Als führender Vertrauensdiensteanbieter in Europa ermöglichen wir die innovativsten, digitalen Geschäftsmodelle.

White Paper

Vertragliche Beziehung eines Zertifizierungsanbieters bzw. Vertrauensdienstes zum Kunden und Signierenden

Swisscom Trust Services

Swisscom Trust Services

Inhalt

Einleitung

In der vertraglichen Beziehung zu unseren Kunden erleben wir immer wieder Kommentierungen unserer Standardvertragstexte, die wir in der Regel ablehnen müssen, da die vertraglichen Beziehungen, die wir als Zertifizierungsanbieter bzw. Vertrauensdienst mit Signierenden und Kunden haben, dem widersprechen. Im Folgenden möchten wir Hintergründe zu der vertraglichen Stellung eines Zertifizierungsdienstes bzw. Vertrauensdienstes näher erläutern.

Der Zertifizierungs- bzw. Vertrauensdienst

In der Signaturgesetzgebung der Schweiz (ZertES, https://www.admin.ch/opc/de/classified-compilation/20131913/index.html) bzw. der EU (eIDAS, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32014R0910) delegiert der Staat bestimmte Aufgaben im Zusammenhang mit der elektronischen Signatur im Rahmen einer Akkreditierung an den Zertifizierungsdienst (Schweiz) oder den Vertrauensdienst (EU). Das sind – wie die Swisscom – in der Regel nicht-staatliche Organisationen, die gesetzlich und regulatorisch geregelte Aufgaben wahrnehmen.
Die Zertifizierungs- und Vertrauensdienste müssen ihre Praktiken und Abläufe, wie sie einen Dienst ausführen, in einem sogenannten "CP/CPS" (Certificate Policy/Certificate Practise Statement) Dokument beschreiben. Die Dienste werden nicht nur zu Beginn der Tätigkeit, sondern regelmässig durch staatlich anerkannte Auditoren auditiert und die Anerkennungsstelle (Schweiz) bzw. Aufsichtsstelle (EU) des Staates entscheiden anhand der Audits über die Zulassung, Weiterbetrieb oder Erweiterung der Zertifizierungsdienste und Vertrauensdienste. Neben den allgemeinen gesetzlichen Vorgaben müssen zahlreiche Normen der europäischen Standardisierungsstellen ETSI und CEN eingehalten werden.
Der Staat publiziert die Einhaltung der Normen und Auditstandards und damit auch die Zulassung als anerkannter Zertifizierungs- bzw. Vertrauensdienst auf seinen Webseiten:

- **Schweiz:** https://www.sas.admin.ch/sas/de/home/akkreditiertestellen/akkrstellensuchesas/pki.html
- **EU (Trust List):** https://webgate.ec.europa.eu/tl-browser/#/tl/AT

Darüber hinaus gibt es auch noch private Anbieter von Validierungsdiensten, die die Zulassung von Anbietern publizieren und damit anzeigen können, welche Signaturen gültig sind oder nicht. Die Zulassung richtet sich in der Regel nicht oder nicht nur an die Auflagen des Staates sondern die privaten Auflagen dieses Unternehmens. Ein Beispiel ist z.B. Adobe mit seiner "Trust List (AATL)": https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html

Für wen wird der Zertifizierungs- bzw. Vertrauensdienst erbracht?

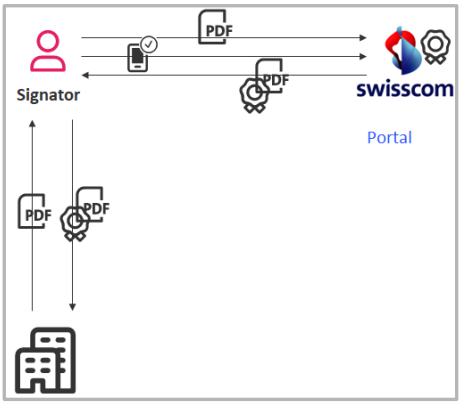
Der Zertifizierungs- bzw. Vertrauensdienst ist verpflichtet, seine Dienstleistung dem zukünftig Signierenden zur Verfügung zu stellen, d.h. die Person entsprechend zu identifizieren und zu registrieren, treuhänderisch für diese Person das Signaturzertifikat bzw. den privaten Schlüssel zum Signaturzertifikat im Falle einer Fernsignatur zu verwalten und sicherzustellen, das das Dokument, welches diese Person in der Signaturapplikation sieht, auch tatsächlich durch Auslösung der Signatur signiert wird (und z.B. nicht im Hintergrund vertauscht wird). Im Rahmen der Fernsignatur muss daher die Authentifizierung zur Freigabe einer Signatur immer direkt gegenüber dem Zertifizierungs- bzw. Vertrauensdienst erfolgen. Es muss nach der CEN Norm 419 241 das sogenannte "Sole Control", also der alleinige Zugriff und Steuerung des privaten Schlüssels sichergestellt werden.
Der Gesetzgeber stellt mit dem Zertifizierungs- und Vertrauensdienst sicher, dass der Signierende die notwendige Sicherheit in der Ausführung seiner Tätigkeit hat und die Prozesse ordnungsgemäss ablaufen. Auch die Verfügbarkeiten des Dienstes und der Datenschutz werden regulatorisch geregelt, sowie die Archivierungsvorschriften und der sichere Betrieb bis hin zu den Regelungen bei Einstellung des Betriebes. Der Zertifizierungs- und Vertrauensdienst muss sich insgesamt bei der Ausübung an alle auf ihn anwendbare Gesetze halten (ETSI EN 319 401). Genaue Informationen zum Umfang und Detail eines Audits ergibt sich z.B: aus https://www.enisa.europa.eu/publications/tsp-conformity-assessment.

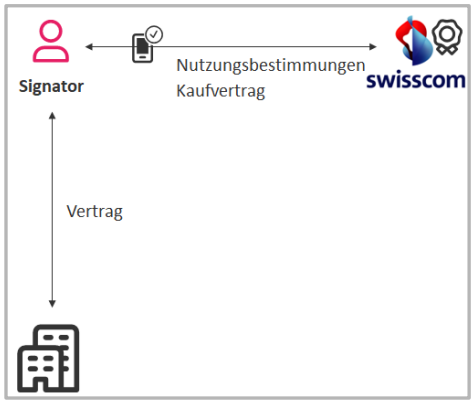
Neben dem Signierenden muss der Empfänger (die sogenannte „Relying Party“) der Signatur vertrauen können und sich darauf verlassen können, dass sie diese prüfen kann und dieser dann auch vertrauen kann.

Diese Aspekte sind in den Nutzungsbestimmungen geregelt, die jeder Signierende vor Erstellung der Signatur bereits bei der Registrierung akzeptieren muss. Swisscom hat somit als Zertifizierungs- und Vertrauensdienst über die vom Signierenden akzeptierten Nutzungsbestimmungen in Bezug auf die Erstellung einer Signatur ein direktes Vertragsverhältnis nur mit dem Signierenden und nicht mit der Partei, die z.B. die Signatur betreibt und sie dem Signierenden zur Verfügung stellt.
Zusammengefasst ist somit der Zertifizierungsdienst bzw. Vertrauensdienst eine Vertrauensvolle Dritte Partei unter der Kontrolle des Staates.

Verantwortung eines Zertifizierungs- bzw. Vertrauensdienstes

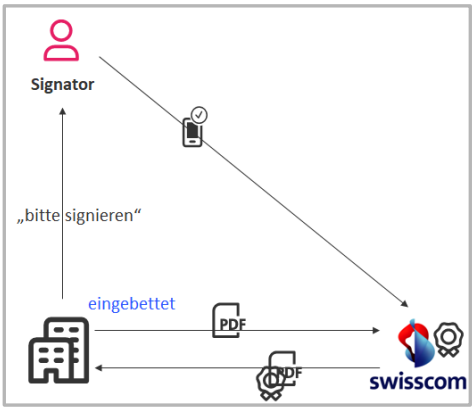
Der Zertifizierungs- bzw. Vertrauensdiensteanbieter ist verantwortlich für die gesamte Signaturstrecke („end2end"), d.h. angefangen von der Registrierung einer Person für den Dienst, bis hin zur Signaturapplikation und Durchführung der (Fern-)signatur und der Sicherstellung der Validierungsmöglichkeit. D.h. er haftet dafür, dass ein Empfänger eines signierten Dokumentes sich auf die Gültigkeit der Signatur verlassen kann.
In der Vergangenheit bot der Zertifizierungs- oder Vertrauensdienst nur Signaturkarten an oder bot alle Dienste selber an. D.h. sollte z.B. ein Signierender ein Dokument für eine Bank unterzeichnen, so händigte die Bank ihm das Dokument aus und bat den Signierenden, dieses elektronisch zu signieren und anschliessend signiert wieder bei ihr einzureichen:

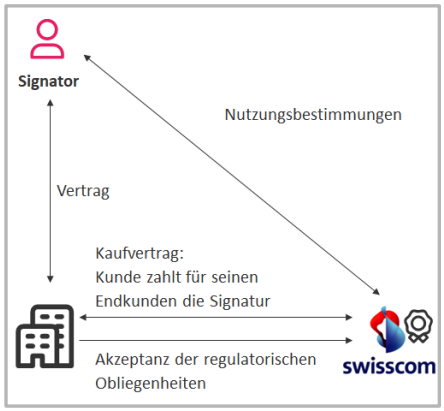




Der Signierende (Signator) schliesst in solchen klassischen Szenarien einen Kaufvertrag für die Dienstleistung einer Signatur mit dem Zertifizierungs- bzw. Vertrauensdienst ab und führte komplett mit diesem die Signatur durch.

Von diesem klassischen Modell wird heute häufig abgewichen. Typischerweise zahlt heutzutage nicht mehr der Signierende selber für die Signatur, sondern die Organisation, die diese Signatur für den Verkaufsabschluss benötigt, z.B. eine Bank oder ein Immobilienmakler. Um einen Kunden nicht zu verlieren und direkt in einer Online-Transaktion zu behalten, wird die Signaturapplikation selber auch nicht mehr vom Zertifizierungs- oder Vertrauensdienstleister betrieben, sondern dieser lagert diesen Teil der Dienstleistung an einen Dritten aus, z.B. einer Bank, die die Signaturmöglichkeit direkt ihren Kunden bieten möchte. Häufig betrifft das nicht nur die Signaturapplikation, sondern auch die Registrierung und Identifikation oder sogar Teile der Willensbekundung zur Signatur (Authentisierung).
Sobald Teile des „end2end" Signaturprozesses ausgelagert werden, ist der Zertifizierungs- bzw. Vertrauensdienst seitens des Gesetzgebers verpflichtet, diese Auslagerungen so zu kontrollieren, dass die Einhaltung der Regularien und Gesetze und damit auch die Nutzungsbestimmungen eingehalten werden können.
Swisscom wird somit seinem Kunden, der einen Teil der Signaturkette, z.B. die Signaturapplikation, übernehmen will und diese in seinem Workflow einbauen will, Auflagen machen. Sofern der Kunde auch noch Identifikations- oder gar Registrierungsaufgaben übernehmen wird, ist ein kompletter Delegationsvertrag notwendig häufig kombiniert mit einer Auditierung oder einer Anmeldung des Registrierungsverfahrens bei der Konformitätsbewertungsstelle. Der Kunde kauft mit der Dienstleistung „Fernsignatur von Swisscom" somit das Recht ein, selber eine Signaturapplikation im Sinne der Regularien und Vorschriften von Swisscom für den Signierenden zu betreiben und über die Schnittstelle entsprechend die Signaturleistung für diese Signaturapplikation zu erhalten. Ggfs. kann der Kunde diese Leistung auch an Dritte, z.B. den Signierenden wiederverkaufen:





Der Kunde reicht somit den Signaturwunsch des Kunden weiter. Vertraglich gelten somit die Nutzungsbestimmungen zwischen Swisscom und dem Signierenden in der Ausführung der Signatur.

Aspekte des Datenschutzes (auch DSGVO)

Swisscom hat einen Vertrag mit dem Signierenden und bearbeitet aufgrund der Zustimmung zu den Nutzungsbestimmungen und den darin enthaltenen Datenschutzbestimmungen seine Daten. Diese Daten verarbeitet Swisscom somit im Sinne des Datenschutzgesetzes als Controller und nicht im Auftrag seines Kunden, der dem Signierenden eine Signaturapplikation für die Swisscom Fernsignatur zur Verfügung stellt. Das gilt im übrigen auch für die RA-Agenten, die eventuell der Kunde im Rahmen der Nutzung der RA-App stellt. Diese wurden von Swisscom identifiziert, geschult und zu Agenten ernannt und haben gegenüber Swisscom ihre Einwilligung zur Datenverarbeitung im Rahmen der Nutzungsbestimmungen gegeben.
Swisscom hat die Verantwortung für die Archivierung und Löschung dieser Daten und darf Fremden ohne Zustimmung auch keine Einsicht in diese Daten geben. Sofern der Kunde die Registrierung der Signierenden übernimmt, gibt es zwei Möglichkeiten:

- Er ist selber Controller, da er ein berechtigtes Eigeninteresse für seinen Geschäftsbetrieb hat, diese Daten zu bearbeiten und hat entsprechend die Zustimmung vom Kunden eingeholt. Z.B. eine Bank benötigt die Daten für die Eröffnung eines Bankkontos.
- Er unterzeichnet eine Auftragsdatenverarbeitung mit Swisscom, da er als verlängerter Arm der Swisscom lediglich die Aufgabe der Registrierung übernimmt.

Alle notwendigen Informationen zum Datenschutz werden von Swisscom in den Datenschutzrichtlinien gegeben, welche unter
CH: http://documents.swisscom.com/product/filestore/lib/65335cab-79dc-4baf-8f0c-25eddea674a5/GDPR-CH-de.pdf
EU: http://documents.swisscom.com/product/filestore/lib/1fab0498-3bfa-43de-86c6-ae98f1dbcca2/GDPR_EU-de.pdf
publiziert. Da Swisscom die Daten der Signierenden sicher verwaltet, werden an Dritte (somit auch an Kunden, die Signaturapplikationen zur Verfügung stellen), keine Details zum Sicherheitsdispositiv dieser Datenverarbeitung bekannt gegeben, aus denen sich dann ggfs. sogar ein Risiko eines Data Breach ergeben könnte.

Datenschutz – Europa – Schweiz

Mit dem Facebook-Urteil (Rechtssache C-311/18 vom 16.7.2020) wurde nochmals aufgrund des «Clarifying Lawful Overseas Use of Data Act – Cloud Act» die Verpflichtung der US Internet Firmen und IT-Dienstleister angegriffen, US Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt, sondern in Schweizern oder EU Rechenzentren. Hierbei reicht auch eine blosse Zweigniederlassung in den USA aus.
Mit der Swisscom (Schweiz) AG und der Tochtergesellschaft Swisscom IT Services Finance S.E. handelt es sich um Firmen, die ausschliesslich nach schweizerischen bzw. EU Recht handeln und keine Niederlassungen in den USA haben und somit nicht dem Cloud Act unterworfen sind. Damit erfolgt kein Zugriff der US Behörden auf die Signaturdaten.
Hierbei ist insbesondere in der EU zu beachten, dass die Schweiz als Staat mit adäquatem Datenschutzniveau in Bezug auf die DSGVO gilt: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en .

Signaturapplikation, Plattformservice und Partnerkonzept

Swisscom offeriert als Swisscom Trust Services keine Signaturapplikationsleistungen, die der Kunde in seine eigene Applikation oder eigenen Workflow einbinden kann. Swisscom Trust Services ist eine reine Plattformdienstleistung, die standardisiert die gesetzlich vorgeschriebenen Signaturdienstleistungen allen Signierenden als Fernsignatur zur Verfügung stellt. Signaturapplikationen selber werden durch Swisscom Partner erstellt oder sogar vom Endkunden selber entwickelt. Projektverträge in Bezug auf die Einbettung der Signaturapplikationssoftware in die Kundenumgebung sind somit mit den Partnern von Swisscom abzuschliessen. Mit der Ausnahme von Docusign ermöglicht Swisscom allen Partnern auch ein Gesamtpaket (Signaturapplikation und Fernsignaturen) als Wiederverkäufer dem Kunden anzubieten. Swisscom Trust Services erbringt somit mit Ausnahme von gesonderten Beratungsleistungen im Vorfeld keine projektspezifischen Leistungen im Rahmen der Signatur oder der Registrierung.
Für alle Kunden und Partner gilt das gleiche Leistungs- und Preisverzeichnis.

Standardverträge

Swisscom bietet Standardserviceverträge, die es dem Kunden ermöglichen, eine eigene Signaturapplikation zu erstellen oder die Signatur eines Swisscom Partners zu nutzen und dem Kunden im eigenen Workflow eine Signatur anzubieten.

Mit der Auslagerung von Prozessen im end2end Signaturprozess an Dritte, z.B. auch an Kunden, unterliegen auch die Verträge dem Audit. Es wird überprüft, ob diese Verträge die notwendigen regulatorischen Auflagen enthalten. Im Falle einer Signaturapplikation sind das z.B. folgende Punkte:

- Es muss sichergestellt werden, dass der Signierende das Dokument sieht, welches er dann auch signiert. Die Signaturapplikation darf nicht so manipuliert werden, dass der Signierende Dokument A sieht, aber über die Fernsignaturschnittstelle Dokument B signiert wird.
- Diese Manipulationen sind so weit möglich auszuschliessen: Das geschieht z.B. dadurch, dass Administratoren, die solche Manipulationen durchführen könnten einen kontrollierten, privilegierten Zugang erhalten und dass die Signaturapplikation auf einer Plattform läuft, die entsprechend gegen Missbrauch nach dem Stand der Technik geschützt wird.
- Die Kommunikation zwischen Signaturapplikation und Fernsignaturdienst ist entsprechend zu schützen und zu verschlüsseln. Die dafür benötigten Zertifikatsschlüssel müssen sorgsam verwahrt sein.

Die diesbezüglichen Auflagen können jederzeit von Swisscom bzw. den Auditoren überprüft werden. Diese Bestimmungen sind verpflichtend durch Unterzeichnung der «Konfigurations- und Annahmeerklärung» bei jedem Servicevertrag einzuhalten.
Im Falle einer Auslagerung von Registrierungsaufgaben sind weitere regulatorische Auflagen einzuhalten, die im Rahmen eines Delegationsvertrages, eines RA-Agenturvertrages und Umsetzungskonzeptes im Einzelnen festgehalten und vom Kunden akzeptiert werden. Diese Dokumente werden bei einem Audit als Standarddokument vorgelegt und die Inhalte dürfen daher nicht geändert und durch Nebenabreden entkräftet werden.

Auflagen bzw. Änderungswünsche des Kunden

Häufig wünscht der Kunde noch Zusätze oder Auflagen in den Verträgen mit Swisscom, die typischerweise anderweitig in einer Auftragsverarbeitung oder einer projektspezifischen Softwareerstellung angewendet werden.
Aus obigen Gründen muss Swisscom als Zertifizierungs- und Vertrauensdienst und Plattformdienst solche Anfragen ablehnen, wie z.B.:

- **DSGVO – Auftragsdatenverarbeitung:** Da Swisscom keine Daten des Kunden bearbeitet, sondern selbst Controller Status hat, wird keine Auftragsdatenverarbeitung unterzeichnet.
- **Auditrechte**: Swisscom hat ein direktes Vertragsverhältnis mit seinen Signierenden und wird insbesondere die nicht öffentlichen Daten keinem Dritten (mit Ausnahme der vorgeschriebenen Auditoren, Aufsichtsstellen, staatlichen Gerichten) zugänglich machen. Alle Auditbegehren eines Kunden für den Signaturservice sind somit aus Datenschutzgründen und Sicherheitsgründen abzulehnen.
- **Einsichtsrechte in Architektur, Offenlegung von technischen Realisierungsdetails (z.B. Backup, Programmier- und Sicherheitsdetails wie Zugriffsschutz, Zugänge, kryptographische Verfahren, etc.):** Alle Hinweise zur Praxis der Dienstausübung veröffentlicht Swisscom in ihrer CP/CPS (https://www.swisscom.ch/de/business/enterprise/angebot/security/digital_certificate_service.html). Aus Sicherheitsgründen werden weitere Details keinem Kunden herausgegeben, so dass nicht ein Wissen aufgebaut werden kann, um ggfs. zielgerichtet Attacken zu entwerfen. Der Zertifizierungs- und Vertrauensdienst verarbeitet Daten mehrerer Tausend und Millionen Signierender gleichzeitig, es ist nie ein projektspezifisches Vorhaben, sondern ein Plattformdienst.
- **Anschluss an das betriebsinterne Monitoring:** Swisscom veröffentlicht Störungen seines Service über die Webseite https://trustservices.swisscom.com/status-service , die auch im Rahmen des RSS Protokolls abonniert werden kann. Darüberhinausgehende Eingriffe in das System zu Monitoringzwecken werden aus Sicherheitsgründen nicht zugelassen.
- **Kundenspezifische Verfahren zu Incidents und Data Breaches:** Die Verfahren der Swisscom sind im Rahmen des Services festgelegt und auditiert und können nicht kundenspezifisch angepasst werden. Antwortzeiten, z.B. im Falle eines Sicherheitsvorfalles, sind bereits in den geltenden Regularien festgesetzt und können nicht angepasst werden.
- **Desaster Recovery Pläne:** Swisscom offeriert seine Services im Rahmen des SLAs und georedundant. Das Desaster Recovery bis hin zur Aufgabe des Betriebes ist in den beigefügten Basisdokumenten zum Vertrag und in der CP/CPS beschrieben.
- **Besondere Versicherungen:** Swisscom ist aufgrund der geltenden Regularien verpflichtet, eine bestimmte Haftpflichtversicherung abzuschliessen. Darüberhinausgehende oder abweichende Versicherungswünsche werden nicht akzeptiert.
- **Anwendbares Recht:** Swisscom Trust Services wird als Leistungserbringer in der Schweiz für seine Fernsignaturdienste nur das anwendbare Schweizer Recht akzeptieren.
- **Andere Verpflichtungen, z.B. Code of Conduct:** Grundsätzlich sind alle Verträge Bestandteil des Auditumfangs. D.h. alle regulatorisch relevanten Vertragsänderungen müssen dem Auditor gemeldet werden und auch der

Konformitätsbewertungsstelle in beiden Rechtsräumen (Schweiz und EU). Auch vertragliche Zusätze, z.B. eigenes NDA nach einem anderen Rechtsraum oder ein Code of Conduct können Elemente enthalten, die wiederum andere Rechtsverträge aushebeln können. Insofern lehnt Swisscom die Verwendung von nicht freigegebenen eigenen Verträgen und Vertragszusätzen ab. Es ist in der Leistungsvergütung auch kein Rechtsbeistand vorgesehen, der diese Abweichungen und Abhängigkeiten prüfen würde.
Swisscom als staatlicher und grösster IT Konzern hält die Grundsätze für verantwortungsbewusstes Handeln ein und überprüft dieses laufend im Rahmen des internen Kontrollsystems. Nähere Informationen zu den Themen

- Swisscom Code of Conduct
- Swisscom Procurement Policy
- Swisscom Anti-Corruption Directive

Können in den nachfolgenden Links gefunden werden. Überdies verfügt die Swisscom Gruppe über ein ausgezeichnetes Rating im Rahmen der Ecovadis Beurteilung.
Internet (Public)
https://www.swisscom.ch/de/about/governance.html
https://www.swisscom.ch/de/about/nachhaltigkeit/partner.html
https://www.swisscom.ch/de/about/unternehmen/nachhaltigkeit/ziele/ratings-policies-zertifikate.html

Code of Conduct:
https://www.swisscom.ch/content/dam/swisscom/de/about/governance/reglemente/documents/verhaltenskodex-der-swisscom.pdf.res/verhaltenskodex-der-swisscom.pdf

Purchasing-Policy:
https://www.swisscom.ch/content/dam/swisscom/de/purchasing/documents/pdf/Einkaufspolicy_2014_online-DE.pdf.res/Einkaufspolicy_2014_online-DE.pdf

Manche Swisscom Partner als Generalunternehmer haben als Projektpartner einen grösseren Spielraum in der Gestaltung ihrer (projektspezifischen) Verträge. Sofern bestimmte Aspekte wichtig sind, sollte überlegt werden, ob der Gesamtvertrag über einen Swisscom Partner, der z.B. landesansässig ist, abgeschlossen wird.

Audit targets

Dieses Kapitel listet im einzeln die Auditanforderungen. Das Audit wird nach IS/IEC 17021-1:2015 durchgeführt.
Es gibt ein jährliches Audit und ein zweijähriges Rezertifizierungsaudit.
Folgende Normen stehen dabei im Mittelpunkt:

General Provisions
ETSI EN 319 401
ETSI EN 319 411-1
ETSI EN 319 411-2
Qualified Trust Services:
ETSI EN 319 411-1
ETSI EN 319 411-2
ETSI TR 119 400
Electronic Signatures:
ETSI EN 319 411-1
ETSI TR 119 400
ETSI EN 319 412-1
ETSI EN 319 412-2
ETSI EN 319 412-3
ETSI EN 319 412-5
Electronic Seals
ETSI EN 319 411-1
ETSI EN 319 412-3
ETSI EN 319 412-5
Electronic Time Stamps:
ETSI EN 319 421
ETSI EN 319 422
Security Requirements for Trustworthy Systems Supporting Server Signing
DIN EN 419 241-1
ETSI EN 419 251

ETSI TS 119 431-1
EN 419 241-1
EN 412 241-2
EN 412 241-5 SCAL-2 according to EN 419 241-1

Aus Risiko-/Einkaufs-orientierter Sicht sind insbesondere folgende Anforderungen interessant:

Backup/Restore:
EN 419 241-1 General, SRG_BK 1.1, SRG_BK2.1, SRG_BK2.2
Change Management:
EN 419 241-1 SRG_SO1.2
Business Termination:
ETSI TS 119 431-1, OVR-6.4.9-10
Financial Requirements:
ETSI TS 119 431-1, OVR-6.7.2-01
Incident Management and Monitoring:
ETSI 419 241-1, SRG_AA.6.1,
ETSI TS 119 431-1, OVR-6.5.4-02, OVR 6.4.8-01
Legal Requirements:
ETSI TS 119 431-1, OVR-6..4-01, OVR-6.7.15-01, OVR-6.8.3-01, OVR-A.1-01
Network Security:
EN 419 241-1, SRG_SO.1.1, SRC_SA.1.3, SRA_SAP.1.4, SRA_SAP.1.5, SRA_SAP.1.6, SRA_SAP.1.7, SRA_SAP.2.1, SRA_SAP.2.8
ETSI TS 119 431-1, SIG-6.3.1-02, OVR-6.5.2-01, OVR-6.5.5-01, SIG-A.5-04, SIG-A.5-05, SIG-A.5-06, SIG-A.5-07, SIG-A.6-01, SIG-A.6-08
Personnel Security:
EN 419 241-1, SRG_M.1.8
ETSI TS 119 431-1, OVR-6.4.4-01
Physical Security:
EN419 241-1, SRG_M.1.9
ETSI TS 119 431-1, OVR-6.4.2-01, OVR-6.4.2-02
Risk Management:
EN 419 241-1, SRA_SAP.1.2
ETSI TS 119 431-1, SIG-6.4.1-06, OVR-7-05
Information Security:
EN 419 241-1, 6.2.1.1 General, 6.2.1.2 Description, 6.2.2.1 Description
ETSI TS 119 431-1, OVR-6.4.1-01, OVR-6.5.4-01
System Access Management:
EN 419 241-1, SRG_M.1.1 – SRG_M.1.7, SRG_M.1.10, 6.2.3.1 General, 6.2.3.2 Remark, SRG_IA.1.1-SRG_IA.1.4, SRG_IA.2.1, 6.2.4.1 General, SRG_SA.1.1, SRG_SA.1.2, 6.2.5.1 General, SRG_AA.5.1, SRG_AR.2.1, SRG_BK.1.2, SRC_SA.1.4, SRC_SA.1.5, SRC_SA.2.1, SRC_SA.2.2, 6.4.1 General, SRA_SAP.1.3, SRA_SAP.1.3, SRA_SAP.2.2, SRA_SKM.2.6, SRA_SKM.2.7, A.22
ETSI TS 119 431-1, SIG-6.3.1-03, SIG-6.3.1-04, OVR-6.4.3-01, OVR-6.5.1-01, OVR-6.5.3-01, SIG-A.5-03, SIG-A.6-02
Secure Device Provisioning (SDPS)
EN 419 241-1, SRA_SKM.1.1

Weitere Fragen

Wir hoffen Ihnen mit diesem White Paper eine Übersicht zu unserer Notwendigkeit von Standardverträgen als anerkannter Zertifizierungs- bzw. Vertrauensdienst gegeben zu haben.
Für weitere Fragen steht unser Swisscom Trust Services Team Ihnen gerne zur Verfügung:

Swisscom Trust Services AG
Sales Support

Konradstrasse 12
8005 Zürich

Schweiz

https://trustservices.swisscom.com
E-Mail: msc.support@swisscom.com