**Signing of Digital Calibration Certificates**

1. **General information on digital signatures**
   1. Background

Issuing, transferring, using and archiving calibration certificates in electronic form brings forward the need of knowing the origin and authenticity of certificate and assurance that data in certificate is complete and unchanged. The set of information that forms a DCC can be signed electronically as we would sign paper documents by hand.

Electronic signature is the broad category of (mathematical) methods for signing a document in electronic form, sometimes called “digital signature” where specific signature technology is implemented.

* 1. Need for digital signing

Choosing means of electronic signing comes down to requirements of parties involved in creation and receiving the calibration certificate. Requirements can deviate depending the use-case, industry branch, legal requirements in country etc

Majority of calibration service providers in Europe are EN-ISO 17025 accredited or follow the requirements of this standard to some extent. Above mentioned standard does not directly require signing of issued certificates but there are general requirements for the integrity of the data and information which can be fulfilled by electronically signing documents. There might be national requirements specifically ordering certificates to be signed.

* 1. Different types and levels of digital signatures

Depending on the situation and legal requirements for the protection of certificates from manipulation (integrity) and proving the identity of the issuer (authenticity) on of the following electronic or digital signature types may be applied:

|  |  |  |
| --- | --- | --- |
| Type | Description | Example |
| 0 (not signed) | ISO/IEC 17025 is not requiring any signature on certificates. If no national regulation would require a sufficient electronic signature, issuer and customer of the certificate may agree to exchange data without any means for protection by signature but bilateral trust. | pure file (e.g., paper like document as .docx (only for humans)) |
| **1 (not signed but protected** | The issuer of the certificate is providing a different method for protection of integrity and authenticity of the certificate to the customer then an electronic signature. For example, the issuer operates a legally secure e-file system with longer-term storage of original certificates or persistent storage of unique fingerprints of certificates. |  |
| **Type 2 (simple signature)** | The electronic document contains an electronic image of a handwritten signature of text on signer in combination with a simple protection from manipulation of the certificate content. | a pdf file with image of signature and write protection from pdf creating software |
| **Type 3 (advanced electronic signature)** | The certificate is protected by deployment of a cryptographic methods based on a Private-Public-Key methods. The customer can verify the signature. The security level is normal. The signature meets the technological requirements established in standards. This type can be further distinguished by that if backgrounds of both the owner of the signature and the issuer of the certificate can be checked. | For example signed pdf but signing service provider is not in EU trusted list (“self declared”) |
| **Type 4 (qualified signature – eIDAS conform):** | Signature with an eIDAS regulation conforming method. Within Europe, such signed documents, their integrity and authenticity are legally watertight. The signature meets the technological requirements established in standards. The backgrounds of both the owner of the signature and the issuer of the certificate are checked. Additionally, the signature is given with a means that is deemed suitable (ID-cards, digital IDs, mobile-IDs). | signed document and signing service provider in EU trusted list (“self declared”)  e.g Estonian governmentally backed signing system with .asice file containers |
| **Type 5 (non-European signature method)** | A signature method with legal acceptance in a non-EU country is uses, e.g., a method valid in the US or in the Asian pacific region. This could be relevant for services offered beyond Europe. |  |

Clearly there will be types beyond Type 5 with as yet undefined additional functionality. This could include software that supports the individual User Groups (or Actors) from the calibration community from NMI to industrial manufacturer. For example members of the national, European and/or international quality infrastructure agree on and manage their own tools and infrastructure for trusted and legally secure signatures particularly for certificates in the quality infrastructure.

There are various commercial providers of signing services available worldwide as well as governmentally backed up services in some countries (EU Trust Providers list is a good source to find eIDAS compliant providers).

Signature can be linked to a physical person or to an organization (legal person), in which case it can be called an electronic seal.

Majority of commercially available services rely on asymmetric encryption and more specifically PKI (<https://en.wikipedia.org/wiki/Public_key_infrastructure>) principle. More information can be found from EMPIR project SmartCom outcome documents (<https://www.ptb.de/empir2018/smartcom/information-communication/publications/> ).

* 1. Considerations when moving to electronical signing

When choosing method for electronic signing we may ask questions:

* is the signature uniquely and securely linked to the signee?
* is the signature linked to the data signed there with in such a way that any subsequent change in the data is detectable?
* is there an audit trail with time stamp available?
* In case of EU users is it in compliance with GDPR and is data processing made (servers located) inside EU/ETA area

Reasons for signing DCC?

* Need from regulation - need something equivalent to hand-written signature
* Signature symbol for quality & trust (part of marketing)
* Postal trust by paper enveloped - DCC is from sender and the document that was meant to be send - digital security by signature too
* Postal secret - only dedicated receiver can see content - possible with signature too

1. **Overview of two examples of digital signing – direct signing of PDF files and “file container” based signing**
   1. PDF signing example

**Principle**

A PDF A\3 (or PDF A\4 f) document is used as a file container including the human-readable part of the certificate (read document with a PDF viewer) and having attached files (attachment within PDF) providing machine-readable data from calibration. The deployment of a signature restricts the ability of further manipulation or change of the information within the PDF (human readable part).

For protecting the attached machine-readable documents from manipulation (making manipulation visible), the concept from METAS for example is introducing unique fingerprints (hash values / check sums) for each attached document. At the assembly of the document, the creator is using a standardized method (hash algorithm) to calculate the fingerprint for each attachment. The values of each fingerprint are stored within the PDF part that is protected by the signature. The user can apply the same method to calculate the hash values of the attached files. If the has values obtained by the user differ from the reference values in the PDF, it is an indicator that data has been manipulated. The has values can also be attached in a machine-readable file.

**Security and legal requirements**

PDF A is supporting different signature methods supporting different legal requirements. These are

* Simple handwritten electronic image or text with name of the signer(s) at signature filed for basic protection of content. After application of the signature, the document is protected from manipulation with basic means applied by PDF creating software.
* Advanced electronic signature (based on PKI certificate with private and public key) for basic check of integrity and authenticity. After application of the signature, the document is protected from manipulation and users can verify the electronic signature.
* Qualified digital signature (based on PKI and for example eIDAS compatible methods) for legally watertight signature. After application of the signature, the document is protected from manipulation and users can verify the electronic signature based on a legally highly secure method.

**Advantages**

If an organization is already working with (electronically signed) PDF documents, the transition to the PDF A file container is easy and existing tools for working with PDF can in many cases be directly used to apply and verify electronic signatures. Thus, it is easy to use for customers, who still depend more on the human readable content.

Many PDF tools provide means to create image of hand-written electronic signatures and electronic signatures based on cryptographic certificates (PKI). Thus, additional costs for signing PDF A could be easier to manage.

**Disadvantages**

The digital (cryptographic) protection of the attached machine-readable files needs this workaround with hash values. To verify that the data has not been manipulated, additional software is needed to be used by creators and users of the calibration data. If atomisation of verification is required, the transcription of the reference hash values from the PDF to software is not trivial.

Deployment and validation of qualified digital signatures / seals require additional tools that are typically not part of standard PDF tools. E.g., DocuSign (used for example in VTT Finland) which is eIDAS conform or PDF-Tools.com.

**Infrastructure and interfaces needed for deployment**

For a manual deployment by humans standard PDF tools can in many cases by used to deploy and validate ‘Image of handwritten signatures’ and ‘advanced electronic signatures’. Specific signature software is needed for higher level qualified digital signatures (e.g., the eIDAS compliant ones).

To automate the signature (signature of batches in automated workflows) tools providing relevant APIs (Application Programming Interfaces) for deployment of signatures and seals in software must be supplied.

In addition, both creators and users of signed PDF data need software (human usable and/or API) to provide calculation and/or validation of the hash values of attached data.

**Potential cost points – for issuer and customer**

Issuers of signed PDF certificates have to take expenses for the tools (e.g., PDF viewer) that allow to create the signatures and/or licences for software for automated deployment of the signatures. Available products typically sell licences on the basis of a fixed fee per person per year. For simple signatures, some open-source tools can be found.

In case of advanced and qualified signatures, the issuer also has to take expenses for obtaining PKI certificates (signature cards) and additional hardware like signature card readers. Again, fees typically are raised per signature PKI certificate per year and buying or renting hardware. If natural persons of an organization are signers, then one certificate per person must be considered. Tools for advanced signatures are a little cheaper to obtain than qualified signatures.

On the customer side, expenses are limited to tools for validation of signatures. Many open access tools (free of charge) are available.

* 1. “file container” based signing

**Principle**

Associated signature container (ASiC) is a data container that is used to hold a group of files and digital signatures and/or time assertions that are associated to those objects. (<https://en.wikipedia.org/wiki/Associated_Signature_Containers>).

The container is in principle a zip-file which has a specific file extension (for example in Estonia ASICE). The structure of signature data is based on XML syntax XAdES ( <https://en.wikipedia.org/wiki/XAdES>).

In Estonia the software that is needed to create and open these containers is provided in coordination of Estonian government (<https://www.id.ee/en/> ) and together with fact that every citizen has mandatory ID-card with digital signing capabilities we get nationwide trusted system for digital signing.

**Creation of the signed document**

When signing a document the software creates files for metadata and signature files. All files with document to sign are zipped and an ASICE extension is set.

When creating a signature the application checks if signer’s certificate is created by institution/company that is listed in European Union TSP (Trusted Service Providers) list, also if the certificate is valid for the operation (it has correct validity time; it has the flag that states that the certificate is for creating signatures).

While creating the signature software also adds current timestamp to the container. The timestamp is signed using timestamp provider which also is in the TSP list.

**Verifying the signed document**

To verify the signature, the file should be opened in the software that was used to generate the signature.

To verify the signature, software uses the signatures and public certificates which are located in the container files.

**Advantages**

Multiple files can be applied

Multiple signatures can be applied.

Files that the signatures are applied to are not altered. Which leads to next point – in case there arises proof that the currently used cryptography is hackable/breakable then the signed files can be re-signed/re- packaged in new technologies without altering the original files.

If once set, then same infrastructure/services are already used for many different purposes – it isn’t DCC or metrology specific solution; no separate cryptographic solutions are needed.

**Disadvantages**

Knowledge of this type of signing is not widespread (Excluding some countries as Estonia for example), so there is need to explain to customers how to use the file containers.

Signing does not work without internet connection.

**Security and legal requirements**

Security of the signed documents is according to eIDAS QES-level regulation.

**Infrastructure and interfaces needed for deployment**

1. Trusted digital cryptographic device linked to a person (for example ID-card, crypto stick, mobile ID) and certificates inside the device are needed.
2. Signing of documents with personal signature can be done using publicly available software and personal ID. When using an electronic signature of organisation, it is necessary to create a software environment which enables the use in the organization (user identification, under what conditions the signing/stamping takes place, what is the status of the stamped documents etc.).

**Potential cost points**

Issuers of container-based signed certificates have to take expenses for the tools – physical PKI signature card or crypto stick (HSM – <https://en.wikipedia.org/wiki/Hardware_security_module>). Even when physical users already have personal tools (eg compulsory ID-Card in Estonia, and signing is free for private use) if these are used for professional use, a fee may apply. If company’s electronic stamp is used, physical crypto stick costs and typically there is also a fee for every signature/stamp given.

Card reader is needed for signature cards.

Automation of company signing/stamping can be done by means of investing in software environment, where validated users can assign company’s electronic stamp “one click” which initiates signing process in separately implemented service that runs the signing.

On the customer side (receiver of signed documents), expenses are limited to tools for opening and validation of signatures. In case of Estonia for example, the software is free and available in app stores by Microsoft, Google or Apple.

### **3. Implementation of DCC signing workflow**

While an application of a digital signature to a document such as the DCC is a rather unspectacular process, setting up the infrastructure for signing and maintaining the infrastructure requires several management and technical implementation work. Here is the DCC2GO blueprint for a potential workflow that organisations could use to implement digital signing of DCCs. It comprises three phases in the life-cycle of digital signing and is based on practical workflows and experience from the organisations of the authors.

Phase 1: Implementation of signature infrastructure (questions to answer before you can start)

* 1. Planning where to use digital signatures

A digital signature may not only be introduced exclusively for DCCs but in the best case, the investment should bring a solution to sign all kinds of documents of one organisation, that need digital signature in the future. Thus, the first step is to bring experts from management, governance and technical/service divisions together to evaluate what documents should be signed, who is going to sign and how many signatures would be applied per day / month / year. You may find, that some signature systems are already in place and consider extension of these to the DCCs. Or alternatively, you find that replacement of the existing systems may be needed in favour of a more universal solution. Even larger organisations are careful with available resources and aim to maintain only one system.

* 1. Evaluation of legal requirements your organization must fulfil

Legal requirements show the boundary conditions which solutions could be introduced for digital signatures. It starts with the basic question, if policies of the organisation permit digital signatures in business processes. The NMI in Germany found for example that they had to negotiate an update of the organization’s policy with the government to allow digital signatures equally to hand-written signatures on paper. In this respect, your national government may define legal requirement which signatures must be used in your business processes that would also affect DCCs. Similar, national calibration and or accreditation guidelines may prescribe specific kinds of digital signature to use. In this step, management and legal experts, but also some IT experts with relevant background will have to work together to evaluate the relevant legal requirements.

* 1. Planning of required infrastructure

Once having the scope of digital signature application and the legal requirements, planning for the technical realization can start. This will include making decisions on what kind of hardware and software to acquire and how many devices, licences, etc. would be needed. It could also require to plan for new facilities (rooms) for signing, some organizations operate a signature server for example in a kind of room that is protected like in a vault. Furthermore, roadmaps are defined for the implementation of the digital signatures including change management, e.g. through pilot services and training of staff. Financial aspects will play an important role when planning the implementation. Not only the hardware and software is of interest but also the costs for longer term maintenance of the signing system (see Phase 3 for details). Acceptance by customers will also need to be considered. At this step not only management and IT experts play an important role, but also the employees who will use the signing system later on and may add technical preferences. For example, some laboratories may already have an automated DCC creation and would benefit from a signature system that allows integration into their software and processes.

* 1. Acquisition and set-up of infrastructure for signing

Following the implementation roadmap, acquisition and set-up of hardware, software and services is done. Depending on the size of the organization and solution to be implemented, this may take a few months, up to more than a year. All members of your organisation will be involved either in implementing or learning to use the new signature system.

Phase 2: Signature in workflow DCC creation / use (daily business)

* 1. Creation of DCC

DCC may be created in various ways, from manually entering information to commercial office software and up to fully automated generation using bespoke software environment.

In any case structure of file system has to be determined – where are files to be signed, where these are moved when signed, where archived for later use after deploying to customer etc.

When planning digital signing of a document, it has to be determined that document is ready for signing – approval from creator and if specified also from supervisor and that signature is attached to final version of the correct document.

* 1. Application of signatures / seals

If personal signatures are chosen, every person entitled to sign has to have means to do it. If there is no national means available (ID-card with electronic capabilities for example), commercially available solutions have to be implemented.

If signature is put into file (PDF for example), there has to be possibility to distinguish the signed files from not signed ones, e.g adding some marker to file name. Container based signing creates a new “container” file with signed document in it, so it’s easily distinguishable as a signed file.

When using organization signatures/stamps it is necessary to implement a software environment where files can be uploaded, identified and their status indicated (in need of signing, approved, rejected etc), users are securely identified and can apply correct status to files. Signature of organization can then applied either automatically by environment or by a person entitled to have the rights.

* 1. Storage of signed DCC

When signing with qualified signature, it gives protection against changing file’s contents but security means against unauthorized erasing or moving the files still have to be applied.

* 1. Transmission of signed DCC to customer

Signature gives protection against unintended tampering of information but general confidentiality rules that apply in organization have to be applied to be sure that DCC reaches the intended recipient and no other. For extra security there are means available for encrypting the signed files, for example in Estonia a signed file can be encrypted so it can be opened only by a person with specific personal ID number, using ID card or other equivalent electronic identifying means.

* 1. Customer validating (DCC and) signature when receiving DCC (DCC integrity, authenticity checking)

Validation possibility has to be a part of chosen signing solution, it can be independent software that can check the certificates or customer can validate the signature by means provided by issuing organization, e.g uploading file to website and getting confirmation of authenticity. In case of signed PDF files, most PDF readers can show details of signature and origin of signing rights (certificates) associated with signature.

Verification of container based signature can be done using the same software as for creating and opening the container.

Phase 3: Maintenance of signing infrastructure (things to consider for keeping it running)

* 1. Updating hardware and software

Chosen solution must be kept up to date as any other software environment, when physical cards, readers or sticks are used, these might wear and have certificates limited by certain time period.

* 1. Late requests for DCC validation

There has to be a plan how to validate a signature that is given certain amount of time ago, maybe limits for applicable validation time have to be given out. It is essential that signature solution provider has a policy for ageing signatures.

General thought has to be given if after longer period of time there would be a possibility to open the files at all. If for example PDF files would not be used anymore, would there still be possibility to open these old files after 10 or 20 years or read the signatures?

* 1. Updating/replacing signatures

Re-signing documents can be needed when cryptographic means used for signing have been updated after previous version is not considered to be safe anymore. For example in Estonia cryptographic means for signing have been updated several times over years but a solution is been made available for users to re-sign the documents with current level security signatures. Signed document remains thereby unchanged.