Digidentity

eSignatures @ FAQ

Questions & Answers

Title	eSignatures @ FAQ - Questions & Answers
Date	28 February 2023
Author	Sander Remmerswaal
Version	2023-v1
Location	https://www.digidentity.eu/en/documentation/
Classification	Public

Digidentity

Revisions

Version	Date	Author	Changes Made (*)
2023-v1	28 February 2023	Sander Remmerswaal	Initial version

(*) All changes are marked in grey highlight.

28 Feb 2023 11:09 +0100
Den Haag

Digidentity B.V.
QUALIFIED BUSINESS SEAL

Digidentity

Contents

Digidentity

Introduction

Digidentity offers electronic signature services such as Advanced Electronic Signatures, Qualified Electronic Signatures and Qualified Electronic Seals.

We noticed that a number of topics about electronic signatures are raising questions. In this Frequently Asked Question (FAQ) document, we provide answers to those questions.

If you have additional questions about electronic signatures or an answer in this document is unclear or even incorrect, please let us know. Send an e-mail to security@digidentity.com with your question or remark. We will address your feedback as soon as possible.

Digidentity

Questions & Answers

The following sections provide answers for known questions regarding electronic signatures.

Is an Electronic Signature legally binding?

Electronic signatures are generally legally binding, but it depends on the legal jurisdiction. The legal validity of an electronic signature typically depends on whether it satisfies the legal requirements for a valid signature under the applicable laws and regulations.

Also, there may be specific contexts where electronic signatures may not be acceptable or legally enforceable. For example, certain legal documents may require a notarised signature.

In the EU, the legal effects of electronic signatures are laid out in Article 25 of eIDAS. An electronic signature (either simple, advanced or qualified) shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form, or that it does not meet the requirements for qualified electronic signatures.

Qualified Electronic Signatures and Seal (QES) explicitly have the equivalent legal effect of handwritten signatures across all EU Member States.

If the validity of an electronic signature is challenged, the party seeking to enforce the signature would typically bear the burden of proving that the signature is authentic, that the signature was made with the knowledge and consent of the signer, and that it meets any applicable legal requirements. This burden of proof may require presenting evidence such as digital certificates, audit logs, or testimonies from witnesses or experts.

The burden of proof for electronic signatures depends on the legal jurisdiction and the specific context of the signature in question.

Digidentity

How to determine if a digital signature is valid?

You can check the validity of a digital signature in a PDF document using Adobe Acrobat Reader. It is important to determine that the signature was valid at the moment of signing.

When a PDF document is signed with a digital signature, several checks and balances are performed to make sure a valid certificate is being used to sign the document. You cannot digitally sign a document when the certificate has expired. You must first obtain a valid certificate to sign a document.

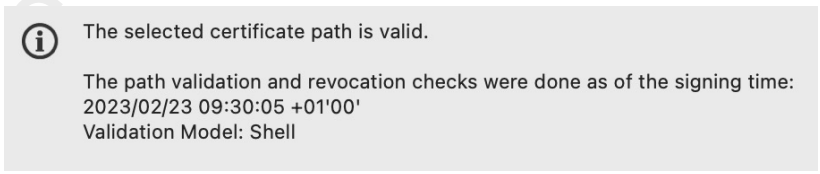
The moment that a document is digitally signed, the signing application verifies if the certificate used to sign the document is valid by checking the revocation status (see section 'What is revocation status service?").

If the certificate is on the Certificate Revocation List (CRL), the certificate is revoked and no longer valid. In the event the certificate is revoked, Digidentity will remove revoked certificates from the Digidentity Wallet so cannot be used to sign documents.

It is important to make a difference between a signature and a certificate. The certificate is used to sign the document. If the certificate was valid at the time of signing, the signature is valid. When the certificate expires or is revoked after signing, the signature remains valid.

In the event the certificate is valid, the signing application will store the revocation status in the document. When opening a PDF document in Adobe Acrobat Reader, the validity of the signature is automatically verified. Adobe shows the result of the validation.

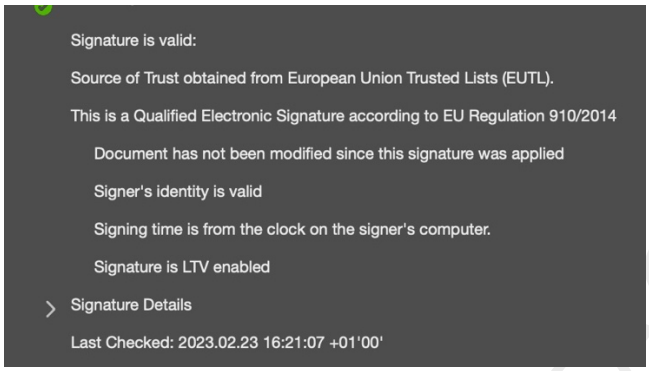
The certificate viewer in Adobe Acrobat Reader displays the message below.



The message informs the user that the certificate was issued from a valid certificate chain (certification path is valid) and that the certificate was not revoked (revocation checks were done) at the time of signing (date 2023/02/23 09:30:05 +01'00).

The signed document contains details on the validity of the certificate at signing which can be used to validate the signature even when the certificate has expired.

The signature panel in Adobe Reader displays the message that the signature is valid:

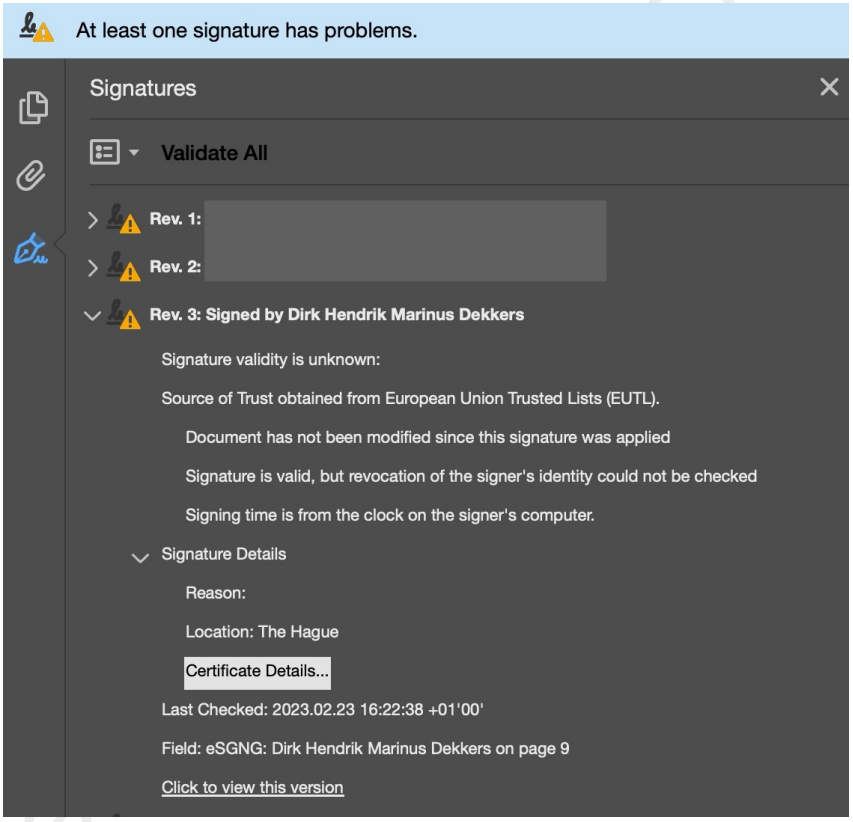


What happened when message "signature has problems" appears?

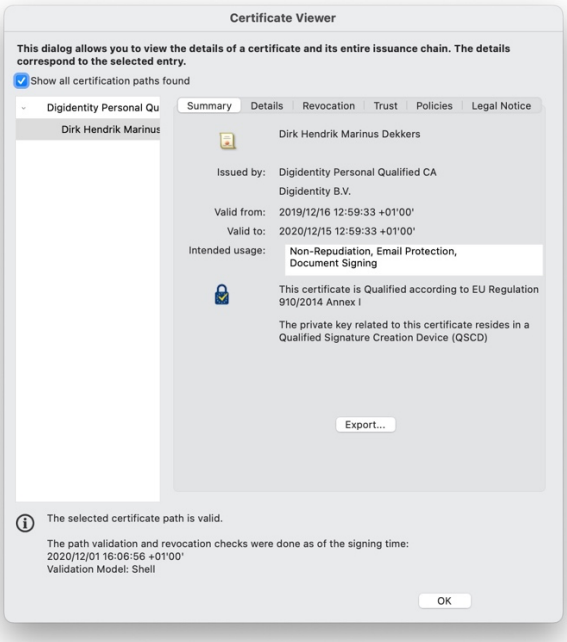
Adobe Acrobat Reader will verify the signature when opening the signed PDF document. The result of the verification is displayed.

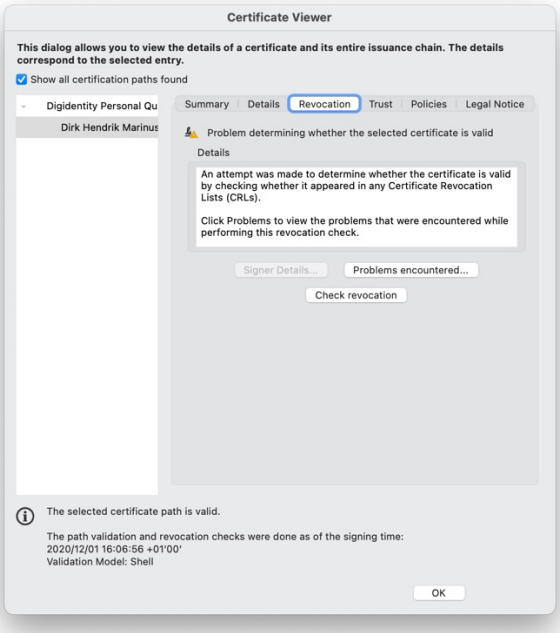
Adobe may show a signature with problems.

The details can be viewed in the signature panel.

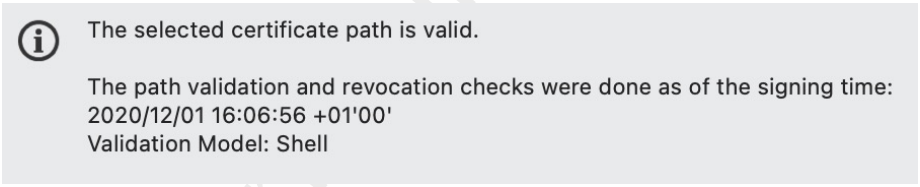


The signature details show that the validity of the signature is unknown. It is important to determine that the signature was valid on the moment of signing. The signature is valid, but the revocation could not be checked. To determine the problem encountered, you can view the Certificate Details.



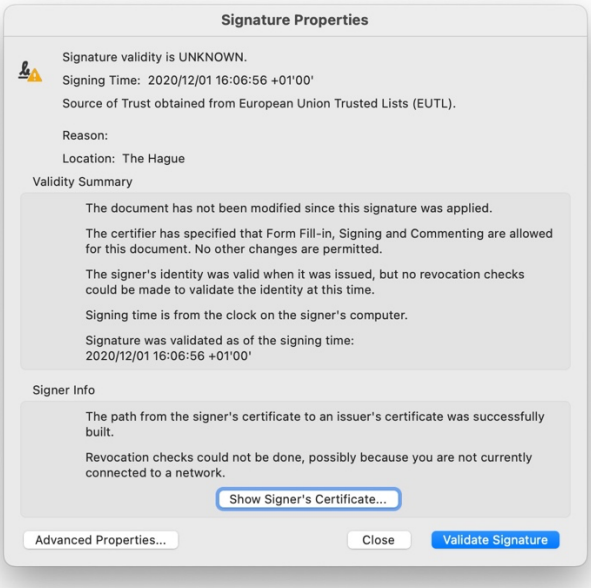


The revocation page displays the encountered problem. Adobe checks the validity of the certificate each time the document is opened. As the certificate expired on 15 December 2020, the certificate used for the signature is not valid anymore.



Adobe did validate the certificate path and revocation at the time of signature creation and concluded that the certificate was valid at the time of signature creation.

The signature properties screen shows:



Adobe shows that the validity is unknown (as the certificate is expired). The document has not been modified since the moment it was signed, signature identity was valid when the certificate was issued, and the signature was validated as of the time of signing (8 September 2020). When a certificate has expired, Adobe does not check revocation status.

So, the signature was valid at the moment of signing (1 December 2020), but the certificate has expired on 15 December 2020 which generated the problem. So, the signature is valid.

What happens when a certificate is revoked?

In the event a signing certificate is revoked, it cannot be used to sign documents. If the certificate is revoked, Digidentity will remove revoked certificates from the Digidentity Wallet so cannot be used to sign documents.

Revocation of the certificate does not result in revocation or invalidation of the signatures created before the revocation of the certificate. As long as the certificate was valid at the time of signing, the signature remains valid.

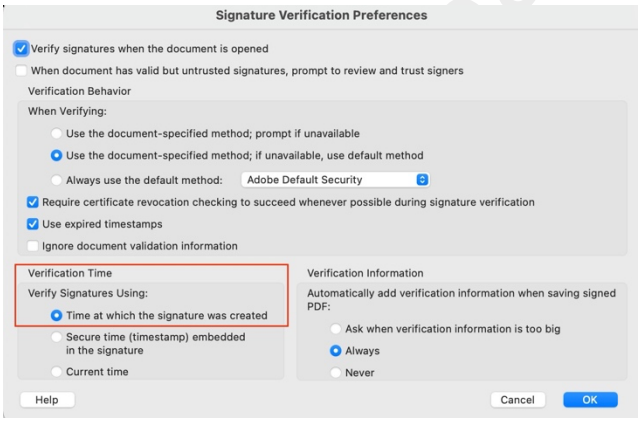
Example:
A document was signed with a qualified signature on 23 February 2023 at 9.30 hours. The signing certificate was revoked on 23 February 2023 at 10.02 hours (see image - time was 10:02 GMT+1).

```
Serial Number: 19851CD12402899BED320192CFB684EA
    Revocation Date: Feb 23 09:02:07 2023 GMT
```

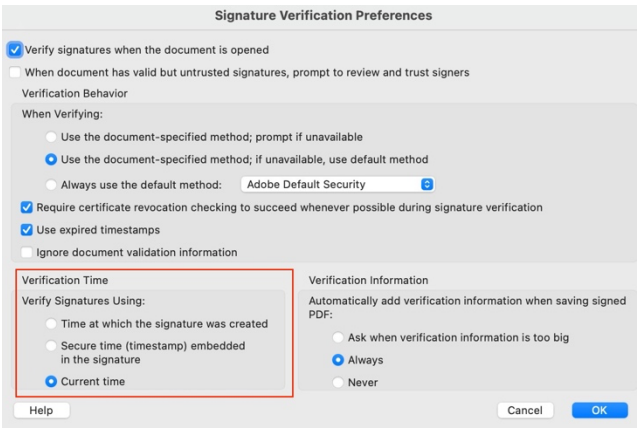
Adobe Acrobat Reader has two settings to verify the validity of the certificate:
[1] Time at which the signature was created
[2] Current time

The result of the verification is dependent on the setting.

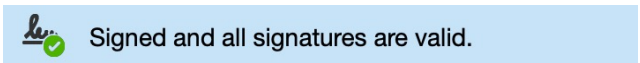
Verification time: Time the signature was created

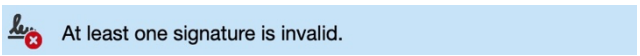


Verification time: Current time

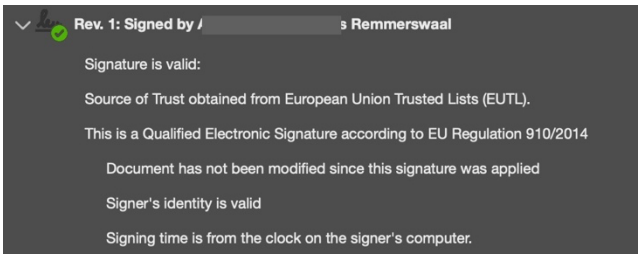


Verification information when opening document





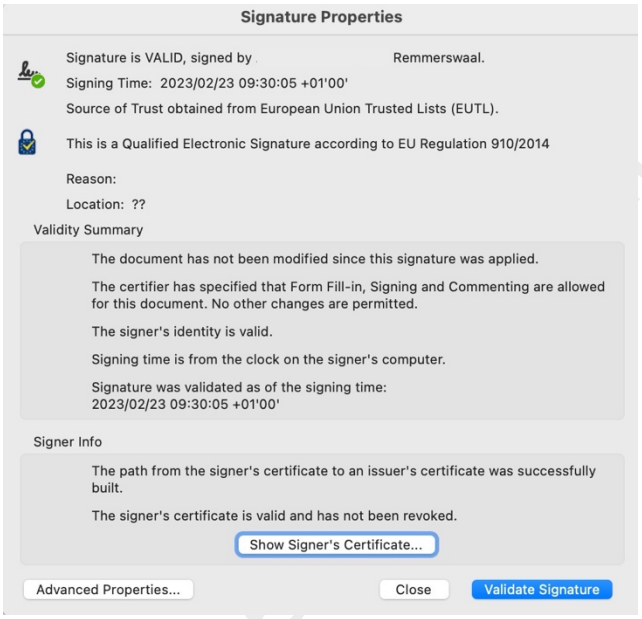
Signature Panel information



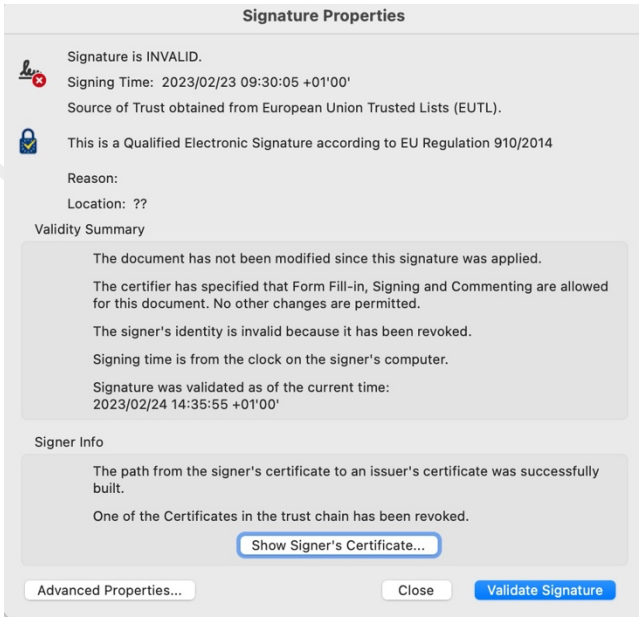
The certificate is revoked and the message is that the signature is valid. This is correct. The certificate is invalid but the signature was created when certificate was valid.

The certificate is revoked and the message is that the signature is invalid. This is not correct. The certificate is invalid but the signature was created when certificate was valid.

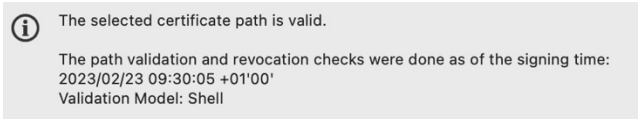
Signature Properties



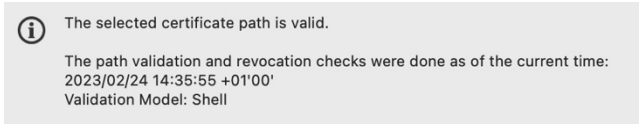
The certificate is revoked (10.02 hours) and the message is that the signature is valid. The signature was created when certificate was valid (9.30 hours).



The certificate is revoked (10.02 hours) and the message is that the signature is invalid. The signature was created when certificate was valid (9.30 hours). Signature is valid.



Validation check at time signature was created



Validation check at current time when certificate was revoked. Signing time determines the validity of the signature not the time of the validation checks.

Digidentity

Depending on the setting in Adobe Acrobat Reader, the signature is deemed valid or invalid. When the current time is used to validate the signature, the certificate status is revoked but as the certificate was valid at the time the signature was created, the signature is valid.

It is important to validate the signature at the time of signature creation. As long as the certificate to sign the document was valid at signing time, the signature is valid. Even if the signing certificate expires or is revoked after signing.

If signatures become invalid after certificate expiration or revocation (which all certificates will do), all signed documents will be useless as all signatures will become invalid, and nobody will use digital signatures.

Digidentity

Is an electronic signature valid when a certificate is no longer valid?

There is a difference between the validity of the signature and the validity of the certificate to create the signature. An electronic signature cannot expire or automatically become invalid, so the signature is valid even if the certificate used to create the signature has expired or was revoked.

Claiming a signature is invalid will always be a manual process and not technical. An electronic signature will not become invalid when the certificate used to create the signature expires or is revoked. If you compare it to a handwritten signature, you cannot claim the written signature is invalid because the pen used to write the signature is out of ink or was thrown away.

In the event that the signer claims the signature has been forged, handwriting experts will be required if the matter is referred to court. For an electronic signature the same applies. The signer will have to initiate legal proceedings in order to claim the signature has been forged.

In case of a legal dispute, experts will be required to provide evidence that the signature was an Advanced Electronic Signature. A Qualified Electronic Signature contains technical evidence which proves the signature is Qualified.

Digidentity

How do you know if a signature is qualified?

A qualified electronic signature on a document has technical proof built into the signing certificate. An electronic certificate for a qualified signature or Seal, contains QC statements.

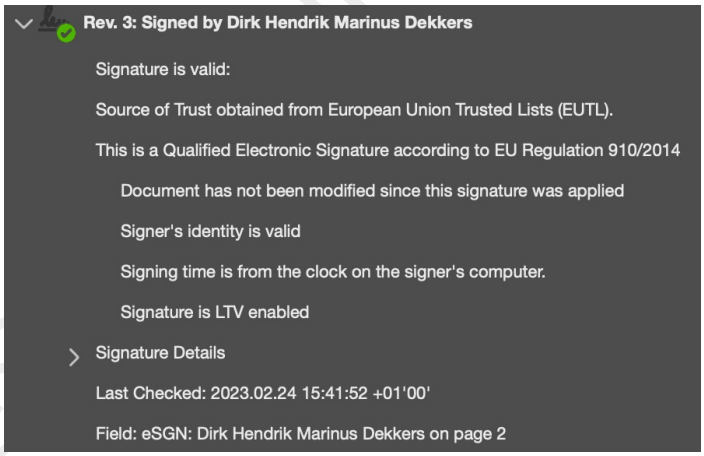
Firstly, the issuer of the certificate must include the QC statements in the certificate profile. This is documented in the Certificate Practice Statement (CPS) of the issuer (https://cps.digidentity.com).

Secondly, the signature can be verified using Adobe Reader and you can view the content of the certificate. Adobe uses the European Trust List for the verification of qualified certificates and uses the Adobe Approved Trust List (AATL) for the verification of advanced certificates.

To view the signing certificate in Adobe Acrobat Reader:

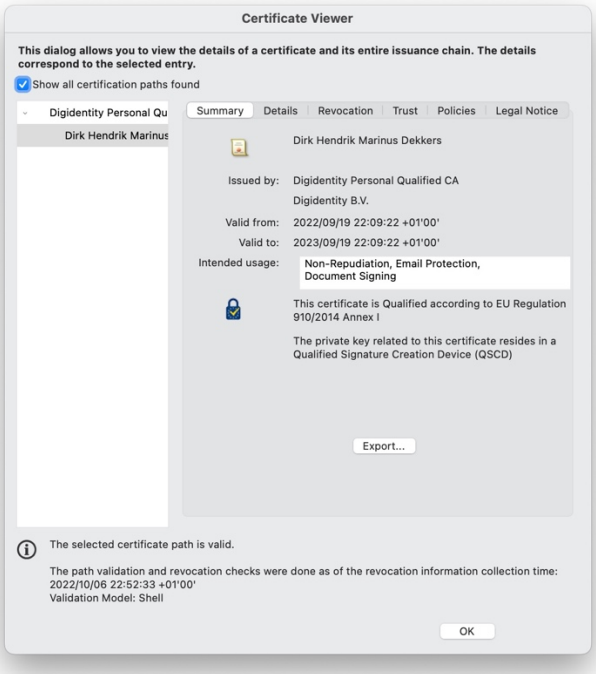
- Open the signed document in Adobe (Adobe will show the status of the electronic signatures)

- Click on the "Signature Panel" button to view the signature details

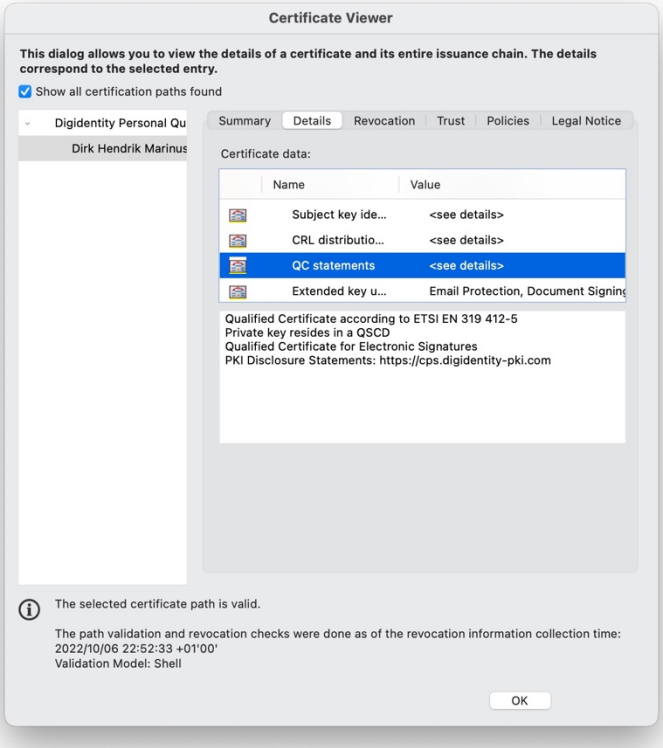


The signature details show the validity of the signature, if the European Trust List (EUTL) is used for validation, the content of the document has not changed, and if an EU qualified signature was used.

- To view the certificate details, you click on "Certificate Details"



The certificate details show the use of an EU Qualified certificate according to EU Regulation 910/2014 (eIDAS) and that a Qualified Signature Creation Device (Digidentity uses an HSM) was used to store the private key. The Details page shows the QC statements in the certificate.



The signing certificate is a qualified certificate.

Digidentity

What is Long Term Validation (LTV)?

A digitally-signed document may be used or archived for many years – even decades. As a signing certificate is valid for a fixed period of time (one year), when the document is opened, the signature will be validated but expiry will be reported. The signature was valid at the moment of signing but without Long Term Validation (LTV), this will not be visible.

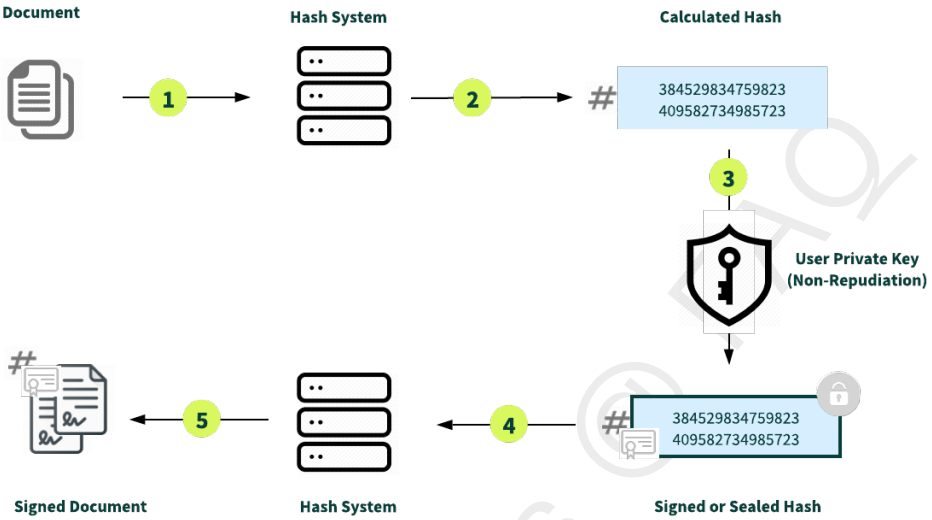
With LTV, a signed document can be validated to confirm that the signature was valid at the time it was signed even if the signing certificate has expired. With LTV enabled, the certificates sign-time status is captured and stored inside the PDF document. This is indicated within the signature details if it is LTV enabled or not. This verification certificate remains in the file itself so that its validity can be determined at a later date, regardless of whether the certificate has expired, been revoked, or the issuing authority no longer exists. Because the record is stored inside the signed document, it is also authenticated by the document's signature, further reducing chances for error or fraud.

LTV helps reduce dependencies on external systems and reduces the potential for future ambiguity around expired or revoked certificates. LTV will be available in 2023.

Digidentity

What is Hash Signing?

Digidentity's eSigning solution is based on hash signing. With hash signing, a unique number (hash) is calculated for the document. The hash is sent to Digidentity for signing with the electronic signature. The hash of the document is signed and embedded in the original document.



A signing process is started in a signing application (e.g., Adobe Sign) or document management system (1). The application calculates a unique number (hash) using a hash algorithm (2) for the document. This algorithm uses specific attributes to always calculate a unique hash.

The unique hash is sent to Digidentity's signing server where the user's Private Key (stored on Digidentity's HSM) is used to sign and seal the hash (3). The user's Public Key is also added to the signed hash.

The hash application receives the signed hash and verifies the signed hash with the hash of the document before attaching the signed hash to the document (5). The document is now digitally signed.

With hash signing, you do not have to send documents containing confidential information to Digidentity. As well as the security advantages, hashes are small in size compared to documents, increasing the performance of the signing process.

How do I verify if a signed document has not been modified?

When you receive a digitally signed document, you can verify the validity of the signature(s). Once you open the document in a digital signature-capable application (e.g., Adobe Reader), the application will automatically use the embedded Public Key to verify the signed hash of the document.

The application will recalculate the hash of the document and compare the hash to the signed hash. If the hashes match, the document has not been modified since it was signed. The application will also validate that the Public Key belongs to the signer.

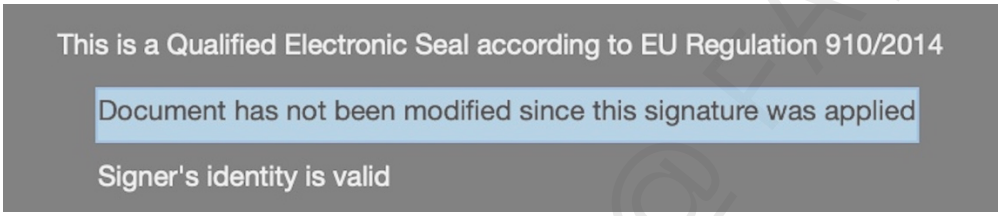
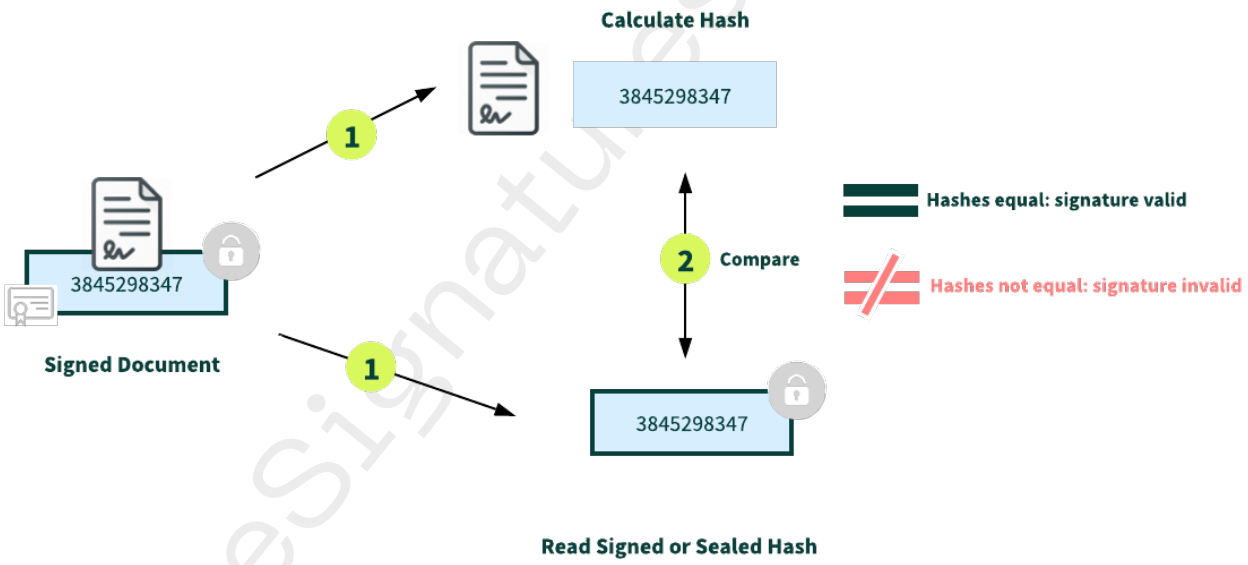


Figure 1 - Validation message in Adobe

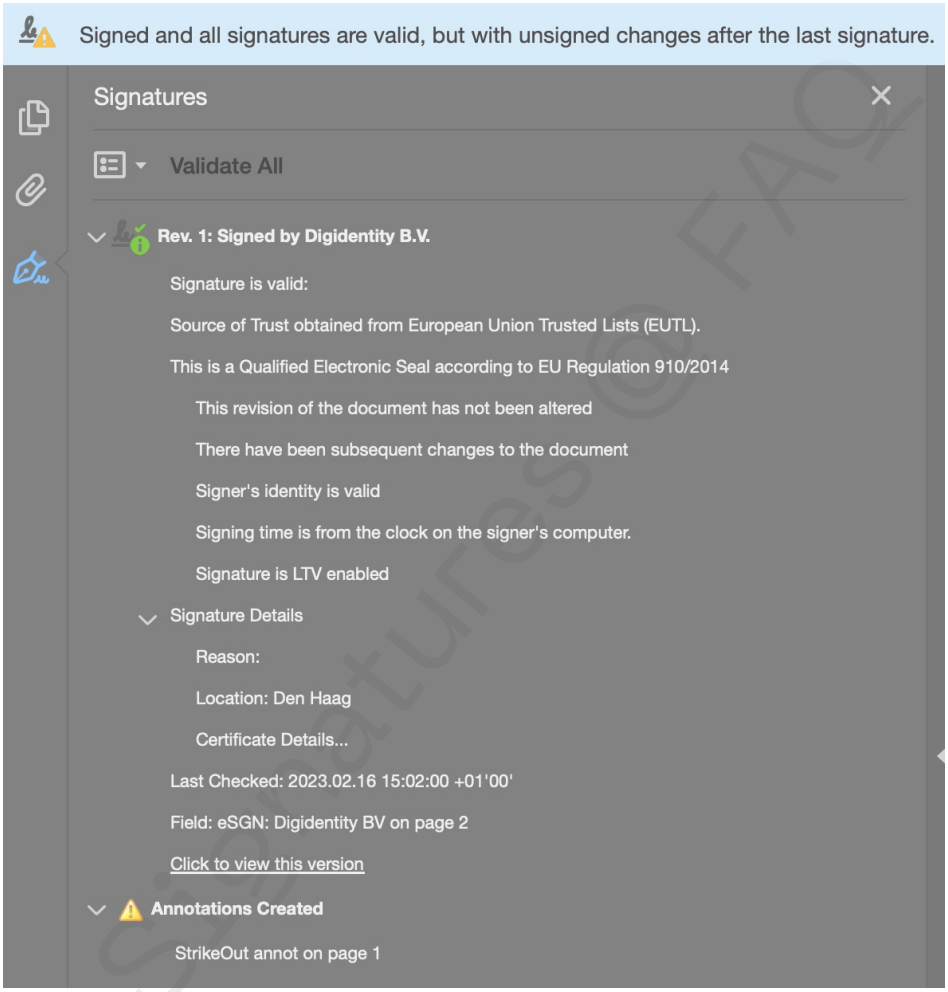


The signed document is received, the hash is recalculated (1) and the signed hash is read (2). Recalculated hash is compared to signed hash (3). When the hashes match, the document has not been modified and signature is valid. If the hashes do not match, the document has been modified and the signature is invalid.

What if the document has been modified after signing?

If the content of the document has changed after the document was signed, the hash will not match and the signature is invalidated for the modified document.

A message will show that the signature is valid, but that changes have been made in the document after the document was signed.



Any modification of the signed document, the changes made after signing are made visible.

Digidentity

What is a Signature Activation Module

Digidentity has developed a Signature Action Module (SAM) to sign documents. Digidentity is in the process of obtaining Common Criteria certification of the SAM against EN 419 241-2 (Protection Profile for QSCD Server Signing), combined with the Digidentity HSM as a Qualified Signature Creation Device (QSCD) for Qualified Remote Server Signing which will be included on the European Trust List (EU TL).

What is a Hardware Security Module (HSM)

Digidentity uses a Hardware Security Module (HSM) to store the private keys instead of a physical smart card. The user (Account Holder) can authorise the use of the private key on the HSM using a Virtual Smart Card within the Digidentity Wallet on their mobile phone by entering their memorised PIN code. The user does not have direct access to the Digidentity HSM.

Does Digidentity use a Qualified Signature Creation Device?

A Qualified Signature/Seal Creation Device (QSCD) is defined in Annex II of EU Regulation 910/2014 (eIDAS). A QSCD offers the highest guarantees of protection against replication or forgery of the private key.

The Digidentity HSM is certified against Common Criteria in conformance with the Protection Profile defined in prEN 419 221-5 and resistant against attack potential 'high'. The Digidentity HSM meets the requirements of Annex II in the eIDAS Regulation and is registered as a Qualified Signature Creation Device (QSCD) on the EU list for QSCD.

A QSCD does not have to be in physical possession of the signer and can be managed by the Qualified Trust Service Provider, called a "remote QSCD". Digidentity offers a remote QSCD with the Virtual Smart Card solution where the private key of the Subscriber remains on the QSCD of Digidentity. Our remote QSCD offers a simple user experience while maintaining the legal assurance provided by Qualified Electronic Signatures (QES) and Seals.

Digidentity

What is Revocation Status Service (CRL and OCSP)?

Certificates for electronic signatures can be revoked in case the private key is compromised, the information in the certificate is incorrect or several other reasons (see Section 4.9 in the Certificate Practice Statement on the Digidentity website https://www.digidentity.eu/en/documentation/)

When a certificate is revoked, the status of the certificate is changed in the database of the CA to 'revoked'. A CA that uses a Certificate Revocation List (CRL), adds the serial number of the certificate is added to the Certificate Revocation List.

Digidentity uses the Virtual Smart Card technology where the private key of the certificate is stored on the HSM. In the event a certificate is revoked, Digidentity sets the status to 'revoked' and deletes the certificate. The user can no longer use the revoked certificate to sign documents.

When the PDF Reader opens a signed document, the application will validate the certificate by contacting the CRL to determine if the certificate is revoked.

Another method to validate a certificate is to use an OCSP request. OCSP (Online Certificate Status Protocol) is a protocol that allows the PDF reader to check in real-time whether the signing certificate is still valid and trustworthy and has not been revoked. The application sends an OSCP request to the OCSP Responder. The OCSP Responder checks the validity directly in the CA system and responds with the status of the certificate.

Digidentity

Relevant content

Content	Link
Cloud Signature Consortium	https://cloudsignatureconsortium.org/
European Commission eIDAS	https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation
EU Regulation 910/2014 (eIDAS)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG
eIDAS 2.0 (proposal)	https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0281&qid=1677414441644
EU Trust List	https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home