Digital signing of original reports

Version 1.0, published 2010-04-20

Contents

1. Summary

ALS is continuing the process of digitization of information flow through the laboratory and will introduce electronic processing of reports from April 2010 to reduce paper usage as part of an ongoing green initiative and provide quicker delivery of final reports to our clients.

ALS Scandinavia final reports will be delivered in electronic format (PDF) after review, approval and certification by qualified personnel.

The final reports will be signed with advanced electronic signature created using a Digital ID securely stored on a SafeNet FIPS 140-1 level 2 cryptographic device issued by GlobalSign Certificate Authority.

PDF digital signatures are non-proprietary, standardized, and recognized as an Advanced Electronic Signature format. PDF digital signatures will be applied directly to the document itself and will be displayed on the document just like wet ink signatures. Moreover, PDF digital signatures are technically integrated into the document itself, meaning you only need one software application (Adobe Reader) to both view the document and validate the electronic signature.

Advanced electronic signature means an electronic signature which meets the following Regulatory Requirements:

- CFR 21 Part 11, Electronic Records; Electronic Signatures
- United Nations Model Electronic Signature Law
- European Union Electronic Signature Directive 1999/93/EC
- Qualified Electronic Signatures Act (SFS 2000:832) (in Swedish)
- US Global and national e-Commerce Act

Digital signatures are the equivalent to traditional handwritten signatures in many aspects; properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a document.

ALS Scandinavia has added a time-stamping functionality to the signing process that manages a long-term validation of digital reports. ALS reports will be signed according to a standard for long-term digital signatures defined by RFC5126.

2. Definitions

CA	**C**ertificate **A**uthority is a logical entity responsible for issuing certificates.
CDS	**C**ertified **D**ocument **S**ervices
CDS Certificate	A signing certificate issued by CA for the purposes of digitally signing of Adobe Acrobat documents.
Certificate	A record that, at a minimum: (a) identifies the CA issuing it; (b) names or otherwise identifies its Subscriber; (c) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; (d) identifies its Operational Period; and (e) contains a Certificate serial number and is digitally signed by the CA.
CRL	**C**ertificate **R**evocation **L**ist is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked or are no longer valid, and therefore should not be relied upon. CRLs may be seen as analogous to a credit card company's "bad customer list". There are two different states of revocation, defined in RFC 3280: Revoked or Hold.
OCSP	**O**nline **C**ertificate **S**tatus **P**rotocol is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders*.
PDF	**P**ortable **D**ocument **F**ormat (PDF) is a generic computer term. The best-known PDF implementation is Adobe PDF, a file format created by Adobe Systems in 1993 for document exchange.
PKI	**P**ublic **K**ey **I**nfrastructure is a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates.
Private Key	The key of a Key Pair used to create a digital signature. This key must be kept a secret.
Public Key	The key of a Key Pair used to verify a digital signature. The Public Key is made freely available to anyone who will receive digitally signed messages from the holder of the Key Pair. The Public Key is usually provided via a CA Certificate. A Public Key is used to verify the digital signature of a message purportedly sent by the holder of the corresponding Private Key.
Root Certificate	A root certificate is the digital certificate of a Certification Authority – for the CDS program this is the Adobe Root Certificate Authority.
TSA	**T**ime**S**tamping **A**uthority is a trusted third party (TTP) issuing cryptographic trusted timestamps.
Timestamp	Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one—not even the owner of the document—should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.
UTC	**C**oordinated **U**niversal **T**ime is a time standard based on International Atomic Time with leap seconds added at irregular intervals to compensate for the Earth's slowing rotation.

3. Aspects concerning digital signature

3.1. Authentication

A basic security issue of digital signing is authentication. Authentication is the process of confirming the signer's identity (name, company, location, contact info, signing reason). Signing with CDS digital signature securely identifies the author of a document.

Authentication
- secured: *A valid ALS Scandinavia identity will be showed in the blue ribbon at the top of the report if the authentication is secured (picture 7, chapter 5).*
- not secured: *Warning "The validity of the document certification is UNKNOWN. The author could not be verified." will be showed in the blue ribbon at the top of the report (picture 2, section 4.4).*

3.2. Verification of document integrity

If a document is digitally signed, any change in the document after signature will invalidate the signature. Furthermore, it is not possible to modify a document and its signature to produce a new document without the signature becoming invalid.

Integrity
- secured: *A valid ALS identity will be showed in the blue ribbon at the top of the report if the integrity is secured (picture 7, chapter 5).*
- not secured: *Warning about modification of the document after certifying will be showed in the blue ribbon at the top of the report.*

3.3. Timestamping of the document approval

A time-stamping function supports assertions of proof that a document existed at a particular time. A time-stamping function is used to prove the existence of certain data before a certain point (e.g. contracts, research data, medical records,...) without the possibility that the owner can backdate the timestamps.

Anyone trusting the timestamper (issued from a TSA) can then verify that the document was not created after the date that the timestamper vouches. It can also no longer be repudiated that the requester of the timestamp was in possession of the original data at the time given by the timestamp.

Timestamping standard is described in detail in RFC 3161.

Date/time timestamp
- secured: *"Date/Time" tab on signature properties (picture 10, chapter 5) inform that signature is timestamped by Timestamp Authority(SEIKO Timestamp Service). Date is formatted to coordinated universal time (UTC - Universal Time, Coordinated).*
Please Note: *In the right bottom corner of the report you can find date and time when the report was approved and signed. Date is formatted to local time (picture 8, chapter 5)*
- not secured: *"Date/Time" tab on signature properties (picture 10, chapter 5) inform that signature Date/Time are from the clock on the signer's computer.*

3.4. Non-repudiation

Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a document. *The signer of the ALS report is always showed in the blue ribbon at the top of the report and no one other than this person can have signed this ALS report. (picture 7, chapter 5)*

3.5. Validation of digital signature

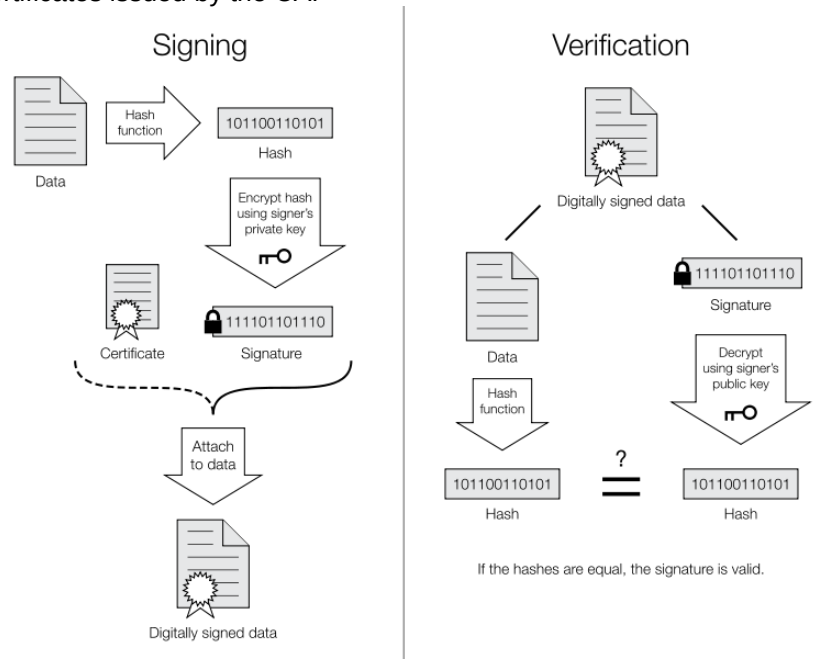
It's easy for end-user to verify the signer's identity (authentication) and the integrity of the document. Validation service is embedded in Adobe Reader v. 6 and above.

Digital signature validation: Click on digital signature for the signatures properties and the complete information about signatory and the document. *(picture 10, chapter 5)*

4. Introduction to digital signing

4.1. Public Key Infrastructure

In cryptography, a PKI is an arrangement that binds public keys with respective user identities by means of a certificate authority (CA). The user identity must be unique for each CA. The binding is established through the registration and issuance process, which, depending on the level of assurance the binding has, may be carried out by software at a CA, or under human supervision. The PKI role that assures this binding is called the Registration Authority (RA). For each user, the user identity, the public key, their binding, validity conditions and other attributes are made traceable in public key certificates issued by the CA.



Picture 1

4.2. Digital Identities

Digital Identities are X.509 compliant digital certificates which allow a participant (person / company / device) taking part in an electronic transaction to prove their identity towards other participants in the transaction. They are the digital equivalent of an ID card and in the case of documentation workflow systems can be used to digitally attest (sign) to the contents of a document.

GlobalSign DocumentSign™ Digital ID for Adobe® PDF certificates are created and delivered in accordance with the Adobe Systems Incorporated CDS (Certified Document Services) certificate and are fully compatible with the Adobe PDF platform allowing certification and approval signatures to be applied using the Adobe range of document creation products.

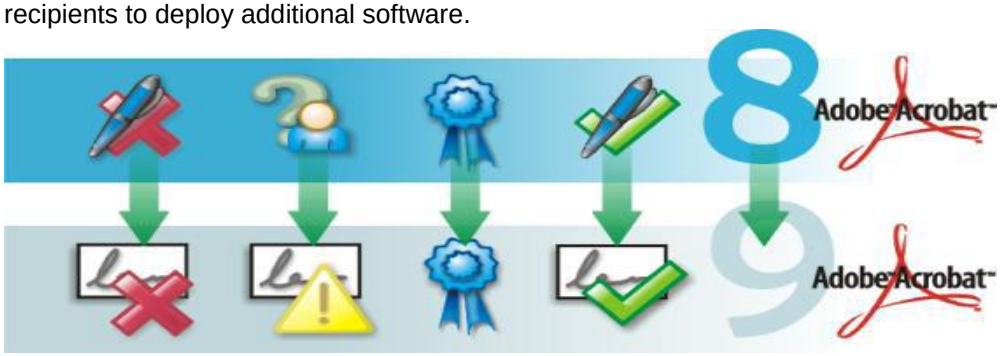
4.3. Advanced electronic signature

Electronic signature is data in electronic form attached to or logically associated with other electronic data, and used to verify that the content originates from the alleged issuer, and has not been altered.

Advanced electronic signature is an electronic signature that
a) is uniquely linked to a signatory,
b) is capable of identifying the signatory,
c) is created using means that are under the signatory's sole control, and
d) is linked to other electronic data in such a way that any alteration to the said data can be detected.

4.4. Certified Document Services (CDS) Program

Certified Document Services (CDS) is one of the services enabled by the Adobe root certificate authority. CDS enables document authors to sign Portable Document Format (PDF) files, using a digital ID, which automatically validate when authors are using free Adobe Reader® software. No additional client software or configuration is required. CDS was designed to enable organizations and individuals who publish high-value documents to large and disparate recipient groups to increase the assurance level that the document's integrity and authenticity are preserved. By adding a CDS signature to a PDF file, document authors can increase this assurance level without requiring recipients to deploy additional software.

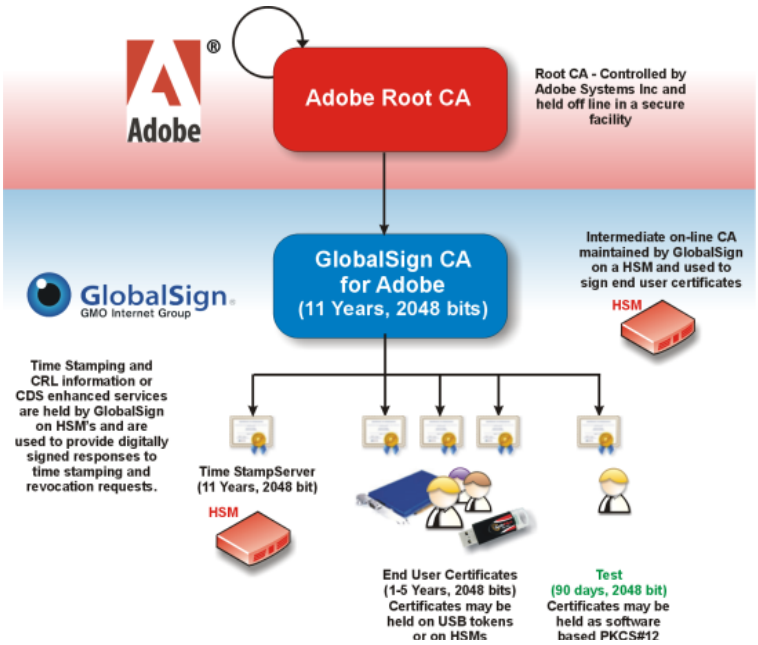


Changed after Signing | **Unknown Author** *(Revoked, Expired or non trusted Digital ID)* | **Certified** | **Signature is valid**

Picture 2

4.5. Root CA and Certificate Hierarchy

A root certificate is the digital certificate of a Certification Authority (CA) – for the CDS program this is the Adobe Root CA. Its public key is used to verify the signature of the Certification Authority, while the corresponding private key is used to sign all certificates issued. The root certificate confirms that the public key and the Certification Authority are linked. By trusting a root certificate, the user accepts the trust provided by the Certification Authority. The PDF reader from version 6.0 onwards trusts the Adobe Root CA the chain of trust from the end entity certificates back to the Adobe root certificate.



Picture 3

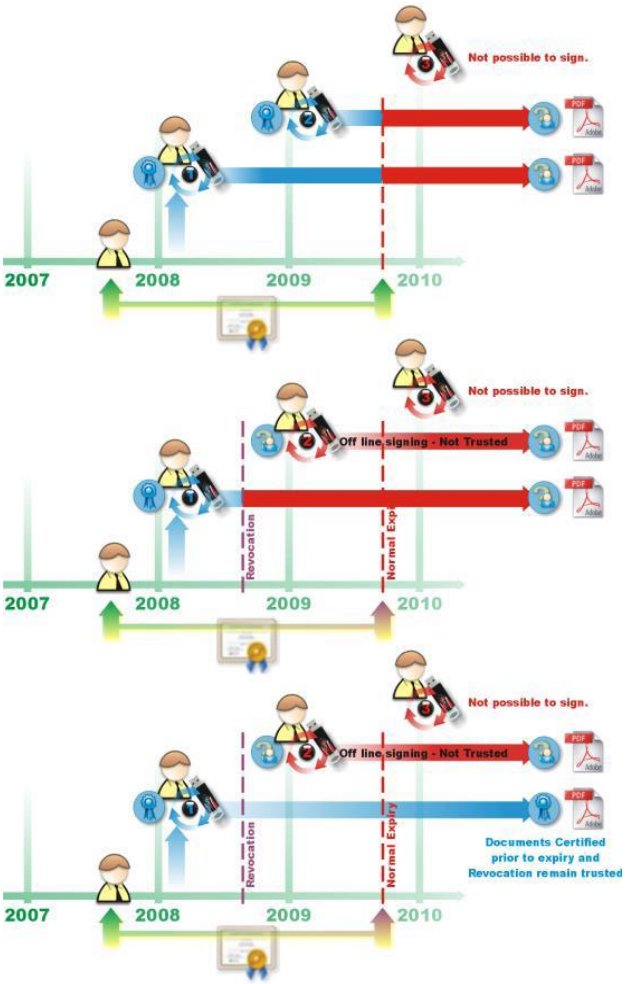
4.6. CDS Services (CRL)

During the signing and certification process, Adobe Acrobat will verify the status of the digital certificate used for signing with the GlobalSign CRL (Certificate Revocation List). If the certificate is still valid the CRL will be embedded within the signature properties of the PDF document. All future trust decisions on the authenticity of the document will indicate that the certificate was valid at the time of signing (Based on the details within the timestamp – See the next section), and therefore regardless of whether the digital certificate later expires, or is revoked, the authenticity of the document can still be verified – Meeting long term archival needs.

Recipients simply need to open the document using the free Adobe Reader to instantly understand if the authenticity of the document can be trusted. Adobe‘s simple to interpret —Blue Ribbon, Question Mark, and Red X trust messaging allows even novice users an easy to understand method to determine if the document is from a legitimate source.

Note the embedded CRL recorded in the PDF signature properties in the example. Signature validation will be performed using the embedded information, therefore producing a valid signature even if the digital ID expires, or becomes revoked, or if the document was opened off-line.

No special plug-in or separate validation engine is required; therefore security always travels with the document



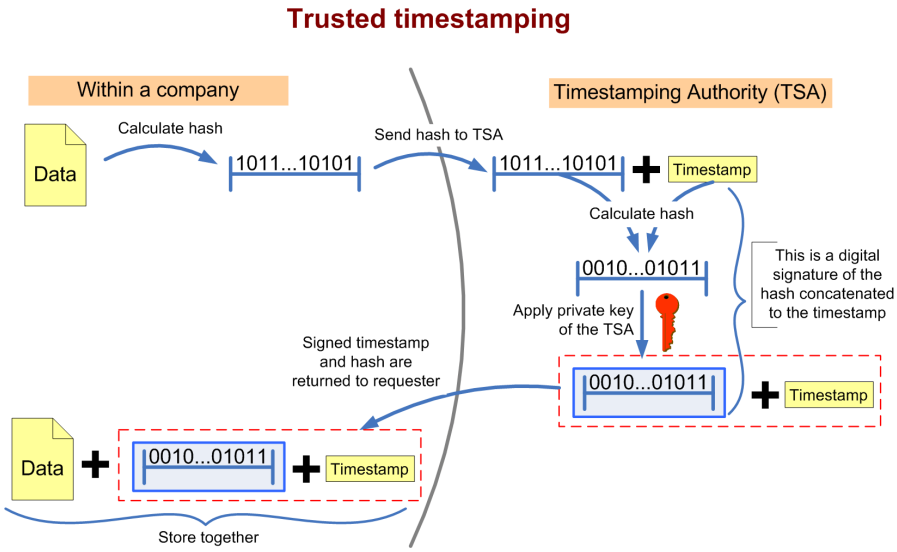
Picture 4

4.7. Digital timestamping

Trusted timestamping is the process of securely keeping track of the creation and modification time of a document. Security here means that no one—not even the owner of the document—should be able to change it once it has been recorded provided that the timestamper's integrity is never compromised.

The administrative aspect involves setting up a publicly available, trusted timestamp management infrastructure to collect, process and renew timestamps.

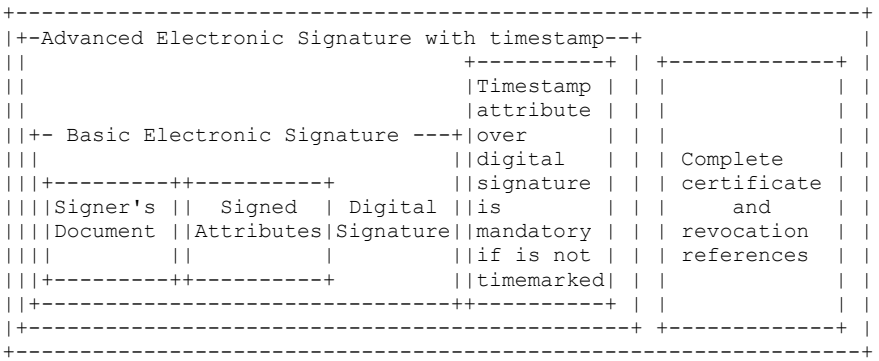
The technique is based on digital signatures and crypto digest functions. First a hash is calculated from the data. A hash is a sort of digital fingerprint of the original data: a string of bits that is different for each set of data. If the original data is changed this will result in a completely different hash. This hash is sent to the TSA. The TSA concatenates a timestamp to the hash and calculates the hash of this concatenation. This hash is in turn digitally signed with the private key of the TSA. This signed hash + the timestamp is sent back to the requester of the timestamp who stores these with the original data (see diagram).
Since the original data can not be calculated from the hash (because the hash function is a one way function), the TSA never gets to see the original data, which allows the use of this method for confidential data.



Picture 5

4.8. Signing with long-term signature

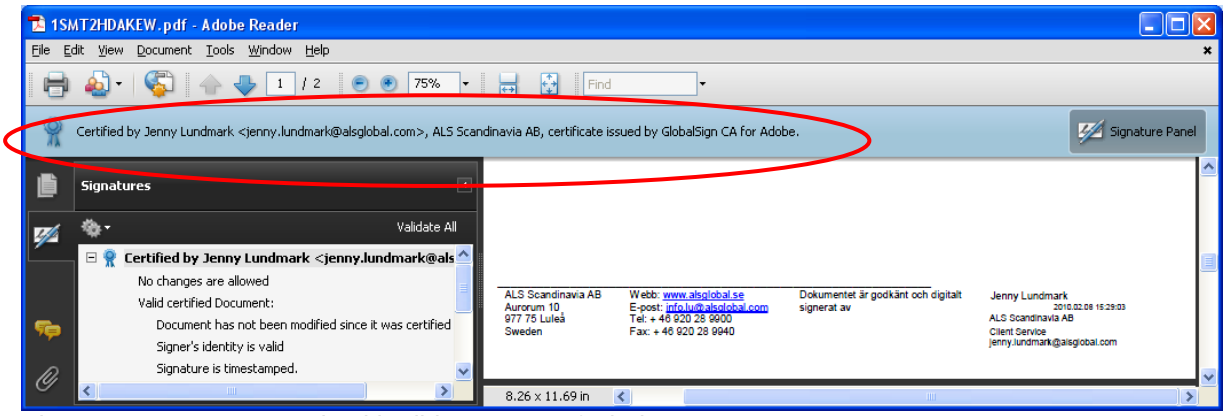
A standard for long-term digital signatures is defined by RFC5126 (and its previous edition, RFC3126). This document defines the format of an electronic signature that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e., repudiates) the validity of the signature.
Electronic Signature with Complete validation data references, in accordance with RFC3126, adds to the Electronic signatures with the time-stamp attribute the complete-certificate-references and complete-revocation-references attributes. The complete-certificate-references attribute contains references to all the certificates present in the certification path used for verifying the signature. The complete-revocation-references attribute contains references to the CRLs and/or OCSPs responses used for verifying the signature. Storing the references allows the values of the certification path and the CRLs or OCSPs responses to be stored elsewhere, reducing the size of a stored electronic signature format.



Picture 6

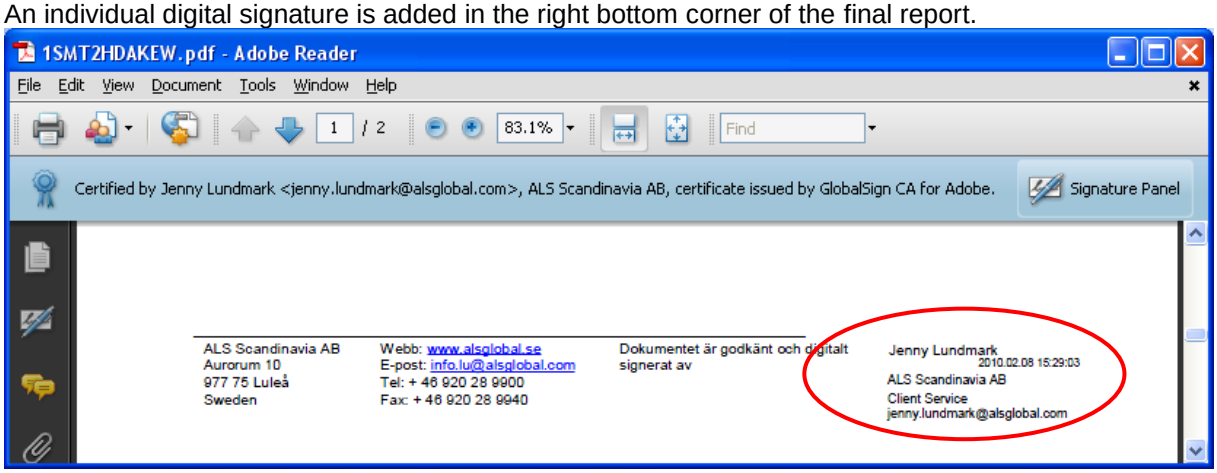
5 Appearance of CDS digital signature in Adobe Reader

A blue ribbon and a blue rosette appear on the top of the document after validation of digital signature if signature is valid. They can be considered as a signs of trust: the information has not been altered since it was signed and verification of the signer's digital identity has been successful.



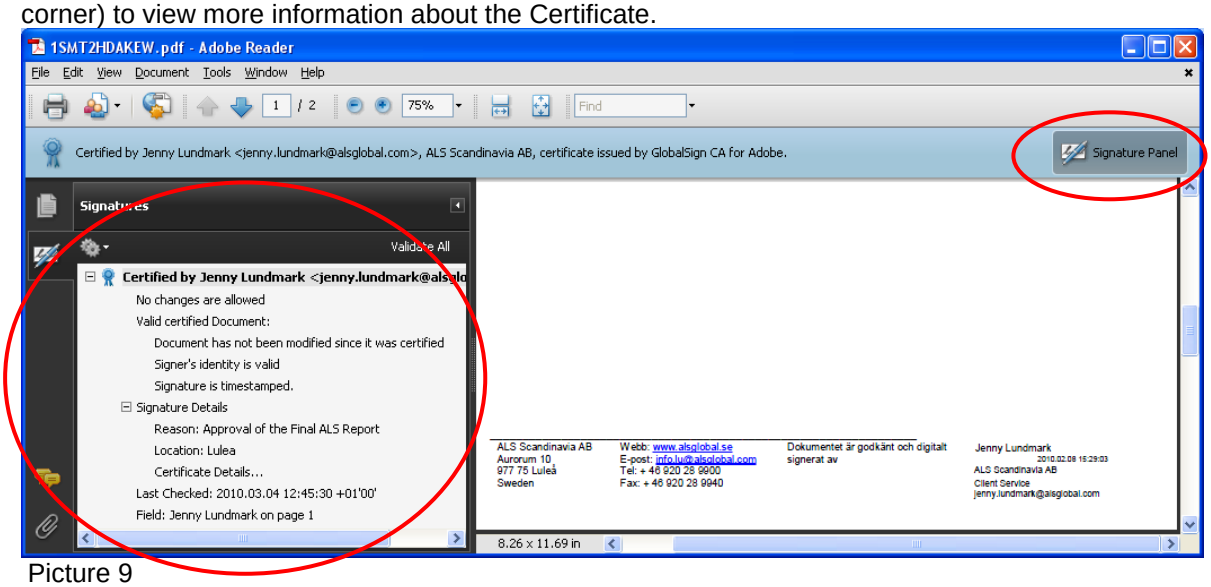
Picture 7. Status summarized in ribbon at top of window

An individual digital signature is added in the right bottom corner of the final report.



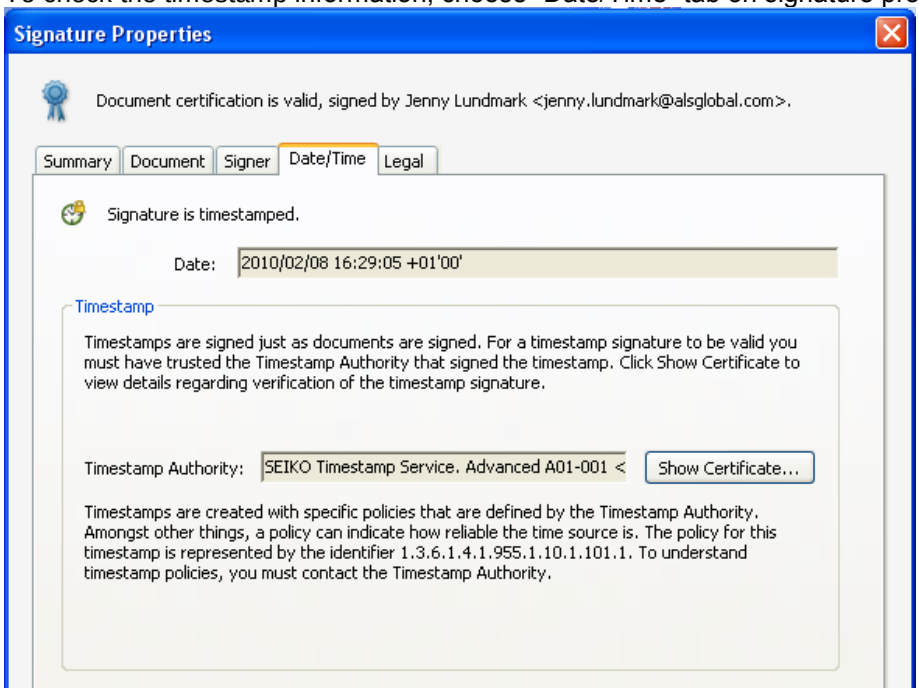
Picture 8

The signature panel can be opened to display all details. Click on the signature panel (upper right corner) to view more information about the Certificate.



Picture 9

To check the timestamp information, choose “Date/Time” tab on signature properties.



Picture 10

6 GlobalSign CA

This GlobalSign CA for Adobe CPS endorses in whole or in part the following industry standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework (obsoletes RFC 2527)
- RFC 2459: Internet X.509 Public Key Infrastructure - Certificate and CRL Profile.
- RFC 2560: X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP
- RFC 3279: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and CRI Profile
- RFC 3161: Internet X.509 Public Key Infrastructure – Compliant Time Stamping Authority
- The ISO 1-7799 standard on security and infrastructure
- Adobe Systems Incorporated CDS Certificate Policy Revision #15 dated February 2007

Please find more information about GlobalSign on
- www.globalsign.com
- http://www.globalsign.com/document-security-compliance/adobe-cds/faq.html
- Certification Practice Statement
  http://www.globalsign.com/repository/globalsign_adobe_cds_cps_v1.2.pdf

7 Links

- RFC 5126 CMS Advanced Electronic Signatures
  http://tools.ietf.org/html/rfc5126

- RFC 3161 Internet X.509 Public Key Infrastructure. Time-Stamp Protocol
  http://www.ietf.org/rfc/rfc3161.txt

- RFC 3039 Internet X.509 Public Key Infrastructure. Qualified Certificates Profile
  http://www.ietf.org/rfc/rfc3039.txt

- Eliminating the Pen...One Step at a Time: PAdES PDF Advanced Electronic Signature Standard Released for EU By John B Harris on September 23, 2009 12:29 PM
  http://blogs.adobe.com/security/2009/09/eliminating_the_penone_step_at.html

- European Union Electronic Signature Directive 1999/93/EC
  http://eur-lex.europa.eu/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

- Qualified Electronic Signatures Act (SFS 2000:832) (in Swedish)
  http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2000:832

- Wikipedia
  http://en.wikipedia.org/wiki/Public_key_infrastructure
  http://en.wikipedia.org/wiki/Trusted_timestamping
  http://en.wikipedia.org/wiki/Digital_signature

- Adobe
  www.adobe.com
  http://www.adobe.com/security/pdfs/digital_signatures_guide.pdf

- GlobalSign
  www.globalsign.com
  http://www.globalsign.com/document-security-compliance/adobe-cds/faq.html
  http://www.globalsign.com/repository/globalsign_adobe_cds_cps_v1.2.pdf