Electronic signature guideline

2023-06-02

Application area and scope of document

The purpose of the document is to serve as a guideline for the member banks of the Swedish Bankers' Association (SBA) when considering relying on electronic signatures. This guideline is not final and may be further elaborated on and aligned.

The scope for these non-binding guidelines is electronic signing tools created according to EU standards, with the primary focus of the Nordic Region. Based on these guidelines, member banks can develop and implement internal guidelines or instructions on how to handle electronic signatures by and between the Swedish Banks and their *Providers of electronic signature tools* or as they see fit.

Consequently, banks may have other requirements in addition to the requirements in this guideline, according to internal instructions.

The guidelines do not relate to digitally signed documents that are printed and scanned or documents signed with a non-valid eID (i.e., a non-valid electronic signature device).

Guidelines

The guidelines are structured in five unique and related guideline areas. To provide context and to serve as an introduction every guideline area is introduced by a user story. The user story is only meant to contextualize the guideline area and is not meant to be an exhaustive list of the guidelines. In the event of inconsistencies between the user story and the guidelines, the guidelines prevail over the user story.

The guideline areas are:

1. Identification of and signature from Signatory.
2. Provider of electronic signature tool.
3. Validation.
4. Portability.
5. Archiving.

Expressions that are explained and defined as part of the "Expressions and definitions section" are written in *italics* in the guidelines.

1. Identification of and signature from Signatory

User story

As a *Relying party*
I need the *SDO (Signed Data Object)* to include in the document who is the actual *Signatory*
So that I can ensure *non-repudiation*

Guidelines

1. It should be possible to identify which *Electronic signature* creation device has been utilized as signing method.
2. The digital signature must be made by the *Signatory* and not the provider of electronic signature tool.
3. The *Electronic signature* creation device, i.e., software or hardware that has been configured to generate an *Electronic signature*, should at least conform to an assurance level of "substantial" or "high" according to *eIDAS*. See examples of requirements of "substantial" assurance level in the appendix.

2. Provider of electronic signature tool

User story

As a *Relying party* of a *SDO*,
I must be able to trust the standards based on the *Provider of electronic signature tool*,
So that *validation* can be efficient and independent of the *Provider of the electronic signature tool*

Guidelines

1. The complete *SDO* should have a standard format according to *ETSI*, for example, *PAdES* or *XAdES* depending on desired usage.
2. The *SDO* should contain proof that the document has not been altered.
3. There should be a clear and visible distinction for the *Signatory* when the *Signatory* is identifying her / himself and when the *Signatory* is signing a document.
4. The principle *"What you see is what you sign"* should be applied. It should be clearly visible for the *Signatory* what content s/he is signing.
5. The *SDO* should contain proof that the document has been sealed by a *Trusted certificate*, by the *Signatory* or the *Provider of electronic signature tool*, and that is has not been altered.
6. There should be proof included in the *SDO* evidencing what parties has signed the document, at an individual level.
7. It is recommended that signatures conform to the level of an *Advanced electronic signature* according to the *eIDAS* regulation. If local law, where the

document is intended to be used, requires *Qualified electronic signature* the signature should conform to the level of a *Qualified electronic signature*.

8. There must be proof that the signature is undeniably done on one unique identifiable document. The association between the signed document and the cryptographic signature must be possible to prove mathematically without the possibility to alter the document without invalidating the signature.
9. It should continuously be ensured that the algorithms used are sustainable and cannot easily be compromised.

3. Validation

<u>User story</u>
As a Relying party of an *SDO*
I need to be able to independently validate legality of the signature
So that i am not dependent on the *Provider of electronic signature tool*.

<u>Guidelines</u>

1. The evidence should not be encrypted to hinder independent *Validation*.
2. All listed guidelines stated in this document, including *Validation* of the signature, must be able to be performed, at any given time during the *SDO*'s life cycle, without the participation and / or help from the *Provider of electronic signature tool*. The *SDO* should not need the addition of external information provided either directly or indirectly from the *Provider of the electronic signature tool* for it to be able to be verified throughout its life cycle.
3. To ensure the *Validation* of a signature it is required that the following information is provided in the *SDO*:
   - Time and date of the signing.
   - IP address connected to the *Signatory*'s *Electronic signature creation device*.
   - Name of the *Signatory*.
   - The signature.
   - The role of the *Signatory* – signer / approver etc.
   - The signing method (see section on "Identification of and signature from Signatory").
   - The hash total of the original document that is connected to the signature above.
4. The evidence included in the *SDO* proving that the *Electronic signature creation device* was not revoked at the time of signing. The evidence (OCSP-file or equivalent) should be protected from manipulation but not be encrypted.

4. Portability

<u>User story</u>
As a *Relying party*
I need to be able to receive and transfer the *SDOs* without compromising the integrity of the *SDO*
So that I can reduce my dependency on *Providers of electronic signature tools*

<u>Guidelines</u>

1. The *SDO* should be transferable in a way that does not compromise the integrity of the *SDO*.

5. Archiving

<u>User story</u>
As a Relying party
I need to be able to store the *SDO* in an archive of my choosing
So that I can retain control of the *SDO* over time

As a Relying Party
I need to be able to ensure LTV (Long Term Validation) of the *SDO* so that it does not lose its integrity
In order to be used in future relations

<u>Guidelines</u>

1. It should be possible to store *SDO*'s outside of the *Provider of electronic signature tools*' technical solution.
2. All *SDO*'s must be able to be stored and transferred digitally in a secure manner. The *Provider of the electronic signature tool* should provide instructions on how to archive the *SDO* in a secure manner, and if and when re-seal needs to be applied.

Governance

The SBA provides a governance structure and change management process for maintaining the Electronic signature guideline. Driving forces for change can be technical developments, legislative modifications, changing business models at suppliers or societal change. Participating banks could also initiate a change to the document for which the process is:

- the participating bank proposes a change that is properly documented to the SBA and explains why the change is necessary.
- the SBA sends the proposal to relevant working groups and sets up a meeting.

- a meeting is held where the proposed change is discussed and accepted or rejected.
- if the proposed change to the guideline is accepted the SBA sends the new version to the participating banks.

Expressions and definitions

Expressions	Definitions
Signed Data Object or SDO	A Signed Data Object is a digitally-signed container for arbitrary message content, i. e., any data that you wish to protect with a personal signature.
Provider of electronic signature tool	Trusted Service Provider or owner of the Certificate used in relation to electronic signature. Usually, third party company issuing digital signing as a service.
Relying Party	An entity receiving the SDO, usually in a legal context. E.g., a Bank.
Signatory	eIDAS Art 3 ” a natural person who creates an electronic signature”.
A third party signature	Any signature initiated by anyone else than the Relying Party of the signed document.
eIDAS	electronic IDentification, Authentication and trust Services is an EU regulation that is included in participating members local legislation. 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.
Qualified electronic signature	As defined in eIDAS art 3 p 12.
Advanced electronic signature	As defined in eIDAS art 26.
Electronic signature	As defined in eIDAS art 3 p 10; “data in electronic form which is attached to or logically associated with other data in electronic form, and which is used by the signatory to sign”.
Qualified electronic seals	As defined in eIDAS Art 38 and 39
Advanced electronic seals	As defined in eIDAS Art 36
Electronic seals	As defined in eIDAS art 3 p 25 ”data in electronic form, which is attached to or logically associated

	with other data in electronic form to ensure the latter's origin and integrity".
Substantial assurance level	As defined in eIDAS art 8.
High assurance level	As defined in eIDAS art 8.
Low assurance level	As defined in eIDAS art 8.
ETSI	European Telecommunications Standards Institute
PAdES	A pdf-file that is signed according to ETSI requirements.
XAdES	An XML-file that is signed according to ETSI requirements.
Trust service provider	As defined in eIDAS art 3 p 19; "a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified trust service provider".
Electronic signature creation device or eID	As defined in eIDAS art 3 p 22; "configured software or hardware used to create an electronic signature".
Trust Service	As defined in eIDAS art 3 p 16, "electronic service normally provided for remuneration which consists of: (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or (b) the creation, verification and validation of certificates for website authentication; or (c) the preservation of electronic signatures, seals or certificates related to those services;
Validation	As defined in eIDAS art 3 p 41, " the process of verifying and confirming that an electronic signature or a seal is valid."
Valid electronic signature creation device or Valid eID	Electronic signature creation device that is accepted by the Relying Party.
Trusted certificate	A trusted certificate is a certificate that is issued to the Provider of electronic signature tool or to a Signatory by a Certification Authority that is included on the EU and European Economic Area trusted lists of qualified trust service providers in accordance with the eIDAS Regulation.
Non-repudiation	Non-repudiation refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract.

Appendix

As an example, the Agency for Digital Government has defined Assurance Level 3 (corresponding to at least "substantial" assurance level as defined in eIDAS) as:

1. The *Signatory*'s identity is verified in the same way as when issuing a satisfactory Swedish identification document.
2. The e-identification can be issued remotely if the issuer has already identified the recipient, for example in connection with the opening of a bank account or at an employment.
3. The signer is identified through, for example, a protected app in a smartphone.
4. There is a high level of trust in the identity, and requirements for two-factor authentication.