Endbenutzer. Der TEILNEHMER hat die vertragsgemässe Nutzung des Dienstes sicherzustellen.

Die Ausstellung der Signaturen und Zeitstempel erfolgt in Übereinstimmung mit den Vorschriften der SwissSign Platinum CP/CPS. Die CP/CPS sind in ihrer jeweils aktuellsten Form unter https://repository.swisssign.com erhältlich.

Voraussetzung für die Nutzung der DIENSTLEISTUNG ist die Einhaltung der kommerziellen Vertragsbedingungen, die Basis für die Nutzung durch den TEILNEHMER sind. Die kommerziellen Vertragsbedingungen sind nicht Gegenstand dieser TEILNEHMERVEREINBARUNG. Sie können auch zwischen Dritten (z.B. Reseller, Arbeitgeber des TEILNEHMERS usw.) bestehen.

Vertraglich ist weiterhin die TEILNEHMERVEREINBARUNG und allfällige kommerzielle Vertragsbedingungen massgeblich sowie für die Ausstellung der Zertifikate die jeweilige CP/CPS. Das PKI Disclosure Agreement ersetzt diese nicht und fasst nur informativ wesentliche Punkte beider Dokumente zum besseren Verständnis für TEILNEHMER, ZERTIFIKATSINHABER und Dritte (RELYING PARTIES) zusammen.

2. CA Kontakt Info

SwissSign AG, Schweiz:
Postadresse: Sägereistrasse 25, 8152 Glattbrugg, Schweiz.
Telefon: +41 848 77 66 55
E-Mail: helpdesk@swisssign.com

SwissSign AG Liechtenstein
Postadresse: Meierhofstrasse 5, 9490 Vaduz, Liechtenstein
Telefon: +41 848 77 66 55
E-Mail: helpdesk@swisssign.com

3. Zertifikatstyp, Validierungsprozesse und Nutzung

3.1 Nutzungszweck

Zeitstempelzertifikate werden gemäss der EU Verordnung 910/2014 („eIDAS Regulation“) und gemäss dem Schweizerischen ZertES Gesetz angeboten. Sie gelten im Rahmen dieser Verordnungen als qualitative Zeitstempel und bestätigen die Unveränderlichkeit eines Dokumentes seit Aufbringen des Zeitstempels und stellen die korrekte Uhrzeit mit diesem Stempel zur Verfügung. Ein Zeitstempel muss zwingend aufgebracht werden im Rahmen einer qualitativen Signatur.

Der qualitative Zeitstempeldienst nach Schweizer Recht ZertES wird angeboten unter http://tsa.swisssign.net oder https://tsa.swisssign.net.
Es sind keine weiteren Benutzernamen oder Passwörter notwendig.

Der qualitative Zeitstempeldienst nach EU Recht wird angeboten unter http://tsa-eu.swisssign.net oder https://tsa-eu.swisssign.net.

Es gelten für beide Zeitstempel die Zeitstempel Policies, die in der letzten Version unter https://repository.swisssign.com zu finden sind.

3.2 Validierungsprozesse

Die Nutzung des Zeitstempels ist allen Nutzern im Rahmen des kommerziellen Vertragsverhältnisses mit SwissSign gestattet. Es wird lediglich die IP Adresse überprüft. Sollte diese missbräuchlich den Zeitstempeldienst nutzen, wird diese gesperrt.

3.3 Einschränkungen

Die Hashes der Zeitstempel können SHA-256, SHA-384 oder SHA-512 sein.

Der Schweizer Zeitstempel nach ZertES weist folgende Parameter aus:

Richtlinien OID:2.16.756.1.89.1.1.3.4
Zertifikatsinhaber
CN: SwissSign TSA 2016-G22
O: SwissSign AG
C: CH
Unterschriftenalgorithmus: SHA256

Der eIDAS konforme Zeitstempel nach liechtensteinischem Signaturgesetz weist folgende Parameter aus:

Derzeit noch nicht angeboten.

Die maximale Gültigkeit des Zeitstempels ist 10 Jahre.

4. Vertrauensbeschränkungen

Die Nutzung des Zeitstempels ergibt sich aus dem unter Ziffer 3 genannten Nutzungszweck.

Die maximale Abweichung der Zeit von der UTC Zeitquelle kann +- 1 Sekunde betragen. Sofern keine Zeitquelle zur Verfügung steht, wird kein Zeitstempel ausgegeben.

Alle Daten im Rahmen des Tätigkeitsjournals (Daten zum Zertifikatslebenszyklus) werden 11 Jahre vorgehalten.

5. Pflichten des TEILNEHMERS

Der TEILNEHMER muss sicherstellen, dass er die Regelungen der TEILNEHMERVEREINBARUNGEN folgt. Diese verpflichten den TEILNEHMER insbesondere zur Einhaltung folgender Pflichten:

Technisch ist die Anzahl der zu erhaltenden Zeitstempel nicht limitiert. Der TEILNEHMER verpflichtet sich, das angekündigte oder bestellte Kontingent oder Freikontingent von Zeitstempeln nicht ohne Rückmeldung an SWISSSIGN zu überschreiten.

Der TEILNEHMER meldet alle für den Zeitstempelservice vorgesehene IP Adressen SWISSSIGN, sofern er mehr als das Freikontingent ausschöpfen möchte. Änderungen werden rechtzeitig (ein Monat Vorlauf) bekannt gegeben.

Die eingesetzte Clientsoftware des TEILNEHMER ist konform zu den Empfehlungen von SWISSSIGN einzusetzen und muss sichere kryptographische Funktionen aufweisen. Im Zweifelsfalle ist SWISSSIGN im Vorhinein über den Einsatz der Clientsoftware zu befragen.

Es wird die maximal zugesagte Performance im Abruf durch den TEILNEHMER nicht überschritten.

Der TEILNEHMER überprüft die SWISSSIGN Revozierungsliste (CRL), dass das Zeitstempelzertifikat nicht revoziert wurde.

Der TEILNEHMER muss alle relevanten Empfänger eines zeitgestempelten Dokumentes („Relying Party“) über die Zeitstempelpolicy und Möglichkeiten zur Überprüfung des Zeitstempels gemäss dem folgenden Abschnitt aufklären.

6. Pflichten der RELYING PARTY und Zertifikatsprüfung

Die Relying Party muss sich vergewissern, dass das dem Zeitstempel zugrunde liegende Zeitstempelzertifikat zum Zeitpunkt der Signatur gültig war und die Signatur korrekt erfolgte:

- Das der Signatur zugrunde liegende Zertifikat und alle Zertifikate in der Zertifikatskette dürfen nicht revoziert sein. SwissSign stellt für die Überprüfung der Gültigkeit des Zertifikates Standarddienste, wie CRL (Certificate Revocation List) und OCSP (Online Certificate Status Protocol) zur Verfügung. Bevor einer Signatur vertraut wird, sollte die Gültigkeit hiermit durch die RELYING PARTY überprüft werden. Die Links zur CRL und OCSP sind Teil des Zertifikates. CRLs sind maximal 10 Tage gültig, werden aber täglich aktualisiert. Daher muss die RELYING PARTY immer auf die neueste CRL Datei zurückgreifen, um die Gültigkeit des Zertifikates zu überprüfen.
- Sollte eine CRL Datei und ein OCSP Service aus technischen Gründen nicht zur Verfügung stehen, muss die RELYING PARTY selber abschätzen, wie lange er sich auf die Gültigkeit der Signatur verlassen kann. Dies hat auch im Kontext der damit verbundenen Transaktion

zu erfolgen und dem daraus verbundenen Risiko. Das Vertrauen sollte nicht länger als 10 Tage gewährt werden.
- Die Gültigkeit der Zertifikate von SwissSign ist beschränkt auf die Gültigkeitsdauer der Zertifikate minus 10 Tage. Daher sollte die RELYING PARTY immer überprüfen, dass das Zertifikat noch gültig ist.
- Bei signierten Dokumenten muss sichergestellt werden, dass die Dokumente nach Aufbringen der Signatur nicht verändert wurden.
- Standardapplikationen sollen unter den Umständen der letzten Punkte die Signatur als vertrauenswürdig anzeigen. Insbesondere sollte die Identität des Zertifikatbesitzers korrekt angezeigt werden.
- SwissSign Zeitstempel sind nicht für den Einsatz in hoch kritischen Infrastrukturen konzipiert. Es sollte vermieden werden, dass aufgrund von Signaturen durch SwissSign Zertifikate automatisiert Entscheidungen getroffen werden, die direkt oder indirekt zu Personenschäden oder beträchtlichen Sachschäden führen können. Beispiele sind hier nicht ausschliesslich: Betrieb von Kraftwerken, Waffensysteme, Flugkontrollsysteme, etc.
- Die Verantwortung für die Risikoabschätzung und Nutzung des Zertifikates in einem bestimmten Einsatzscenario liegt bei der RELYING PARTY.
- Die Nutzung von nicht mehr gültigen Signaturen ist auszuschliessen.
- Im Rahmen der Nutzung unter eIDAS muss die RELYING PARTY gemäss der ETSI Norm 319 421 sicherstellen, dass das SWISSSIGN Zeitstempelzertifikat als qualifiziertes Zertifikat auf der eIDAS Trusted List aufgeführt ist.

7. Begrenzte Haftung

Die Begrenzungen in der Haftung ergeben sich aus den Bestimmungen der CP/CPS. Alle qualifizierte Zertifikate und Siegelzertifikate der Platinum Root CA unterliegen der gesetzlich bestimmten Haftung gemäss ZertES (Schweizer qualifizierte Zertifikate) und eIDAS (EU qualifizierte Zertifikate).

SWISSSIGN haftet gegenüber dem TEILNEHMER für alle Schäden, die sie dem TEILNEHMER verursacht, sofern sie nicht beweist, dass sie kein Verschulden betrifft. Die Haftung für leichte Fahrlässigkeit ist ausgeschlossen.

Gegenüber Dritten gelten die Haftungsvorschriften der CP/CPS.

Keine Partei haftet für das ordentliche Funktionieren von Systemen Dritter, so insbesondere des Internets. SWISSSIGN haftet nicht für die vom TEILNEHMER verwendeten Systeme und Software.

Der TEILNEHMER verpflichtet sich, SWISSSIGN von sämtlichen Ansprüchen Dritter freizustellen, die aus der vertrags- bzw. rechtswidrigen oder missbräuchlichen Nutzung der ZERTIFIKATSDIENSTLEISTUNG resultieren. Die Freistellung umfasst auch die Verpflichtung, SWISSSIGN von Rechtsverteidigungskosten (z. B. Gerichts- und Anwaltskosten) vollständig freizustellen.

Beide Parteien haften für das Verhalten ihrer Hilfspersonen sowie beigezogener Dritter (z.B. Subunternehmer, Zulieferanten) wie für ihr eigenes.

Bei Personenschäden haften die Parteien für jedes Verschulden. In keinem Fall haften die Parteien insbesondere für indirekte Schäden, für mittelbare Schäden, für Folgeschäden, für Datenverlust, für Mehraufwand oder Ansprüche Dritter, für entgangenen Gewinn oder nicht realisierte Einsparungen sowie für Schäden aus verspäteter Lieferung oder Leistung.

In jedem Falle gelten vorrangig die Haftungsvorschriften des Schweizer Bundesgesetzes über die elektronische Signatur sowie von Art. 59a des Schweizerischen Obligationenrechts für Zertifikate, die von der Schweizerischen CA signiert wurden, bzw. die Haftungsvorschriften des liechtensteinischen SigG im Falle von Zertifikaten, die von der liechtensteinischen CA signiert wurden.

8. Mitgeltende Unterlagen

Für den TEILNEHMER und den ZERTIFIKATSINHABER sowie der RELYING PARTY sind folgende Dokumente relevant, die in ihrer letztgültigen Form unter https://repostitory.swisssign.com zu finden sind:

- CP/CPS Platinum
  Zertifizierungsrichtlinien und Ausführungsbedingungen der SwissSign CA.
- Zeitstempel Policy (TSA Policy)

- TEILNEHMERVEREINBARUNG Zeitstempel und Signaturservice/Subscriber Agreement TSA and Signing Service
  Regelung der Rechte und Pflichten des TEILNEHMERS und ZERTIFIKATSINHABERS in Bezug auf eine Zertifikatsdienstleistung.
- Relying Party Agreement
  Regelung der Rechte und Pflichten einer RELYING PARTY.

9. Datenschutz

Die SWISSSIGN verpflichtet sich, die anwendbaren Datenschutzgesetzgebungen für ihre jeweilige CA einzuhalten.

Grundsätzlich überträgt der TEILNEHMER im Rahmen der Zeitstempeldienstleistung nur einen Hash seiner Dokumentendaten, aus denen der Dokumenteninhalt nicht rekonstruiert werden kann. Des Weiteren wird die IP Adresse übertragen.

Die für die Leistungserbringung notwendigen Daten werden durch SWISSSIGN gespeichert und vertraulich behandelt. Die im Rahmen der Prüftätigkeit erhobenen Daten, insbesondere Personendaten dürfen nur für den Zweck und im Umfang, soweit dieser für die Erfüllung und Durchführung des ZERTIFIKATSDIENSTLEISTUNG erforderlich ist, verwendet werden. Die Nutzung für andere Zwecke oder gar die Weitergabe an Dritte ist strikt untersagt. Vorbehalten bleibt die Weitergabe an (z. B. im Falle einer Kontrolle, externe Registrierungstätigkeit) beauftragte, berechtigte Dritte oder durch behördliche Anordnungen. Beauftrage, berechtigte Dritte unterliegen den Datenschutzbestimmungen in gleicher Weise wie SWISSSIGN.

Zum Schutz der Daten wird Sicherheitstechnologie nach Stand der Technik eingesetzt.

Der TEILNEHMER und ZERTIFIKATSINHABER seinerseits verpflichtet sich, die auf ihn lokal anwendbaren Datenschutzvorschriften einzuhalten sowie die Datenschutzbestimmungen der CP/CPS.

10. Rückerstattungen

Die Möglichkeiten zur Rückerstattung bereits erbrachter Signaturen ergeben sich aus den kommerziellen AGBs. Die letztgültige Version ist abrufbar unter
https://www.swisssign.com/de/agb.

11. Anwendbares Recht und Beschwerden

Alle Beschwerden sind über das Kontaktformular https://www.swisssign.com/de/kontakt an SwissSign einzureichen.

11.1 Aussergerichtliche Streitbeilegung

Die Parteien bemühen sich bei Streitigkeiten vor Anrufung der ordentlichen Gerichte, eine einvernehmliche Lösung zu suchen, und verpflichten sich im Rahmen ihrer gesetzlichen Pflichten, an gesetzlich vorgesehenen aussergerichtlichen Streitbeilegungsverfahren teilzunehmen.

11.2 Anwendbares Recht und Gerichtsstand

Auf das Rechtsverhältnis aus der TEILNEHMERVEREINBARUNG ist ausschliesslich schweizerisches Recht anwendbar. Vorbehalten ist das liechtensteinische Signaturrecht für Zertifikate, die von der liechtensteinischen CA ausgestellt und signiert wurden. Die Bestimmungen des Übereinkommens der Vereinten Nationen vom 11. April 1980 über Verträge über den internationalen Warenkauf (Wiener Kaufrecht, CISG) sind in jedem Falle wegbedungen.

Ausschliesslicher Gerichtsstand ist Zürich, Schweiz. Für Teilnehmer und Zertifikatsinhaber mit ausländischem Wohn- bzw. Geschäftssitz gilt Zürich, Schweiz, als Betreibungsort und als ausschliesslicher Gerichtsstand für alle zivilrechtlichen Verfahren.

11.3 TSP und Repository Lizenzen, Vertrauenshinweise und Audit

Soweit die Ausstellung und Verwaltung von Zeitstempeln gesetzlichen Anforderungen untersteht (z.B. Schweiz: ZertES, ElDI-V; Liechtenstein: Signaturgesetz, EiDAS), gewährleistet SWISSSIGN die Einhaltung der betreffenden Vorgaben und Ausführungsbestimmungen. Die SWISSSIGN untersteht insoweit der Aufsicht der zuständigen Stellen (Schweiz: Anerkennungsstelle KPMG

Schweiz; Liechtenstein: Amtes für Kommunikation mit Audit durch TÜV IT Nord, Deutschland) und es erfolgen Audits und Prüfungen unter Beachtung der für die betreffenden Zertifikate relevanten Standards (z.B. ETSI, CA Browser Forum) und gesetzlichen Regelungen.