The Digital Calibration Certificate

Siegfried Hackel[1], Frank Härtig[2], Julia Hornig[3], Thomas Wiedenhöfer[4]

Abstract

A digital calibration certificate (DCC) serves for the electronic storage, the authenticated, encrypted and signed transmission and the uniform interpretation of calibration results. Under the leadership of the Physikalisch-Technische Bundesanstalt (PTB), a concept is being developed that will allow these data to be handled in the future. The target group are all facilities worldwide, which need proof of the metrological traceability of their measurement results. These include metrology institutes and designated institutes, national calibration offices, calibration laboratories and many facilities in industry that require proof of their quality management systems.

The analogue calibration certificate has so far rarely generated a surplus value for a company since the data obtained during the calibration are time-consuming and error-prone. The DCC compensates for this crucial disadvantage of its analogue counterpart. Thanks to its machine readability, digitally supported production and quality monitoring processes are greatly supported. This creates a crucial added value for a company that uses the DCC.

In addition to the structure of the DCC, special framework conditions must be laid down for its transfer. These include cryptographic protection procedures. They ensure the electronic transmission of the contents as well as the integrity and authenticity of the contents of the DCC. The core competency for appropriate procedures is not in the field of metrology institutes. For this purpose, previous results and external expertise will be used. However, the framework conditions are defined by the metrology institutes, taking legal requirements into consideration.

The aim is to create an internationally recognized DCC format. This is to be established as an exchange format in the entire field of metrology. Based on the DCC, exchange formats should be developed in legal metrology, for digital type examination certificates and for the "digital twin" (DT), see Chapter 5.

[1] Dr. Siegfried Hackel, Area 1.01, e-mail: siegfried.hackel@ptb.de

[2] Prof. h. c. Dr.-Ing. Frank Härtig, Division 1, e-mail: frank.haertig@ptb.de

[3] Dr.-Ing. Julia Hornig, Department 1.2, e-mail: julia.hornig@ptb.de

[4] Thomas Wiedenhöfer, Division 1, e-mail: thomas.wiedenhoefer@ptb.de

1 Introduction

The calibration of measuring instruments is an essential pillar for correct and comparable measurements and manufacturing in industry. Without this, it is not possible to make profound statements about the quality of a manufactured product. Table 1 gives a hierarchical overview of the calibration certificates provided in Germany.

The calibration certificate has been used for many decades to verify the calibration of a measuring instrument. It is issued by PTB and by the Deutsche Akkreditierungsstelle GmbH (DAkkS) to accredited calibrating laboratories. DAkkS is the national accreditation body of Germany.

The structural design of the DCC is of fundamental importance. PTB [1, 2] and

Calibration institute	Standard type	Calibrations per year
PTB	National standard	≈ 10 000
Accredited calibration laboratory	Reference standards	Some 100 000
Internal calibration laboratory	Working standards and factory standards	Many millions

Table 1: Hierarchical overview of the calibration certificates provided in Germany.

doi: 10.7795/310.20170403

DAkkS [3] have issued corresponding regulations. General information, such as for example the calibrating object, is shown in a strongly regulated form. This creates a uniform basis, which can be managed by the national calibration offices. In contrast, the measuring results concern only special professional groups. These often have individual data exchange formats that have established themselves in the market and should therefore be retained (e.g., [4]). Essentially, the structural design of a DCC is a technical question which is coming under the responsibility of metrology institutes for the first time.

2 Basic norms and standards

The goal is to create an internationally recognized DCC format. The format should be set up in the whole area of metrology as an exchange format. It should then be valid for the digital twin (see Chapter 5) as well as in legal metrology and should then be used for digital type examination certificates.

2.1 Metrological norms

As with its analogue counterpart, the following norms and guidance notes are also applicable to the DCC:

- the SI units [5],
- the International vocabulary of metrology (VIM) [6],
- the GUM [7],
- the CODATA table: [8]; its review: [9], and
- ISO/IEC 17025 [10].

The development of the DCC has taken account of the fact that new versions of SI [11] and ISO/IEC 17025 [12] are pending. It is crucial that all specifications in the DCC have to be made according to these regulations.

2.2 XML as a data exchange format

The DCC is provided in the Extensible Markup Language (XML). XML was developed by the World Wide Web Consortium (W3C) and was published on the web [13]. It has established itself internationally as a data exchange format. Cryptographic methods can be robustly applied to XML-based data structures [14, 15]. Further information about XML is to be found, e.g., under [16, 17]. There is already a very developed approach for data exchange from the VDI / VDE [4].

A major advantage of XML is its machine readability. In addition, XML is also basically readable for a human being. It is also very important that XML is a long-term storage data format. This is of importance because the files must still be readable in several decades. For further information on long-term storage data formats, see [14, 18].

IEC TS 6270 "Identification of units of measurement for computer-based processing" [19] shows the handling of the SI units and derived units in XML. They can be found in the Common Data Directory on the IEC website [20].

2.3 Cryptographic protection methods

On the one hand, the integrity and authenticity of the data must be respected for a DCC. On the other hand, electronically stored data can easily be changed and copied as desired. Therefore, the use of cryptographic protection methods for the DCC is necessary. A good summary of cryptography can be found in [21].

In Germany, there has been legal regulation and related instruments for this purpose for many years. The use of qualified electronic signatures (QeS) and time stamps according to Germany's electronic signature law (SigG) [22] and its signature ordinance (SigV) [23] have ensured that integrity and authenticity are preserved. Documents bearing a QeS are to be treated legally as certificates. They are considered as safe in court. This has been verified in several fictitious court trials [14].

A QeS generation has a validity of approximately five years. Before the expiration date, it is replaced by a new QeS generation. For this reason, more than 10 years ago, PTB developed a procedure for ensuring the long-term preservation of cryptographically signed documents. This has resulted in an international standard [24], a DIN standard [25] as well as a translation recommendation from the Federal Office for Information Security (BSI) [26]. Various manufacturers have certified their products according to [24, 26]. PTB has such a product.

In addition to the installation of the QeS, the encryption of the DCC for safe transport from the calibration laboratory to the customer has been established with this method. In addition, the customer receives the public key of the calibration laboratory.

For the above reasons, there have been applications in Germany for a long time, for which the protection of integrity and authenticity have been of vital interest. Examples which may be mentioned are:

- legislation on personal status (registry office; effects on the law of inheritance),
- waste management, and
- procurement for the federal administration in Germany.

doi: 10.7795/310.20170403

In the meantime, many EU Member States have also adopted corresponding legal regulations. Therefore, the EU has adopted the so-called eIDAS Regulation [27], which is valid alongside SigG [22] and SigV [23]. In addition to the QeS, digital seals can also be used. The implementation of the eIDAS Regulation has not yet been completed.

3 Structure of the digital calibration certificate

The general structure of a DCC is subdivided into four areas:

- administrative data (regulated area),
- measurement results (partially regulated area),
- comments (not regulated area), and
- document (additional area).

XML is provided as a data format with the corresponding schema files.

3.1 Administrative data (regulated area)

Administrative data contains information of central interest. The data fields are fixed. The information is usually on the first page of an analogue calibration certificate. The data are used to clearly identify the calibration laboratory, the calibration object and the calibration customer.

Table 2 lists the fields fixed by PTB and DAkkS. They apply to the DCC accordingly.

The identifiers are defined. The data, such as, e.g. "date of calibration" are formatted according to international standards. Letters are allowed in the form of Unicode. Numbers are represented in

Table 2:
List of fixed fields from [1 – 3].

English	German	Meaning / remark	Ref.
Letterhead	Briefkopf	Name and address of laboratory	[1 – 3]
Accredited by the	akkreditiert durch die	e.g. DAkkS	[3]
As a calibration laboratory in the	als Kalibrier-laboratorium im	e.g. DKD	[3]
Calibration certificate	Kalibrierschein		[1 – 3]
Object	Gegenstand	Name of the device, brief characterization	[1 – 3]
Manufacturer	Hersteller	Name of the manufacturer	[1 – 3]
Type	Typ	Type of the device	[1 – 3]
Serial No.	Kennnummer[1, 2] Fabrikat/Serien-Nr. [3]	Number of the examined device, standard, preparation	[1 – 3]
Applicant [1, 2] customer [3]	Auftraggeber	Name of the customer, street, place of business	[1 – 3]
Number of pages	*Anzahl der Seiten*	*See Note 1 below Table 2*	*[1, 2]*
Number of pages of the certificate	*Anzahl der Seiten des Kalibrierscheines*	*See Note 1 below Table 2*	*[1 – 3]*
Reference No.	Geschäftszeichen		[1, 2]
Calibration mark	Kalibrierzeichen	Unambiguous	[1 – 3]
Date of calibration	Datum der Kalibrierung	Date or start to end of calibration	[1 – 3]
Date	Datum	Date of issue of the calibration certificate	[1 – 3]
Signature / seal	*Unterschrift / Siegel*	*See Note 1 below Table 2*	*[1, 2]*
Head of the calibration laboratory	*Leiter des Kalibrierlaboratoriums*	*See Note 1 below Table 2*	*[3]*
Person in charge	*Bearbeiter*	*See Note 1 below Table 2*	*[3]*
Mutual Recognition Arrange-ment (MRA)	Gegenseitige Anerken-nungsvereinbarung	Yes / no	[1 – 3]

Note 1:
With the DCC, the number of pages is obsolete since no printout occurs. The manipulation of the DCC is excluded using hashes, see Section 2.3.

Note 2:
The method for attaching cryptographic signatures to the DCC allows one or more signatures to be attached. It is also possible to sign several DCCs simultaneously (keyword: mass signature). According to the eIDAS Regulation, the fixing of a seal is also possible. Further information is to be found in Section 2.3.

the form of Arabic numerals. The main language is English, but the information can also be given in another language.

3.2 Measurement results (partially regulated area)

The representation of the measurement results is one of the most challenging tasks to be solved in the shape of the DCC. The reason for this is the variety with which measurement results are presented. In addition, it is necessary to integrate already existing and established data exchange formats into the concept as in [4]. At the same time, a simple structure can be presented for those who do not already have an existing data exchange format. Therefore, this area cannot be generally regulated.

However, what is strongly regulated is that the measurement results must be presented completely and only on the basis of the SI [5]. They can be represented as a scalar, vector, matrix or tensor. A complete measurement result includes the following data:

- identifier,
- measurement value,
- expanded measurement uncertainty,
- coverage factor,
- unit, and
- time.

The information on the time is furthermore optional. The identifiers are composed of Unicode letters. The numbers and time formats are defined according to existing standards. The representation of the enlargement factor and the unit are given. The guidelines are based on the standards of the BIPM.

Units that are outside the SI can also be displayed (e.g. nautical miles, millimetres of mercury, degree of Oechsle). Irrespective of this, the data in SI are always valid.

The use of an individual data structure is possible provided the results are complete and take the SI

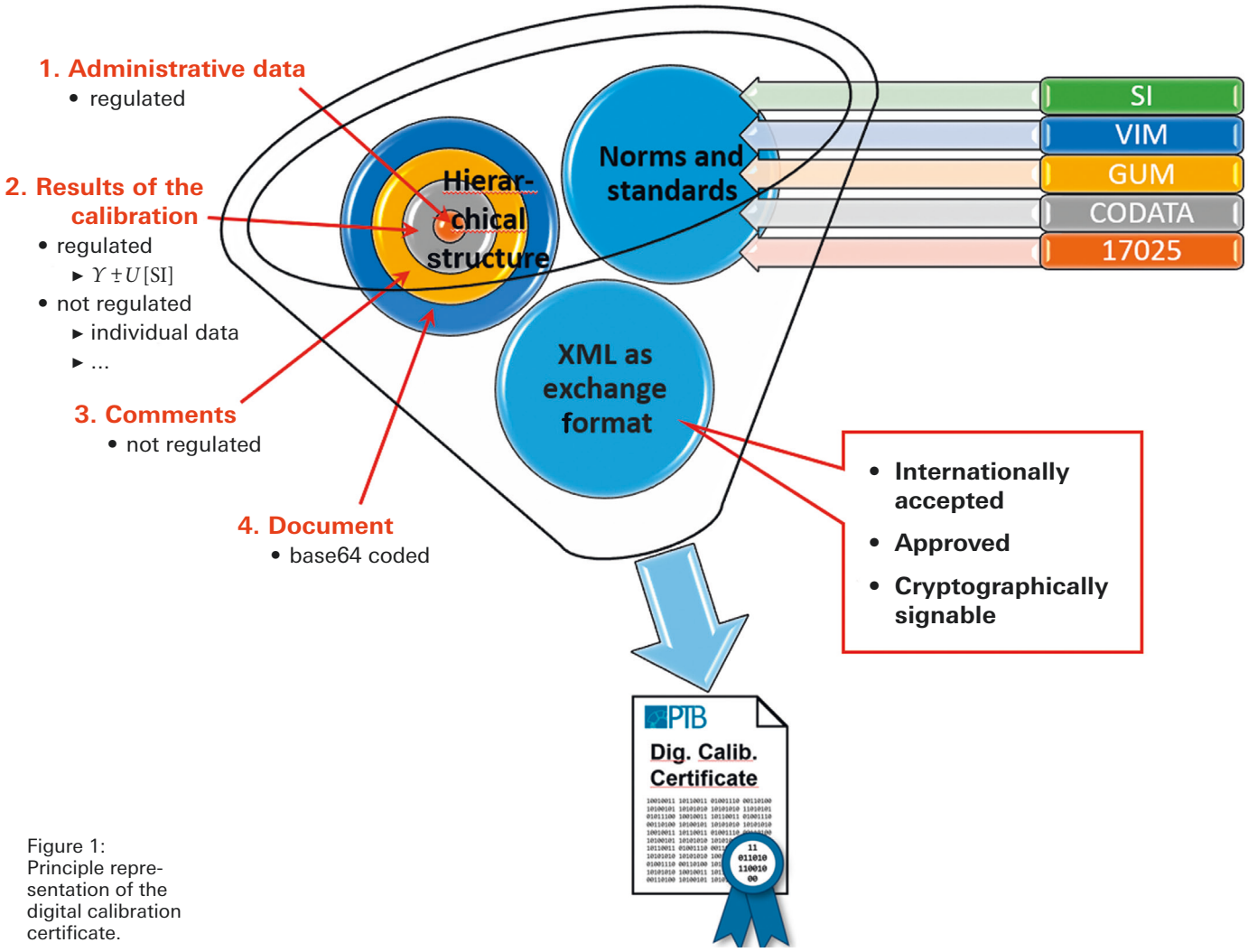

Figure 1:
Principle representation of the digital calibration certificate.

doi: 10.7795/310.20170403

into account. In the case of the individual data structures, it must be considered that often descriptive components and information on measurement uncertainties are not available. In these cases, adjustments must be made. In addition, tools must be provided to visualize the content.

The universal data structure is a linear structure. It consists of blocks of text and blocks with measurement results. The text blocks serve as an explanation of the results of the measurements and can be carried out, in addition to English, in other languages. The advantage of the universal data structure is its simple and universal use. Within the scope of developments, PTB will develop tools for creating universal data structures, as well as provide tools for their visualization.

3.3 Comments (not regulated area)

The comments section contains individual information about a measurement process, which provides further information on the measurement results. This range can be used optionally and without requirement. Possible data are, for example, graphics from measurement curves, video or audio information, as well as individual measurement series in any format.

3.4 Document (additional area)

In this area, an optional version of the calibration certificate stored in PDF-A can be stored according to the previous paper publication. Users of the DCC can thus see an image of their usual calibration certificate during the transition to a digital world. Using the Base64 encoding scheme [28], the PDF-A can be stored in XML together with the information set mentioned above.

4 Need for action when handling digital calibration certificates

4.1 Problem of retractability

A DCC must also be able to be retracted. It is, however, possible at any time to make copies of a DCC which are identical to the original. SigG [22], SigV [23] and the eIDAS Regulation [27] do not provide for the withdrawal of digitally signed documents.

4.2 Solutions for the retraction of digital data

Two different methods have been investigated. Both need a trustworthy body, which still has to be established.

According to SigG and SigV, it is possible to block a QeS through an entry in a register. The validity period of a QeS is also recorded in this register. Both pieces of information can be requested by a user of the infrastructure. This is done by querying the certification authority (CA) according to the online certificate status protocol (OCSP) [29]. In analogy to this, a trustworthy site could be used to provide a list of valid DCCs. An automated query for this service together with an integrity and authenticity check would have to be realized. The simplest variant of the service would be to keep a list of the hash values of each DCC.

Another possibility would be the use of blockchain technology, see, e.g., [30]. The retraction of electronically issued certificates was shown by the example of an examination certificate [31]. There is already a higher education institution that is using the procedure [32]. The method is tamper-resistant in a public blockchain with a

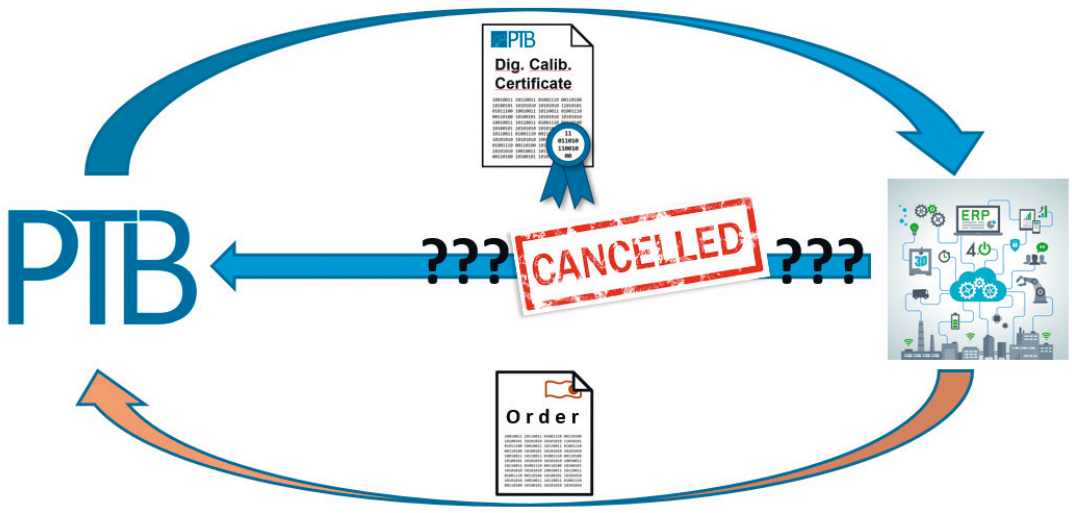

Figure 2:
Digital calibration certificates must be retractable.

trustworthy site. However, the blockchain also has weaknesses in long-term availability, in addition to its cryptographic weaknesses (It is not defined which software and which method is used.). Another disadvantage of the blockchain is that the calculation of a blockchain is very computationally intensive and thus energy-intensive. Therefore, it is only suitable for a manageable number of records (approximately to 105) if the records themselves are in the range of a few MB.

4.3 Validity of the digital calibration certificate in Germany, the EU and the world

A legal view on the validity and legal resilience of DCCs in Germany seems to be given by the numerous investigations undertaken in the field of use of the QeS, see below. Comparable studies are planned at EU level as well as at the international level.

5 Digital twin – Project Gemimeg

In the future, a customer of PTB (or a calibration laboratory) will decide whether a DCC for the relevant calibration material would be satisfactory or whether referring to the consistent further development of the DCC, the DT, would be preferable. The DT will include additional data and software as well as the DCC. Figure 3 shows the generic approach of the DT.

The DT of the calibrated measuring instrument provides plenty of new possibilities. Added value can be generated by the simulation of manufacturing processes alone. This results in a significant increase in the quality of the production, since the behaviour of the measuring device is precisely known. In the production of small quantities, this results in an increase in efficiency because the simulation of the production process results in a significant advantage. This becomes clear when considering the life cycles in the reference model of industrial 4.0 components (e.g. [33]) and the RAMI 4.0 model [34].

6 References

[1] *PTB form for issuing a calibration certificate with reference to CMC*, PTB.

[2] *PTB form for issuing a calibration certificate without reference to CMC*, PTB.

[3] *DAkkS*: Paper DAkkS-DKD-5, Anleitung zum Erstellen eines Kalibrierscheines, http://www.dakks.de/sites/default/files/dakks-dkd-5_20101221_v1.2.pdf. (Last accessed: 15.1.2018).

[4] VDI/VDE GUIDELINE, VDI/VDE 2623: *Format for data exchange in management of measuring and test equipment*, February 2012.

[5] BIPM: *Standard, Le Système international d'unités/ The International System of Units* (Brochure sur le SI/SI brochure), 2006.

[6] B. Brinkmann: *International vocabulary of metrology, Basic and general concepts and associated terms (VIM)*, ISO/IEC Guide 99:2007 = Vocabulaire international de métrologie, Wissen : Messwesen, Berlin, Vienna, Zurich, Beuth, 2012.

[7] BIPM: *Standard JCGM 104:2009: Evaluation of measurement data – An introduction to the "Guide to the expression of uncertainty in measurement" and related documents*, July 2009.

[8] CODATA recommended values of the fundamental physical constants.

[9] P. J. Mohr, D. B. Newell, B. N. Taylor: *CODATA recommended values of the fundamental physical constants,* Reviews of Modern Physics 88 3, p. 337, 2014.

[10] DIN EN ISO/IEC DIN EN ISO/IEC 17025:2005, *General requirements for the competence of testing and calibration laboratories*, August 2005.

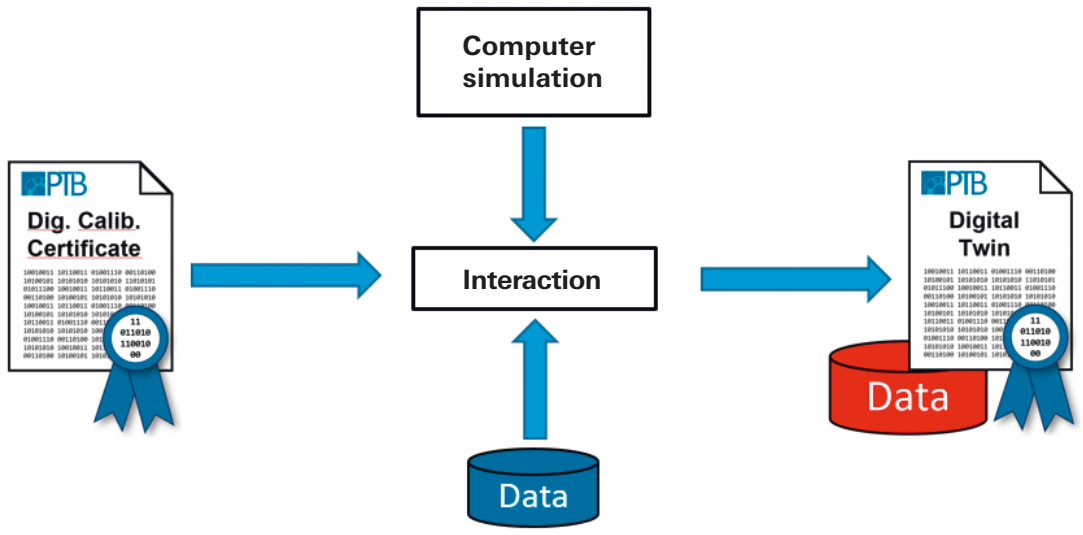

Figure 3: Generic approach of the digital twin.

doi: 10.7795/310.20170403

[11] Draft. *The International System of Units (SI) – DRAFT*.
[12] ISO/IEC/DIS ISO/IEC/DIS 17025, 2016-10-21, ISO/IEC/DIS 17025 – Clean version (ISO/CASCO/WG 44 N 96).
[13] *Extensible Markup Language (XML) 1.0* (Fifth Edition), https://www.w3.org/TR/xml/. (Last accessed: 10.10.2017).
[14] P. C. Johannes: *Beweissicheres elektronisches Laborbuch, Anforderungen, Konzepte und Umsetzung zur langfristigen, beweiswerterhaltenden Archivierung elektronischer Forschungsdaten und -dokumentation*, Der Elektronische Rechtsverkehr, Vol. 29, Baden-Baden, Nomos, 2013.
[15] www.archisafe.de, http://www.ptb.de/cms/archisafe/startseite.html. (Last accessed: 06.06.2017).
[16] Wikipedia: *Extensible Markup Language*, https://de.wikipedia.org/w/index.php?oldid=164814823. (Last accessed: 07.06.2017).
[17] H. Vonhoegen: *Einstieg in XML, Grundlagen, Praxis, Referenz*, Rheinwerk computing, Bonn, Rheinwerk, 2015.
[18] nestor – Home, http://www.langzeitarchivierung.de/Subsites/nestor/DE/Home/home_node.html. (Last accessed: 11.10.2017).
[19] *Technical Specification, Identification of units of measurement for computer-based processing*, January 2017.
[20] IEC: *Common Data Directory*, IEC 61360, https://cdd.iec.ch/. (Last accessed: 11.10.2017).
[21] K. Schmeh: *Kryptografie, Verfahren, Protokolle, Infrastrukturen*, iX-Edition, Heidelberg, dpunkt-Verl., 2009.
[22] SigG, *unofficial table of contents*, http://www.gesetze-im-internet.de/sigg_2001/. (Last accessed: 06.06.2017).
[23] SigV, unofficial table of contents, http://www.gesetze-im-internet.de/sigv_2001/. (Last accessed: 06.06.2017).
[24] BSI-CC-PP-0049-2014, https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0049+PP0049_2014.html. (Last accessed: 06.06.2017).
[25] DIN 31647:2015-05, Beuth.de, https://www.beuth.de/de/norm/din-31647/229134562. (Last accessed: 11.10.2017).
[26] BSI TR-ESOR, Main document, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html. (Last accessed: 19.07.2017).
[27] EU: eIDAS, Official Journal L 257/2014, http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2014:257:FULL&from=EN. (Last accessed: 11.10.2017).
[28] Wikipedia: Base64, https://de.wikipedia.org/w/index.php?oldid=164159739. (Last accessed: 07.06.2017).
[29] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, 2017, https://tools.ietf.org/html/rfc6960. (Last accessed: 11.10.2017).
[30] Deloitte: V*orstellung der Blockchain-Technologie, "Hallo, Welt!"*, https://www.bing.com/search?q=blockchain+zeugnis&PC=U316&FORM=CHROMN. (Last accessed: 21.07.2017).
[31] *Information about Showcase, Zeugnisvalidierung über Blockchains*, Innovation Lab at the Digitalgipfel 2017, Speyer 2017.
[32] *Academic Certificates on the Blockchain* (up to March 2017), https://digitalcurrency.unic.ac.cy/free-introductory-mooc/self-verifiable-certificates-on-the-bitcoin-blockchain/academic-certificates-on-the-blockchain/. (Last accessed: 21.07.2017).
[33] Plattform Industrie 4.0 (Ed.): Struktur der Verwaltungsschale – Fortentwicklung des Referenzmodells für die Industrie 4.0-Komponente.
[34] R. Heidel, F. Elmas: *Industrie 4.0 Basiswissen RAMI4.0*, Referenzarchitekturmodell mit Industrie 4.0-Komponente, Berlin, Vienna, Zurich, Beuth Verlag GmbH, VDE Verlag GmbH, 2017.

Acknowledgment

The authors would like to thank Mr. Czaske (PTB), Mr. Wolf (DAkkS) and Mr. Ulbig (PTB) for their interesting and active discussion and Mr. Czaske for his review of the manuscript.