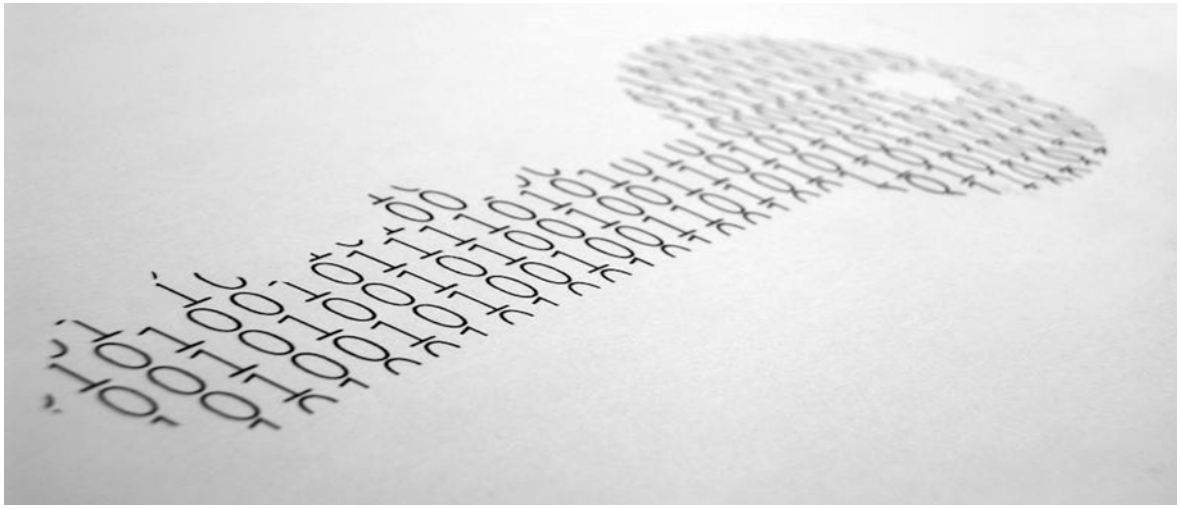

Notes concerning the legal significance of SwissSign certificates

White Paper

SwissSign AG
Sägereistrasse 25
CH-8152 Glattbrugg

hereafter referred to as the "SwissSign"

Glattbrugg, 6 March 2015

1. Introduction

SwissSign AG is a provider of digital certificates domiciled in Switzerland. It operates public key infrastructure (PKI) for a broad spectrum of certificates. Alongside various types of SSL certificates, it issues certificates for email encryption, secure login and digital signatures. SwissSign AG offers its certificate products and services in Switzerland and abroad.

2. Accreditation in Switzerland

SwissSign AG has a special status in Switzerland, as it has been a "recognised provider of certificate services" for the issue of qualified certificates under the Swiss Federal Electronic Signatures Act (ESA) for a number of years. This enables SwissSign AG to issue qualified certificates and products for qualified electronic signatures, which have an enhanced validity under Swiss law. SwissSign issues e.g. the SuisseID, with which it is possible to create a qualified electronic signature using its qualified certificate, which is equivalent to a handwritten signature under the Swiss Code of Obligations. However, recognition also enables SwissSign to issue digital certificates for businesses and organisations for electronic invoicing (OEIDI) and archival (BRO) compliant with Swiss law. The details are regulated in the relevant Swiss legislation and implementing provisions.

The remaining certificate products and services are not recognised. However, the certifications associated with recognition (e.g. ISO 27001, ETSI TS 101456, ETSI TS 101862, ETSI TS 102023, ETSI TS 101861, SR943.03 (ESA), SR943.032 (ESAO), SR943032:1:2005 (TAV)) guarantee a controlled quality and compliance with the relevant international technical standards for all certificates offered by SwissSign AG.

3. Recognition of qualified certificates abroad

As regards the regulation of qualified certificates (SuisseID) and qualified electronic signatures, the ESA in principle follows the requirements of European law (Directive 1999/93/EC of 13 December 1999 on a Community framework for electronic signatures). Similarly, the international recognition of the providers of certificate services originating from other countries or of the qualified certificates issued by them requires either unilateral recognition of a country by law or multilateral recognition by treaty adhered to by various countries. Within the EU, the forthcoming eIDAS Regulation will replace unilateral recognition with an act of Community law. Article 7(1) of the EU Directive provides for (a) accreditation in a Member State and compliance with the prerequisites laid down by the Directive and (b) the guarantee by a provider established in a Member State for a provider established in the third country, in addition to recognition under the terms of bilateral or multilateral agreements. The ESA envisages the conclusion of international treaties as a recognition option for Switzerland; at present, no such agreement to which Switzerland is a party is in force. SwissSign is not accredited in a EU Member State and is not associated with a foreign provider within the meaning of the Directive. Other countries are not known to recognise unilaterally qualified certificates issued according to the ESA.

The European EiDAS Regulation will attempt, at least within Europe, to recognise digital signatures also from other countries. Similar efforts are also being pursued on global level by the UN (UNCITRAL) with a model law on eCommerce. Until the regulations and model laws have

reached maturity or been comprehensively implemented and Switzerland has acceded to these instruments, signatures established by SwissSign certificates must not be regarded as equivalent to handwritten signatures within foreign legal systems.

4. Recognition of other certificates (e.g. Gold), legal transactions not subject to formal requirements

The international use of electronic signatures thus appears at first sight to be severely restricted. However, it must be noted that recognition relates predominantly to the equal treatment of handwritten and digital signatures or to the use of digital signatures for administrative purposes. Most legal transactions are not subject to specific formal requirements. In some senses, voluntary compliance with formalities may be beneficial within legal relations (e.g. recognition, facilitation of the burden of proof, protection against hasty action, perpetuation etc.). Formalities are widespread within the areas not subject to formal requirements specifically within international legal relations, even though they are not required under commercial practice. The digital signature of electronic documents may also, depending upon the type of signature, fulfil one or more functions of handwritten signatures even without formal international recognition,[1] and thus have gradual benefits compared to a situation in which no formal arrangements are applied.

In international situations, the private international law of individual countries may contain reference rules concerning the formal validity of legal transactions. For instance, Article 124(2) of the Swiss Federal Act on Private International Law stipulates that contracts are formally valid if they comply in formal terms with the law applicable to the contract or with the law at the place of conclusion. Foreign legal systems contain comparable provisions. Through the application of private international law, foreign laws governing certification and signatures may also apply across borders if reference is made to foreign formal requirements.

According to the national law in foreign countries, qualified electronic signatures from Switzerland cannot be treated as equivalent to qualified electronic signatures [under local law], and thus to handwritten signatures. On the other hand, in certain cases, e.g. in the event that a choice of law in favour of Swiss law is made, the local private international law may provide for the applicability of Swiss formal requirements, with the result that a transaction signed with a qualified electronic signature according to the Swiss ESA may also be formally valid abroad. It is not unusual that contractual parties from third countries elect the Swiss law as the most convenient or "neutral" legal system, which means that none of the contractual parties or none of the persons acting for the contractual parties has its registered office or domicile in Switzerland.

The legal effects of signatures based on qualified certificates are determined in specific individual cases according to statutory requirements and the practice of the courts and administrative authorities from the national legal system competent to make the assessment along with any private agreements in place. Acceptance of a qualified electronic signature created according to the ESA as being equivalent to a handwritten signature is valid only in Switzerland.

Clarification of the legal effects in the specific individual case is a matter for the Customer alone.

[1] See further Simon Schlauri, Elektronische Signaturen, p. 263, para. 833.

5. Discrepancy between acceptance by the law and acceptance for the purposes of application

It is a problem that qualified certificates are frequently accepted as valid by the legal system concerned, whilst software producers (e.g. Adobe PDF, email software providers, etc.) do not by contrast accept these certificates as reliable. Situations may accordingly arise in which a certificate is valid as a matter of law, whilst being classed as "not reliable" or "invalid" by the software. Accordingly, the authorities nowadays are frequently more willing to communicate using e.g. American certificates, which are recognised as reliable in standard software, than with certificates defined under the relevant country's case law.

6. Definition of advanced signatures from a comparative law perspective

Alongside qualified certificates, advanced certificates are also very interesting as evidence in many areas. The requirements under the Swiss ESA applicable to advanced electronic signatures are identical to the requirements laid down by Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, and are also reflected in the general framework laid down by the UNCITRAL (UN) Model Law on Electronic Signatures.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures	Federal Act of 19 December 2003 on certification services in the area of the electronic signature (Electronic Signatures Act, ESA)	UNCITRAL Model Law on Electronic Signatures
For the purpose of this Directive: 2. "advanced electronic signature" means an electronic signature which meets the following requirements:	In terms of the present law: b. advanced electronic signature means an electronic signature which meets the following requirements:	The model describes: 3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if:
(a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory;	1. It is uniquely linked to the holder. 2. It is capable of identifying the holder	(a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person;
(c) it is created using means that the signatory can maintain under his sole control; and	3. It is created using means that the holder can maintain under his sole control.	(b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;
(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;	4. It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;	(c) Any alteration to the electronic signature, made after the time of signing, is detectable; and[2] (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

[2] Any changes to the signature in all cases have the effect that the signature is no longer attributed to the signatory.

Qualified certificates of SwissSign may thus be used without any difficulty for advanced electronic signatures.

Likewise, gold certificates of SwissSign issued to specific persons may be used for advanced electronic signatures. The issuing processes followed by SwissSign for gold certificates ensure that gold certificates comply with the necessary requirements applicable to the creation of advanced electronic certificates.

7. Organisation certificates and time stamps

According to Swiss law (OEIDI), organisation certificates may be used for issues relating to business management under the BRO. These certificates may also be used abroad, although no longer in accordance with the BRO regulation. An organisation wishing to use these certificates – also as a third party – for the processing of business records must be registered in the Swiss Commercial Registry. However, firms may use the certificate abroad as an advanced organisation certificate in order to demonstrate the integrity and irrepudiability of their company documents. This may occur at any place where there are no special provisions on the management of business records as provided for under the Swiss BRO regulation.

8. Conclusion

An advanced signature is sufficient for an estimated >95% of cases arising in commerce and administration.

This means that SwissSign has been able to continue to expand as a leading provider of certificates in Europe. Thanks to the classification of SwissSign certificates as "reliable" by all common email systems, browsers and PDF readers, the organisation certificate itself is well received abroad as evidence of integrity in relation to electronic archiving, as Adobe can automatically examine the signatures for their reliability. Leading groups in Germany explicitly require that inter alia emails be signed with SwissSign certificates as they consider them to provide a high degree of probative force. Even foreign municipal administrations and governmental service providers use Swiss certificates effectively in their business processes.