As the leading trust service provider in Europe, we enable the most innovative digital business models.

White Paper

Contractual Relationship Of A Certification Provider Or Trust Service To The Customer And Signatory

Swisscom Trust Services

Swisscom Trust Services

Content

Introduction....3
The certification/trust service....3
For whom is the certification/trust service provided?....3
Responsibility of a certification/trust service....4
Aspects of data privacy (also GDPR)....5
Data privacy – US – EU – Switzerland....5
Signature application, platform service and partner concept....6
Standard contracts....6
Conditions or change requests of the customer....6
Further questions....8

Introduction

In the contractual relationship with our customers, we repeatedly experience comments on our standard contract texts, which we usually have to reject because the contractual relationships we have as a certification provider or trust service with signatories and customers contradict this. In the following we would like to explain the background to the contractual status of a certification service or trusted third party service in more detail.

The signing process

The signature process is generally carried out by a signature application from a partner of Swisscom Trust Services. It can also be Swisscom itself that provides a signature application. The signature application enables the signer to send the hash (fingerprint) of the document data to Swisscom requesting a signature of this hash and to sign it after explicit approval by the signer. Thus, Swisscom Trust Services has no insight into the document data and acts solely in a B2C relationship contractually on behalf of the signer. The partner or signature application operator provides the necessary means for the signature process and determines through hash generation which data will be signed, creating a signed document from the signed hashes. Swisscom thus creates signatures exclusively on behalf of the signer and not on behalf of the operator of the signature application or the signature application partner or any other third party.
The signatory approves the signature using a signature approval means, a one-factor or, in the case of qualified electronic signatures, a two-factor authentication.

The certification/trust service

In the signature legislation of Switzerland (ZertES, https://www.admin.ch/opc/de/classified-compilation/20131913/index.html) and the EU (eIDAS, https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=celex%3A32014R0910), the state delegates certain tasks related to the electronic signature in the context of accreditation to the certification service (Switzerland) or the trust service (EU). These are - like Swisscom - generally non-governmental organisations that perform tasks regulated by law and regulation. Certification/registration and trust services shall describe their practices and procedures for performing a service in a so-called "CP/CPS" (Certificate Policy/Certificate Practise Statement) document. The services are not only audited at the beginning of the activity, but also regularly by state-recognised auditors. Based on the audits, the recognition authority (Switzerland) or supervisory authority (EU) of the state decides on the approval, continued operation or extension of the certification services and trust services. In addition to the general legal requirements, numerous standards of the European standardisation bodies ETSI and CEN must be observed.
The state publishes the compliance with norms and audit standards and thus also the approval as a recognized certification or trust service on its websites:

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

In addition, there are also private providers of validation services that publish the approval of providers and can thus indicate which signatures are valid or not. As a rule, the approval is not or not only based on the requirements of the state but also on private requirements of this company. One example is Adobe with its "Trust List (AATL)": https://helpx.adobe.com/acrobat/kb/approved-trust-list1.html

For whom is the certification/trust service provided?

The certification or trust service is obliged to make its service available to the future signatory, i.e. to identify and register the person accordingly, to administer the signature certificate or the private key to the signature certificate in the case of a remote signature on behalf of this person and to ensure that the document which this person sees in the signature application is actually signed by authorizing the signature (and e.g. is not exchanged in the background). In the context of remote signatures, the authentication for the release of a signature must therefore always be carried out directly with the certification or trust service. According to CEN standard 419 241, the so-called "sole control", i.e. the sole access and control of the private key, must be ensured.
With the certification and trust service, the legislator ensures that the signatory has the necessary security in the execution of his activity and that the processes run properly. The availability of the service is also regulated, as well

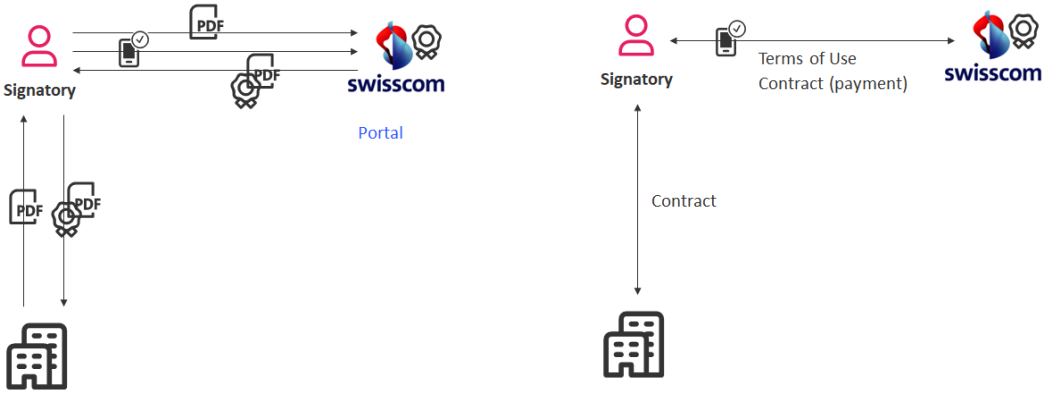
as the archiving regulations, data protection and secure operation, including the regulations in the event of discontinuation of operation. The certification and trust service must comply with all laws applicable to it (ETSI EN 319 401). Precise information on the scope and detail of an audit can be found, for example, at https://www.enisa.europa.eu/publications/tsp-conformity-assessment .

In addition to the signatory, the recipient (the so-called "relying party") must be able to trust the signature and be confident that it can verify it and then trust the signatory.

These aspects are regulated in the terms of use, which each signatory must accept during registration before the signature is created. As a certification and trust service, Swisscom therefore has a direct contractual relationship only with the signatory, and not with the party who, for example, operates the signature and makes it available to the signatory, through the terms of use accepted by the signatory with regard to the creation of a signature.
In summary the certification service and/or trust service is a trusted third party under the regulation of the state.

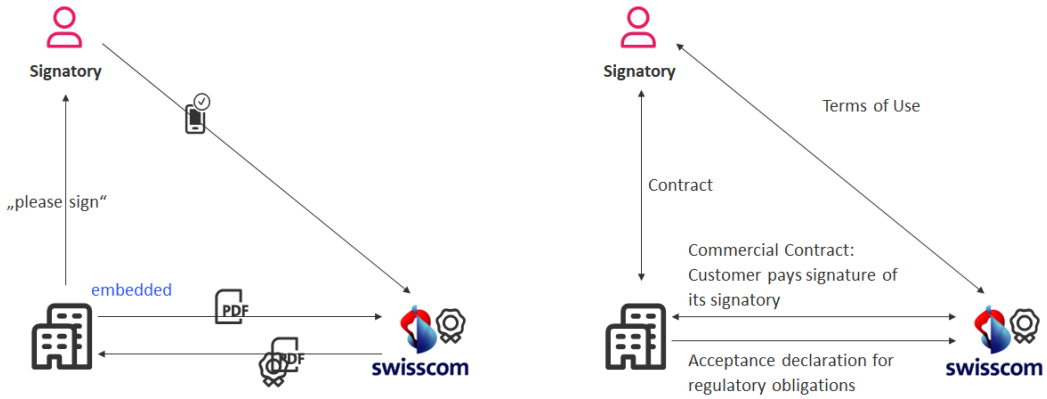
Responsibility of a certification/trust service

The certification/trusted service provider is responsible for the entire signature chain ("end2end"), i.e. starting with the registration of a person for the service, through to the signature application and execution of the (remote) signature and ensuring the possibility of validation. In other words, he is responsible for ensuring that a recipient of a signed document can rely on the validity of the signature.
In the past, the certification or trust service only offered signature cards or offered all services itself. This means that if, for example, a signatory was to sign a document for a bank, the bank would hand the document over to him and ask the signatory to sign it electronically and then sign it and return it to the bank:



In such classic scenarios, the signatory concludes a purchase contract for the service of a signature with the certification or trust service and executes the signature completely with the latter.

Today, there are frequent deviations from this classic model. Typically, today it is no longer the signatory himself who pays for the signature, but the organization that needs the signature to complete the sale, e.g. a bank or a real estate agent. In order not to lose a customer and keep them directly in an online transaction, the signature application itself is no longer operated by the certification or trust service provider, but the latter outsources this part of the service to a third party, e.g. a bank that wants to offer the signature option directly to its customers. Often this not only concerns the signature application, but also the registration and identification or even parts of the declaration of intent to sign (authentication).
As soon as parts of the "end2end" signature process are outsourced, the certification/trust service is obliged by law to control these outsourcings in such a way that compliance with the regulations and laws and thus also the terms of use can be ensured.
Swisscom will thus impose conditions on its customers who wish to take over part of the signature chain, e.g. the signature application, and integrate it into their workflow. If the customer will also take over identification or even registration tasks, a complete delegation agreement is necessary, often combined with an audit or notification of the registration procedure to the conformity assessment body. With the "Remote signature service" from Swisscom, the customer thus purchases the right to operate a signature application for the signatory himself in accordance with Swisscom's rules and regulations and to receive the signature service for this signature application via the interface. If necessary, the customer may also resell this service to third parties, e.g. the signatory:



As a relay station the customer passes the request to sign through to the trusted service provider.
The terms of use between Swisscom and the signatory are thus contractually valid in the execution of the signature.

Aspects of data privacy (also GDPR)

Swisscom has a contract with the signatory and processes its data on the basis of its agreement to the conditions of use and the data protection provisions contained therein. Swisscom therefore processes this data in accordance with the Data Protection Act as controller and not on behalf of its customer, who provides the signatory with a signature application for the Swisscom remote signature. Incidentally, this also applies to the RA agents that may be provided by the customer within the scope of using the RA app. These have been identified, trained and appointed as agents by Swisscom and have given Swisscom directly their consent to data processing within the framework of the terms of use.
Swisscom is responsible for archiving and deleting this data and may not allow third parties to view this data without consent. If the customer takes over the registration of the signatories, there are two possibilities:

- It is a controller himself, as it has a legitimate self-interest for its business operations to process this data and has obtained the consent of the customer accordingly. For example, a bank needs the data to open a bank account.
- In case it does not need the registered data for own purposes it signs an order data processing contract with Swisscom, as it, as the “extended arm” of Swisscom, only takes part on the task of registration.

All necessary information on data protection is provided by Swisscom in the data protection guidelines, which are available at
CH: http://documents.swisscom.com/product/filestore/lib/b95cda36-6275-426c-ae8b-d5104ea11dbe/GDPR-CH-en.pdf
EU: http://documents.swisscom.com/product/filestore/lib/f3daec38-8db9-465c-9c81-e4ba8f30143e/GDPR_EU-en.pdf
As Swisscom manages the data of the signatories securely, no details of the security arrangements for this data processing are disclosed to third parties (thus also to customers who provide signature applications), in order to avoid a risk of data breach.

Data privacy – US – EU – Switzerland

With the Facebook ruling (Case C-311/18 of 16.7.2020), the obligation of US Internet companies and IT service providers to guarantee US authorities access to stored data even if the data is not stored in the USA but in Swiss or EU data centres was again attacked on the basis of the "Clarifying Lawful Overseas Use of Data Act - Cloud Act".
Swisscom (Switzerland) Ltd and its subsidiary Swisscom IT Services Finance S.E. are companies that operate exclusively under Swiss or EU law and have no branches in the USA and are therefore not subject to the Cloud Act. This means that the US authorities do not have access to the signature data, and it should be noted that Switzerland is considered a country with adequate data protection in relation to the DSGVO, particularly in the EU: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en .

Confidentiality Principles

Various laws in the banking sector, e-health, defence, etc., require data confidentiality. These confidentiality regulations do not generally apply to the signature service of Swisscom Trust Services because they do not create signatures on behalf of the obligated party under these laws but directly from the signer in a B2C relationship. The obligated party is often the operator of the signature application and provides it to the signer. The data transmitted for signature only contains the hash of the data and never the content of a document. Therefore, Swisscom Trust Services receives all relevant (personal) data directly from the signer.

Signature application, platform service and partner concept

As Swisscom Trust Services, Swisscom does not offer signature application services that the customer can integrate into its own application or workflow. Swisscom Trust Services is a pure platform service that makes the legally required signature services available to all signatories as remote signatures in a standardised form. Signature applications are created by Swisscom partners or even developed by the end customer himself. Project contracts relating to the embedding of the signature application software in the customer environment must therefore be concluded with Swisscom partners. Except for the signature application Docusign, Swisscom also enables all partners to offer a complete package (signature application and remote signatures) as resellers to the customer. Swisscom Trust Services therefore does not provide any project-specific services in the context of the signature or registration, except for separate consulting services in advance.
The same service and price list applies to all customers and partners.

Standard contracts

Swisscom offers standard service contracts that enable the customer to create his own signature application or to use the signature of a Swisscom partner and offer the customer a signature in its own workflow.
With the outsourcing of processes in the end2end signature process to third parties, e.g. also to customers, the contracts are also subject to audit. It is checked whether these contracts contain the necessary regulatory requirements. In case of a signature application these are e.g. the following points:

- It must be ensured that the signer sees the document, which he then signs. The signature application must not be manipulated in such a way that the signing party sees document A, but that document B is signed via the remote signature interface.
- These manipulations are to be ruled out as far as possible: This is done, for example, by giving administrators who could carry out such manipulations privileged access and by running the signature application on a platform that is protected against misuse according to the state of the art.
- The communication between signature application and remote signature service must be protected and encrypted accordingly. The certificate keys required for this purpose must be stored carefully.

The relevant conditions can be checked at any time by Swisscom or the auditors. It is mandatory to comply with these provisions by signing the "Configuration and Acceptance Declaration" with each service contract.
If registration tasks are outsourced, further regulatory requirements must be complied with, which are set out in detail in a delegation agreement or RA agency contract and implementation concept and accepted by the customer. These documents are presented as a standard document during an audit and the contents may therefore not be changed and invalidated by collateral agreements.

Conditions or change requests of the customer

Frequently, the customer still wishes to have additions or conditions in the contracts with Swisscom, which are typically applied elsewhere in an order processing or project-specific software development.
For the above reasons, Swisscom as a certification and trust service and platform service must reject such requests, such as :

- **DSGVO - data processing agreement:** As Swisscom does not process any data of the customer, but has controller status itself, no data processing agreement is signed.

- **Audit rights**: Swisscom has a direct contractual relationship with its signatories and in particular will not make non-public data available to any third parties (with the exception of the prescribed auditors, supervisory bodies, state courts). All audit requests by a customer for the signature service must therefore be rejected for data protection and security reasons.
- **Rights of inspection in architecture, disclosure of technical implementation details (e.g. backup, exact location of the datacenters, database software in use, programming and security details such as access protection, accesses, cryptographic procedures, etc.):** Swisscom publishes all information on the practice of service provision in its CP/CPS (https://www.swisscom.ch/de/business/enterprise/angebot/security/digital_certificate_service.html). For security reasons, no further details are disclosed to any customer, so that no knowledge can be built up to design attacks in a targeted manner if necessary. The certification and trust service processes data of several thousand and million signatories simultaneously; it is never a project-specific project, but a platform service.
- **Confidentiality agreements:** Swisscom has a direct contractual relationship with its signatories and by use of the hash in the signature no third party data is shared. The confidentiality between the signatory and Swisscom is ensured by the terms of use and the appropriate laws (eIDAS/ZertES) under which Swisscom operates its trust service. Thus, Swisscom will not sign any additional confidentiality agreement.
- **Connection to internal monitoring:** Swisscom publishes any incidents in its service on the https://trust-services.swisscom.com/status-service website, which can also be subscribed to using the RSS protocol. For security reasons, no further interventions in the system for monitoring purposes are permitted.
- **Customer-specific procedures for incidents and data breaches:** Swisscom's procedures are defined and audited as part of the service and cannot be adapted to customer-specific requirements. Response times, e.g. in the event of a security incident, are already defined in the applicable regulations and cannot be adapted.
- **Disaster recovery plans:** Swisscom offers its services within the framework of the SLA and georedundant. Disaster recovery up to and including the discontinuation of operations is described in the basic documents attached to the contract and in the CP/CPS.
- **Special insurance:** Swisscom is obliged by the applicable regulations to take out a specific liability insurance policy. Insurance requests e.g. that go beyond or deviate from this will not be accepted.
- **Applicable law:** As a service provider in Switzerland, Swisscom Trust Services will only accept the applicable Swiss law for its remote signature services.
- **Other obligations, e.g. Code of Conduct:** In principle, all contracts are part of the audit scope. This means that all regulatory relevant contract changes must be reported to the auditor and to the conformity assessment body in both jurisdictions (Switzerland and EU). Contractual amendments, e.g. an own NDA according to another applicable law or a Code of Conduct may also contain elements which in turn may undermine other legal contracts. In this respect, Swisscom rejects the use of its own contracts and contractual addenda that have not been approved. Nor does the service fee provide for any legal assistance which would check these deviations and dependencies.
  Swisscom as state-owned and largest IT group in Switzerland, complies with the principles of responsible conduct and reviews these on an ongoing basis as part of its internal control system. Further information on the topics
  - - Swisscom Code of Conduct
  - - Swisscom Procurement Policy
  - - Swisscom Anti-Corruption Directive

  can be found in the links below. Furthermore, the Swisscom Group has an excellent rating in the Ecovadis assessment.
  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/en/about/governance/regulations/documents/swisscom-code-of-conduct.pdf.res/swisscom-code-of-conduct.pdf

Purchasing Policy:

- https://www.swisscom.ch/content/dam/swisscom/en/purchasing/documents/pdf/Einkaufspolicy_2014_online-EN.pdf.res/Einkaufspolicy_2014_online-EN.pdf

As project partners, some Swisscom partners as general contractors have greater leeway in drawing up their (project specific) contracts. If certain aspects are important, it should be considered whether the overall contract should be concluded through a Swisscom partner who resides, for example, in the country of the customer.

Audit targets

This chapter lists the audit targets. The audit is done according to IS/IEC 17021-1:2015**.**
Yearly surveillance audit, 2-year recertification audit.
Following regulations will be audited:

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

Interesting topics from risk oriented view are:

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

Further questions

We hope that this white paper will give you an overview of our need for standard contracts as a recognised certification/trust service.

Our Swisscom Trust Services team will be happy to answer any further questions you may have:

Swisscom (Switzerland) AG
Sales Support

Konradstrasse 12

8005 Zurich

Switzerland

https://trustservices.swisscom.com
e-mail: msc.support@swisscom.com