Chapter 15
Digital Signature

Weyde Lin

15.1 Introduction

The chapter "Digital Signature" covers the use of cryptographic methods and asymmetric cryptography to sign data and provide origin authentication, data integrity, and signer non-repudiation. The signing process involves generating a hash of the data using a cryptographic hashing function, encrypting the hash with the signing party's private key, and sending the data and encrypted hash to the verifying party. The verifying party can determine the validity of the signature by generating a hash of the data and comparing it to the decrypted hash. The digital signature market is expected to grow by around 30% annually over the next few years, with a focus on reducing friction for users and ensuring security. In Switzerland, organizations can either make their digital signature solution for internal use or buy a solution from established companies offering digital signature services.

15.2 Analysis

A digital signature uses cryptographic hashing functions and asymmetric cryptography to sign data. It also provides origin authentication (attribution to a particular individual), data integrity (proof that data has not been tampered with in transit or otherwise), and signer non-repudiation (signers cannot deny that they signed data). It is possible to apply a digital signature to any data, including emails, contracts (e.g., in PDF format), and messages. A qualified electronic signature (QES) is based on a

W. Lin (✉)
Eraneos Switzerland AG, Zurich, Switzerland
e-mail: Weyde.Lin@eraneos.ch

V. Mulder et al. (eds.), *Trends in Data Protection and Encryption Technologies*,
https://doi.org/10.1007/978-3-031-33386-6_15

digital signature. In many legislative frameworks, a QES is the digital equivalent of a handwritten signature.

15.2.1 Definition

Figure 15.1 illustrates the signing and verifying of a digital signature. To digitally sign data, two cryptography functions are used [1, 2]. The first step is to generate a hash (fingerprint) of the data using a cryptographic hashing function (see Hash Functions in Chap. 5). The hash is then encrypted by the signing party using its private key. This encrypted hash is the data's digital signature. Finally, the data and the signature are sent to the verifying party as separate files in a container or embedded in the data (e.g., signed PDF). As part of the verification process, the verifying party generates the hash of the data using the same cryptographic hashing function. Additionally, the verifying party decrypts the signature using the signing party's public key, resulting in a decrypted hash that the signer can only generate. The verifying party can determine whether the digital signature is valid by comparing the decrypted hash with the calculated hash [3]. When a public key is used with a public key certificate (i.e., a certificate that confirms the validity of a public key and contains information about the key owner), it can be identified who signed the document, or it can be proved that it was signed by a specific individual (see Public Key Infrastructure in Chap. 10).

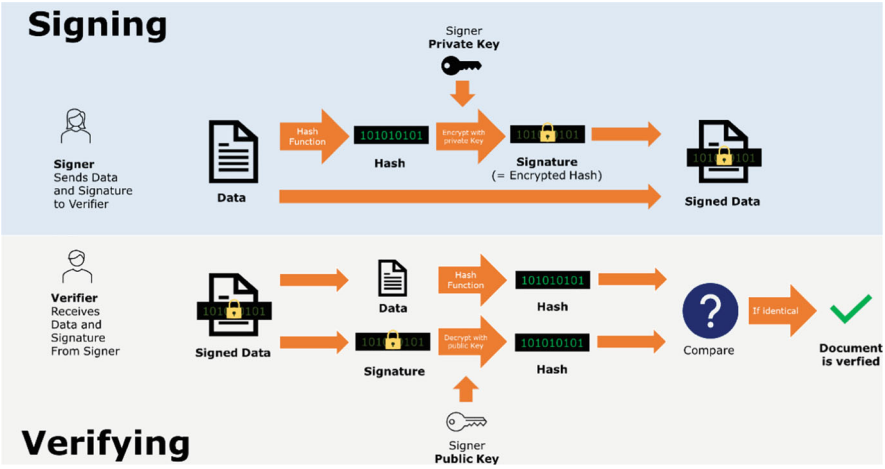

Fig. 15.1 Schematic depiction of digital data signing and verifying process

15.2.2 Trends

With the increasing digitalization of business processes and other processes in general, the ability to apply and verify digital signatures will become increasingly important: the digital signature market size is expected to grow by approximately 30% annually over the next few years [4]. However, it is essential to note that although the EU and Switzerland both have laws regarding qualified electronic signatures (QES), and they are technically compatible, the issue of mutual legal recognition still needs to be fully resolved [5].

Through the use of digital signatures, current paper-based processes will not only be replaced, but they will also be improved, e.g, through audit trails (i.e., tracking documents from beginning to end by digitally signing each process step and saving them alongside the document, ensuring document integrity at each stage and providing legal protection as admissibility in court). For digital and electronic signatures to reach widespread adoption, it is necessary to reduce the friction for the user, for example, by making it possible to generate signatures on mobile devices. The wide acceptance of the digital signature also requires it to be secure. Digital signatures, however, are only as secure as the cryptographical methods (e.g., hash functions) they are based upon. As computation power increases and quantum computing becomes feasible, attacks on underlying cryptographic methods become more effective [6], thereby endangering the security of digital signatures as well (see Post-Quantum Cryptography in Chap. 10).

15.3 Consequences for Switzerland

15.3.1 Implementation Possibilities: Make or Buy

Make: It is important to note that a digital signature is only helpful if all parties use the same standard. As a result, making your digital signature products is only suitable for internal use within an organization which is rarely the case—as such, creating your solution for signing data allows you to control all aspects of the signing process. Military applications may benefit from this technology.

Buy: Many other use cases, especially those in which data is shared with third parties, could benefit from buying from one of the established companies offering digital signature services (e.g., DocuSign, Connective, Adobe Sign, One Span, Evidos, Signicat, Signing Hub, Cryptomathic) or electronic signatures (accredited by ZertES (Federal law on electronic signatures): Swisscom (Schweiz) AG, QuoVadis Trustlink Schweiz AG, SwissSign AG, Bundesamt für Informatik und Telekommunikation BIT [7]). Furthermore, in civil society and the economy, purchasing commercial off-the-shelf (COTS) products from accredited companies is beneficial since they are already certified, meet the legal framework, and should be compatible with other products.

15.3.1.1 Distinction from Electronic Signature

Electronic signatures are sometimes used as synonyms for digital signatures [8]. Despite this, in many legislations (e.g., eIDAS in the European Union or ZertES in Switzerland), the term electronic signature (or e-signature) has a particular meaning. It refers to signing data with the same legal status as a handwritten signature. Electronic signatures are often based on a digital signature. In the EU (eIDAS Regulation [9]) and Switzerland (ZertES [10] and VzertES [11]), this is codified in the law. Electronic signatures can be classified into the following types:

- Qualified electronic signature (QES): QESs is recognized as equivalent to handwritten signatures in Switzerland and the European Union. A QES is based on a digital signature and can be used for documents that require a legal form (e.g., employment contracts)
- Advanced electronic signature (AES): An advanced electronic signature is also based on a digital signature but does not provide liability protection. It defines specific technical requirements for electronic signatures and allows for the signer's identification. AES can be used for documents that do not require a legal form (e.g., rental agreement)
- Basic electronic signature: A handwritten or scanned signature can be used, as well as a signature recorded with a stylus on a tablet. There is no legal or technical requirement for this type of signature.

Everything regarding the usage of the electronic signature can be found in the Federal Act on certification services in the field of electronic signatures and other applications of digital certificates [12].

15.3.1.2 Code Signing

A particular case of the digital signature is code signing, which entails digitally signing executables and scripts. By doing so, it is possible to verify the code's author and ensure that it has not been altered or compromised since it was signed.

15.4 Conclusion

As (business) processes become more digitalized, digital and qualified electronic signatures will play an increasingly important role. As part of these processes, verifying the authorship of some data and whether the data was altered during transport will be necessary. However, a digital signature is only as secure as the cryptographic mechanism underlying it (e.g., hash functions, public key encryption), so the developments in those fields must be studied and adapted for use in digital signatures.

References

1. CSRC Content Editor. digital signature - Glossary | CSRC. https://csrc.nist.gov/glossary/term/digital_signature, July 2022.
2. Kazue Sako. Digital Signature Schemes. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security*, pages 343–344. Springer US, Boston, MA, 2011.
3. Ravneet Kaur and Amandeep Kaur. Digital Signature. In *2012 International Conference on Computing Sciences*, pages 295–301, September 2012.
4. Spiller, Patrik and Hirs, Daniel and Vanhaecht, Jan and Frik, Joran and Maager, Patrick. E-signing. https://www2.deloitte.com/ch/en/pages/strategy-operations/articles/e-signing-market-size-and-vendor-landscape.html.
5. Warum eine Unterschriftenpanne Stadler Milliarden kosten könnte. *SRF 4 News*, September 2021.
6. COMPUTER SECURITY RESOURCE CENTER at NIST. Post-Quantum Cryptography. https://csrc.nist.gov/Projects/post-quantum-cryptography.
7. Swiss Accreditation Service SAS. Electronic signature. https://www.sas.admin.ch/sas/en/home/akkreditiertestellen/akkrstellensuchesas/pki1.html.
8. COMPUTER SECURITY RESOURCE CENTER at NIST. electronic signature. https://csrc.nist.gov/glossary/term/electronic_signature.
9. European Commission. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.
10. Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. https://www.fedlex.admin.ch/eli/cc/2016/752/de.
11. Verordnung über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate. https://www.fedlex.admin.ch/eli/cc/2016/753/de.
12. SR 943.03 - Bundesgesetz vom 18. März 2016 über Zertifizierungsdienste im Bereich der elektronischen Signatur und anderer Anwendungen digitaler Zertifikate (Bundesgesetz über die elektronische Signatur). https://www.fedlex.admin.ch/eli/cc/2016/752/de.