SmartCom

Document specifying rules for the secure use of DCC covering legal aspects of metrology

DCC

EN

DOI: 10.5281/zenodo.3664211

Document specifying rules for the secure use of DCC covering legal aspects of metrology

Version 1.0

DOI: 10.5281/zenodo.3664211

Editors

Aalto University, Finland:
P. Nikander, T. Elo, T. Mustapää, P. Kuosmanen

Tallinn University of Technology, Estonia:
K. Hovhannisyan, O. Maennel

National Physical Laboratory, United Kingdom:
C. Brown, J. Dawkins, S. Rhodes, I. Smith

Physikalisch Technische Bundesanstalt, Germany:
D. Hutzschenreuter, H. Weber, W. Heeren, S. Schönhals, Th. Wiedenhöfer

Comprising the results from our research and the fruitful and intensive discussions with all our other project partners worldwide.

Contact: smartcom@ptb.de

Tallinn February 2020

DOI: 10.5281/zenodo.3664211

Table of Contents

DOI: 10.5281/zenodo.3664211

1 Introduction

Traceability in metrology refers to a traceability of measurement results in an unbroken chain to nationally realized reference units of measure like for second, metre or kilogram and by this to the units defined by the International System of Units (SI) [1]. Today, this traceability is established by chain-link of calibrations of measuring equipment (items). The measuring equipment can be artefacts or measuring instruments. At each calibration, information on the accuracy of measuring equipment is evaluated, for example as a statement of measurement uncertainty. The information is reported by means of a calibration certificate.

The calibration is an essential part of a well-defined national quality infrastructure organised by governmental organisations. On top of the national regulation is an international quality infrastructure which is established by national metrology institutes and international organisations like the International Committee for Weights and Measures (CIPM), the International Standards Organisation (ISO), etc. The objectives of the international network are to ensures a worldwide comparability of measurements.

While the accumulation and assessment of measurement data for calibration has been digitalised in many aspects in recent years, the reporting of the calibration certificate still relies on a printed paper documents with handwritten signatures. Reliable concepts for a digital handling of certificates are urgently needed providing a digital counterpart to these analogue documents.

This document will outline the "as-is" state of the existing European and international quality infrastructure for calibration. State-of-the-art cryptographic methods are presented and applications of these methods for securing and transmitting digital calibration certificates are discussed. Both, chances and risks of the digital calibration certificate are outlined.

DOI: 10.5281/zenodo.3664211

2 European state-of-the-art

The Regional Metrology Organisation (RMO) of Europe is EURAMET which coordinates the cooperation of National Metrology Institutes (NMI) in Europe.

In addition to EURAMET, there is the European co-operation for Accreditation (EA) that is appointed by the European Commission to develop and maintain a harmonised accreditation infrastructure [2]. The EA members are currently 50 National Accreditation Bodies (NAB). The NABs are officially accepted by their national governments, to assess and verify organisations performing conformity assessment activities such as certification, verification, inspection, testing and calibration against international standards.

While there is only one NAB per Member State, there may be plenty of accredited bodies for the conformity assessment in the same member state.

Today's European state-of-the-art handling of calibration certificates is outlined in the following for three representative examples of national accreditation networks: Germany, United Kingdom and Estonia.

2.1 Calibration chain in Germany

The calibration chain in Germany is illustrated in Figure 1 and can be described as follows [3]:

- At the top are the national standards, which in our case are located at PTB in Braunschweig. The PTB has the legal mandate to represent the SI units and to make available and pass on the national standards. PTB performs around 5000 calibrations per year.

DOI: 10.5281/zenodo.3664211

- The second level subsumes all accredited calibration laboratories observed and tested by the "Deutsche Akkreditierungsstelle GmbH, DAkkS" (the German NAB) which ensures uniform and consistent quality standards of the metrological infrastructure. Here, calibration certificates are issued for the working standards and factory standards, which in turn are derived from the reference standards. The DAkkS laboratories perform around ten times as many calibrations as PTB per year.

- On the third level in-house calibration laboratories are to be found, which monitor the in-house measuring equipment in the company based on the calibration certificates of the accredited calibration laboratories mentioned above. In-house calibrations are around ten times as much as calibrations carried out in DAkkS laboratories.

- Last in line are all company divisions that carry out measurements and tests on production level.

DOI: 10.5281/zenodo.3664211

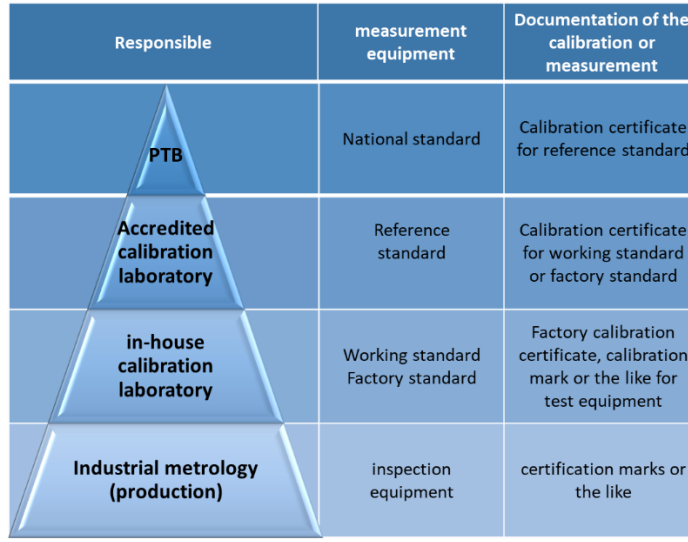

Figure 1 *Calibration chain in Germany [3]*

2.2 Calibration chain in the UK

The calibration chain in the UK is described as follows:

- In the UK, the national bodies that propagate the international standards through traceable procedures are divided into legal and standard metrology organisations. Standard metrology is managed by the national NMI, the National Physical Laboratory (NPL accredited to ISO 157025:2017) and legal metrology by the Office for Product Safety and Standards (OPSS). NPL performs typically 7000 calibrations per year.

- Designated Institutes (DIs) perform calibrations in specific areas. For example, the National Engineering Laboratory (NEL) performs metrology for fluid flow; the UK National Measurement Laboratory (NML) for Chemical and Bio-Measurement.

DOI: 10.5281/zenodo.3664211

- The United Kingdom Accreditation Service (UKAS) is the UK's National Accreditation Body (NAB), responsible for determining, in the public interest, the technical competence and integrity of organisations such as those offering testing, calibration and certification services.

- ISO 17025 accredited Calibration and Testing laboratories form the next layer for the traceable calibration chain.

- Finally, at the end of the chain are the metrology functions within industrial organisations whose operations and products are fundamentally dependent on traceable accuracy e.g. in the aero-engine manufacturing industry.

- As part of a trial procedure within the Electromagnetic and Electrochemical Technologies division at NPL, signed PDF versions of calibration certificates are being provided to customers. This is a first step towards digital calibration certificate communication, in the sense that the document is electronically signed, but the certificate is not fully digital and still needs to be viewed on a screen to extract relevant information. It is not 'machine readable' in terms of the aims of this project.

2.3 Calibration chain in Estonia

The calibration chain in Estonia is described as follows:

- Metrology in Estonia is governed by the Ministry of Economic Affairs and Communications.

- The organisations that provide metrological services include: The Central Office of Metrology, National standard laboratories, Reference standard laboratories, legal

DOI: 10.5281/zenodo.3664211

metrology and accreditation authorities, and accredited calibration and verification laboratories.

- The institutions involved in the metrological service ensure the traceability of national measurements and measurements in private law.

- The functions of the metrology authority and National standard laboratory are fulfilled by AS Metrosert within the framework of an administrative agreement, as well as representation of Estonia within EURAMET.

- AS Metrosert is accredited by the Estonian Accreditation Centre (EAK), that confirms the conformity of the laboratory to the requirements of EVS-EN ISO/IEC 17025:2017.

- Metrosert as an accredited laboratory performs calibration (around 15,000 annually) and verification (around 15,00 annually, 4000 with certificates) procedures with approximately 95% delivered as electronically stamped PDFs in 2019. This digital stamping procedure has been approved by the EAK.

- Digital stamping is conducted with a use of a hardware token, a service that is provided to Metrosert by *SK.ee.* Every time a digital stamping takes place, appropriate queries are initiated to SK.ee.

- This digital stamp service used on the PDF DCC is currently based on the Estonian ID-Card Software and is managed by the Estonian Information System Authority.

- Metrosert internally have implemented special IT solutions to manage the complete production process of digitally stamped PDF DCCs from customer request for a particular

DOI: 10.5281/zenodo.3664211

calibration, review of the content of the certificates to final delivery of the PDF DCC by Metrosert.

- MÕIS is another internally developed solution that allows customers to manage data of their measurement instruments. This platform helps to view the calibration history of the instruments, attach certificates and view digitally stamped DCCs.

While the Estonian case is a comprehensive example for the utilisation of existing national accepted tools for digital stamping and the exchange of signed digital documents, it is not covering the aspects of machine-readable calibration data. The PDF format is a digital format for human-readable documents. It does not provide a stable format for universal, exchangeable and machine-readable calibration data. Therefore, achieving interoperability of only human-readable data from PDFs with automated and software-controlled manufacturing systems suffers from similar issues as working with analogue calibration certificates.

2.4 eIDAS – European regulation for securing digital data

eIDAS is an EU law, regulating electronic signatures, electronic transactions, involved bodies, and their embedded processes to provide a safe way for users to conduct business online. The goal is to provide sufficient interoperability and transparency to conduct digital business securely within the European Single Market.

eIDAS was established in EU Regulation 910/2014 and has been applicable since 1st June 2016. Since 29th September 2018 organisations delivering public digital services within the EU must recognise electronic identification from all EU member states.

DOI: 10.5281/zenodo.3664211

eIDAS covers not only signatures for individuals, ‘electronic signatures’, but also provides for role-based signatures in the form of ‘electronic seals’. The process of changing a person/individual performing a role must be allowed and should follow an automated process.

DOI: 10.5281/zenodo.3664211

3 International challenges / issues

International outline of metrology organisations

The international traceability chain and the relationships and hierarchies of the various metrological organisations is shown in Figure 2.

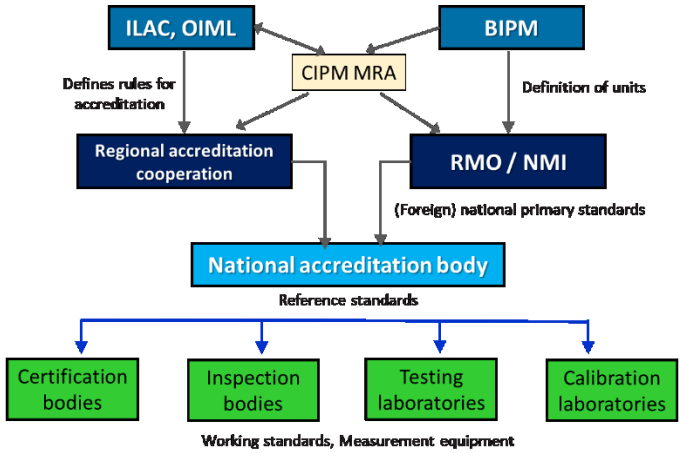

Figure 2 *International traceability chain*

At the forefront of international metrology is the Bureau International des Poids et Mesures BIPM, which defines the units and works with its member states and strategic partners worldwide to ensure and develop global comparability of measurements.

The international organisations such as Organisation Internationale de Métrologie Légale OIML and International Laboratory Accreditation Cooperation ILAC provide legal regulations on measurements, measuring instruments and the use of measured values support fair trade and promote people's trust in official measurements.

DOI: 10.5281/zenodo.3664211

The metrology institutes of the BIPM member states are coordinated in the Regional Metrology Organisations RMOs.

Currently six RMOs are recognized within the framework of the CIPM MRA (e.g. EURAMET from section 2). Similar reginal organisations exist in the area of accreditation and calibration.

In the framework of international and regional metrology organisations in Figure 2, the Measures Mutual Recognition Arrangement MRA established by the International Committee for Weights and Measures CIPM allows for mutual recognition of national measurement standards and for the recognition of the validity of calibration and measurement certificates issued by national metrology institutes.

Directives and regulations from the international and regional metrology organisations are the basis for national accreditation and calibration.

Alongside the framework in metrology, the international quality infrastructure is also supported by international organisations like ISO and IEC providing fundamental technical standards like ISO 80000 (the international system of quantities).

Challenges and issues for the secure use of DCCs in the international metrology organisation

The aspects of cryptographically securing the application of DCCs have proven to be particularly complex. No international standard has yet been found for secure transmission, digital stamps and signatures and the withdrawal of data. The implementation of internationally harmonised approaches is encountering the following general challenges and issues:

- It is still unclear to what dimension international acceptance of cryptographic securing is needed in future metrological applications. While the need of acceptance on a regional level is very clear as there are thousands of calibrations made every day, the international harmonisation may only be needed between the leading organisations.

DOI: 10.5281/zenodo.3664211

- The process for developing internationally acceptable methods for securing DCCs must be organised including different stakeholders from the international Quality infrastructure who are not directly involved in the area of cryptography and ICT. There is the risk of a rejection of topic as "No Issue" of metrology.

- When looking at the diversity of requirements in strongly regulated areas of legal metrology it turns out to be most likely that no complete international harmonisation may be achievable. But even harmonisation for the communication of data only for particular measurement device classes like weighing instruments can be of great benefit for international metrology.

DOI: 10.5281/zenodo.3664211

4 Minimum requirements for secure DCC transfer

The foundations for the secure use of Digital Calibration Certificates (DCC) and relevant cryptographical methods are the framework conditions for a secure transfer of DCCs that were identified as minimum requirements in the SmartCom project:

- Preservation of readability, integrity and authenticity [4, 5]
  - data not to be used out of context
- Long-term preservation of information [5, 6]
- Stable data format [4]
- Use of (qualified/advanced) electronic signatures [7,8]
  - Ensuring certainty of document's origin and integrity [6]
  - Allow for assigning representatives: a qualified electronic signature from the authorised representative of the legal person should be equally acceptable [6]
- Verifiable existence of user certificate at the time of signature [4]
  - Ensure legal validity over long periods of time (irrespective of future technological changes) [5, 6]
  - Documentation of validity period [5]
- Assurance that the person claiming a particular identity is in fact the person to which that identity was assigned [6]
- Allow for mutual recognition across borders [6, 8]
- EU- and worldwide
- Comply with privacy policy: processing and storage of personal data [4, 5, 6, 9]

DOI: 10.5281/zenodo.3664211

- Interoperability [4]: allow for
  - exchange of documents between different application systems
  - change of data format within application systems
  - replacement of entire application systems or single components
- Preservation of controllability of data [10]
- Allow for verification/ validation of data [5]
- Ensure usability: secure usability w/o special knowledge [10, 11]
- Scalability and modularity
  - Allow for supplements, amendments and substitution [10]
  - Unambiguous identification of modifications; in case of completely new report: unambiguous designation with reference to original document [5]
- Allow for withdrawal [7]
- Security by design (end-to-end encryption) [10, 12]

An implementation of the above requirements demands to consider two aspects: a) additional data structures in DCCs supporting the use as a digital document and b) an external infrastructure for the exchange and verification of DCCs.

These minimum requirements must be considered by any cryptographic solution selected for the secure use of DCCs and thus also by the potential infrastructure established for this purpose.

DOI: 10.5281/zenodo.3664211

5 Potential future infrastructure requirements

In the previous sections, a broad outline of the issues and challenges for future digital communications of metrology information has been given. Moreover, the requirements for secure digital communications for Digital Calibration Certificates derived in the context of SmartCom have been presented. However, the future of digital metrology in relation to Industry 4.0 will also demand an ever-increasing role for digital communication of metrology information in general. Here, interconnected smart sensors are a good example of this need.

Transmission of digital metrology data over public networks such as the Internet requires a robust security strategy to be adopted. Without this strategy in place, it will not be possible to guarantee that the data received has not been affected in the transmission process by a wide range of causes not least by bad actors in the internet domain e.g. cyber-criminals. This is relevant not only to legal metrology information but to all metrological data (i.e. science and industry).

Within the scope of this project, a range of current internet-based security protocols have been considered and the most appropriate is based on the use of Public/Private key encryption standards.

5.1 Overview of current international technical situation for certification of public keys

At this point in time, there is no single technical solution in place that would allow digital signatures to be created that would be legally binding worldwide, or even for a large

DOI: 10.5281/zenodo.3664211

proportion of the world. Already there are significant differences in the technical solutions used in Europe and Asia.

Europe currently relies on eIDAS regulation, the use of long-term keys, governmentally issued Smart Cards and corresponding X.509 certificates; while large parts of Asia relies on FIDO (Fast Identity Online) de-facto standards, based on biometric authentication and resulting short term keys. It is an open question whether these two systems can be aligned for technically signing documents.

For the non-legally binding case, there are two infrastructures that are used worldwide:

- For the Internet Security TLS (Transport Layer Security) there is a defacto infrastructure maintained by the major operating system vendors (Microsoft, Apple, etc.) and major browser vendors (Google, Mozilla, etc.). The TLS Key management infrastructure is based on the ITU-T (International Telecommunications Union) standard X.509 [13]. TLS is used for securing web-page access (HTTPS) and for securing email (S/MIME), among other things.

- For the Internet naming system DNS (Domain Name System), there is the DNSSEC infrastructure which is still in the adoption phase. The infrastructure is standardised by the IETF (Internet Engineering Task Force) and maintained in parallel with the DNS system itself. This system is unsuitable for legally binding signatures

Other than the Internet X.509 for TLS and other protocols, and DNSSEC, there does not appear to be any other cryptographic key management infrastructures of significance that work worldwide.

DOI: 10.5281/zenodo.3664211

5.2 Proposed future international metrology security infrastructure

Within an NMI, or any organisation that produces calibration certificates, there are traceable chains of accreditation, authorisation and identity validation of people, processes and equipment that are integral to the issuing of calibration certificates. In future, this complex hierarchy has to become digital. Physical signatures will be replaced by digital signatures. Currently the IT/IS infrastructure to support these digital ways of working i.e. a root certificate authority (CA) as part of a PKI [1] (Public Key Infrastructure), does not yet exist formally within the metrology community. As a consequence of the analysis performed within the SmartCom project of current digital infrastructures that already exist outside of metrology, a recommendation from SmartCom is that this IT/IS infrastructure in the form of a root certificate authority (CA) as part of a PKI be put in place. Precisely how this would be done, and the arguments for and against any form of implementation is beyond the scope of the current project but could be considered within a future project.

Currently, OIML and WELMEC legal metrology standards relating to software operating in devices [14,15] is limited to autonomously operating instruments that communicate at most over Local Area Networks (LANs) to simple peripheral type equipment and not on Wide Area Networks (WANs) such as the internet. A further recommendation of SmartCom is that

[1] 'Public' here is meant in the sense of being public to the metrology community

DOI: 10.5281/zenodo.3664211

standards that cover security of digitised metrology information transmitted over public networks be developed.

As mentioned earlier, the need for securing all digital metrology communication will inevitably mean that these standards would also be relevant, in part, to scientific and industrial metrology related communications as well as legal metrology.

Finally, the idea of conceptualisation of metrology information in general needs further development beyond the current scope of SmartCom. For the purpose of exchange of digital metrology related information between two devices (without human interaction); or between machine and human, it will be necessary to link this information to clear and unambiguous descriptions of its actual meaning. Currently, the technologies associated with Ontologies, Taxonomies and semantic Linked Data storage provide a direction for future research into ways of delivering the required precision definitions for all types and layers of the metrology infrastructure. Associated meta-data standards will need to be developed for all layers of digital metrology infrastructure. Again, this is beyond the scope of the current project but should be considered in any follow up project.

DOI: 10.5281/zenodo.3664211

6 References

[1] BIPM Brochure, *The international System of Units (SI) 9th edition 2019*, https://www.bipm.org/en/publications/si-brochure/ (accessed February 2020)

[2] P. Howarth, F. Redgrave *"*Metrology – in short*"* 3rd edition, ISBN 978-87-988154-5-7, July 2008

[3] DAkkS-Schrift 71 SD 0 006, *Rückführung von Mess- und Prüfmitteln auf nationale Normale,* 2010

[4] *BSI Technische Richtlinie 03125 – Beweiserhaltung kryptographisch signierter Dokument*, Bundesamt für Sicherheit in der Informationstechnik, Version 1.1, 2011.

[5] DIN EN ISO/IEC 17025:2018-03, *General requirements for the competence of testing and calibration laboratories*, German and English version, DIN Deutsches Institut für Normung e. V., Berlin

[6] "*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*", Official Journal of the European Union, L 257, pp.73-115, 2014.

[7] S. Hackel et al., "The Digital Calibration Certificate", Metrology for the Digitalization of the Economy and Society, PTB-Mitteilungen 127 (2017), Heft 4, doi: 10.7795/310.20170403

[8] Hoppe and Klein, "Remote-Erstellung von qualifizierten elektronischen Signaturen bei

DOI: 10.5281/zenodo.3664211

Vertrauensdiensteanbietern", 15. Deutscher IT-Sicherheitskongress, BSI, Bonn, May 2017.

[9] General Data Protection Regulation. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, Official Journal of the European Union (OJ), L 119, pp. 1-88, 2016.

[10] R. Fay et al., "Gefahrlos durch den Nebel – Ein Sicherheitskonzept für das Fog-Computing", 15. Deutscher IT-Sicherheitskongress, BSI, Bonn, May 2017.

[11] G., Peter. "Lessons Learned in Implementing and Deploying Crypto Software", In Proceedings of the 11th USENIX security symposium, pp. 315-325. 2002.

[12] B., Elaine. "Recommendation for Key Management, Part 1: General", NIST Special Publication 800-57 Part 1 Revision 4, Section 5, pp. 29–61, January 2016. http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4 (accessed February 2020)

[13] "*Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks*", ITU-T Recommendation X.509, 2019, https://www.itu.int/en/publications/ITU-T/Pages/default.aspx (accessed February 2020)

[14] OIML D 31, *General requirements for software controlled measuring instruments,* Edition 2008 (E), https://www.oiml.org/en/files/pdf_d/d031-e08.pdf (accessed November 2019)

DOI: 10.5281/zenodo.3664211

[15] WELMEC 7.2, *Software Guide (Measuring Instruments Directive 2014/32/EU)*, 2019, https://www.welmec.org/fileadmin/user_files/publications/WG_07/Guides/WELMEC_Guide_7.2_Software_Guide_2019.pdf (accessed February 2020)

DOI: 10.5281/zenodo.3664211

The content presented was developed within the framework of the EU-funded project SmartCom *"Communication and validation of smart data in IoT-networks" with the* support of international partners from science and industry.

https://www.ptb.de/empir2018/smartcom
(retrieved February 2020)

The EMPIR initiative is co-funded by the European Union's Horizon 2020 research and innovation programme and the EMPIR Participating States

DOI: 10.5281/zenodo.3664211