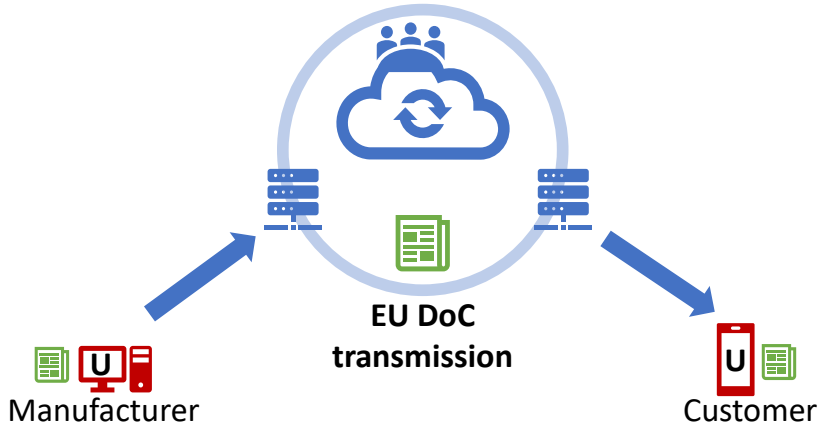
SmartCom

Guideline describing the concept of UniTerm and how to establish secure communication interfaces in legal metrology

- Exchange of a machine-readable EU Declaration of Conformity -

EN

UniTerm



DOI 10.5281/zenodo.5704676

DOI 10.5281/zenodo.5704676

DOI 10.5281/zenodo.5704676

Guideline describing the concept of UniTerm and how to establish secure communication interfaces in legal metrology

- Exchange of a machine-readable EU Declaration of Conformity -

Version 1.0

DOI 10.5281/zenodo.5704676

Editors

Aalto University, Finland:
T. Mustapää, J. Taponen

Tallinn University of Technology, Estonia:
O. Maennel

Physikalisch Technische Bundesanstalt, Germany:
D. Hutzschenreuter, W. Heeren, C. Brown, O. Baer

University of Cassino and Southern Lazio, Italy
G. Miele

Sartorius Lab Instruments
J. Haller

Mettler-Toledo
C. Müller-Schöll

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

Contact: smartcom@ptb.de

Braunschweig November 2021

DOI 10.5281/zenodo.5704676

Table of Contents

DOI 10.5281/zenodo.5704676

1 Introduction

Current legal requirements, concerning the technology supporting legal metrological activity, are governed, amongst others, by legal obligations of the manufacturer stated in EU regulations NAWID [1] and MID [2].

With the advent of IoT and Industry 4.0, legal metrology activity will in future operate within and over networks including intranets and internets. This in its turn provides for the possibility of connection to cloud-based computer services that can collect and analyse data relating to legal metrology. These services can also include remote access interfaces to the various legal metrology instruments offering the potential to calibrate and update devices without the need to physically "visit" the instrument.

An overview of the current requirements imposed by the standards bodies OIML and WELMEC has been provided in the SmartCom deliverable D4 "Document Specifying Rules for the Secure Use of DCC Covering Legal Aspects of Metrology" [3]. However, in their current state, the regulations provided by these institutions do not yet cover the case of legal instruments communicating over an intranet or internet in any general sense. The purpose of this document is to describe possible future technical solutions relating to how legal metrology activity can be implemented in general in a network and cloud services environment.

Specifically, this work will consider a limited interpretation of the EU Declaration of Conformity requirements for the formal acceptance of a new product (e.g. weighing scales) in the EU as a typical example of legal metrology information that needs to be communicated

DOI 10.5281/zenodo.5704676

safely and securely between relevant stakeholders involved in placing measurement instruments on the market.

DOI 10.5281/zenodo.5704676

2 Background

In the current section, the background information on the lifecycle of an instrument covered by legal metrology is provided. The focus is placed on the online conformity assessment phase, used in the current document as an example of digitization. The use of the XML language as a tool to generate machine-readable data is justified. Introduction to digital communication security is given to complete the background information.

2.1 Lifecycle of an instrument covered by Legal Metrology

Generally, the lifecycle of any instrument can be divided into four phases, which in its turn can consist of several steps necessary in a legal metrology lifecycle:

I. Development phase

- Implementation of legal requirements as URS (User Requirements Specification) and respective acceptance criteria
- Testing of developments against the requirements
- Documentation in User Acceptance Test reports

II. (Type) Approval phase

- Application for (type) approval
- Testing and assessing against legal requirements
- Documentation in test reports and (Type) Approval/Examination Certificates

DOI 10.5281/zenodo.5704676

III. Production phase

- Zero series testing against legal requirements and internal release of the product
- Testing of produced instruments against legal requirements (100 % and/or product audits)
- Conformity assessment of produced instruments
- Issuing of required documents (e.g. EU declaration of conformity)
- Affixing of required labels and markings (e.g. CE marking in the EU)

IV. Market phase

- Placing the instrument on the market
- Registration at verification authorities
- Verification/inspection (repeated)
- Repair and/or software update (repeated)
- Deregistration at verification authorities

There may be differences depending on the type of measuring instrument (water meter, electricity meter, weighing instrument, etc.) and on the region, where it is put on the market. Thus, the above list may contain steps that are not necessary in all cases and it may also be incomplete for other cases. Nevertheless, the main phases and steps within the lifecycle of such instruments can be considered the same.

It is strikingly obvious that for most (if not all) of these steps, similar information is transferred from one stakeholder to another. As a very simple example, a unique identifier of a particular instrument (usually the serial number) or a basic metrological parameter like the

DOI 10.5281/zenodo.5704676

verification scale interval *e* in the case of non-automatic weighing instruments, can be considered here. While the former exists “only” for the two last phases, the latter can be considered a parameter that is relevant (and transferred) throughout the complete lifecycle.

It can be assumed that relevant data exists in at least 4 different databases at the 4 main stakeholders of the above lifecycle – the manufacturer’s database of produced instruments, the database of approved/certified instrument/types at the respective authority/notified body, the database of verification and/or market surveillance authorities and the user’s database of his instruments. In current practice, it is likely that most (if not all) transfers from one database to another are done manually at least to some extent, which is a time-consuming and an error-prone process.

2.2 Data exchange via XML

Ever since the ability to network personal computers became a realistic possibility (in the 1980's), there has been the need to exchange information, typically computer files, between users working on separate computers. At this time, the ability to transfer files was limited by not only the brand of computer a user was using, but also what format the file had. In the 1980's, due to the cost of storage (RAM and disk), the format used to store information tended to be proprietary and binary (as the binary format was able to compress information into the smallest space). However, the chance of one computer being able to decode a proprietary binary file from another computer type was very small.

DOI 10.5281/zenodo.5704676

At the time, international text standards (e.g. ASCII) existed and were used by most computer manufacturers which made the possibility of being able to transfer text files more realistic. Around 1998, the first version of XML (Extensible Markup Language) [4], a text-based standard for encoding and storing information was released. Importantly the X in XML means eXtensible; which basically means XML can, combined with suitable definitions, store any form of information. Briefly, XML is a text-based markup language able to describe/define data. It can be used to store information of any kind in a text file. But text storage is not as memory efficient as binary storage. Eventually, as disk and computer memory became cheaper, XML-based storage became a realistic option for storing and communicating data/information. Today, XML-based information container technology is fundamental to storage, communications, security, and many other systems in modern computers.

XML is therefore the ideal container document for metrological information such as calibration and test data. It is also ideal for storing and communicating EU Conformity data. The ability to validate the contents of an XML file against a schema document, (which contains the definitions of the types of content the XML file can contain) provides a mechanism for checking that the contents conform to the specification.

2.3 Digital communication security

As the current format for the EU declaration of conformity has been a paper document or PDF file, there has not been one specific way for securing the documents to ensure data integrity, confidentiality and authenticity.

DOI 10.5281/zenodo.5704676

For formats such as XML, which have been in use for many years, there are already existing standards and technologies, such as digital signatures and encryption, to secure the information.

According to the EU, the term *electronic signature* is defined wider than the term *digital signature*, hence not all *electronic signatures* are legally binding. More details on these definitions are provided in section 4.5.

Compared to traditional handwritten signatures, digital signatures offer the possibility for the receiver to validate the origin of a file and ensure that its content has not been tampered with. The legal equivalence of digital signatures compared to handwritten signatures is dependent on regional and/or national laws and regulations, which means that these regulations may limit the use of specific signature formats.

If the information in a file is considered to be confidential, the file can be encrypted so that only the sender and the receiver can view the original information. The security solutions suitable for the digital EU DoC are discussed in more detail in section 4.

DOI 10.5281/zenodo.5704676

3 Example of a digitisable process – EU declaration of conformity (DoC)

From the different steps within the *lifecycle of an instrument* in legal metrology (see section 2.1), the EU Declaration of Conformity (EU DoC) is taken here as an example for digitisation. Within the "New Legislative Framework" of the European Union [5], the main purpose of the EU DoC is to document which Union harmonisation legislation applies to a particular instrument and who is responsible for compliance with the EU legislation requirements.

3.1 EU DoC – requirements and usage

The *EU DoC* must be drawn up and signed by the manufacturer (or his authorised representative) and must be kept for 10 years from the date of placing the product on the market. Once the EU DoC has been drawn up, the manufacturer must take over responsibility for the compliance of the object of the declaration (the instrument), with the requirements that are given within the Union harmonisation legislation (see below). Although this is formally not required, it is common practice to deliver the EU DoC to the end-user together with the concerned object of the declaration, usually as a printed hardcopy. It contains only basic information about the object of the declaration (see below) but can nevertheless be considered as some kind of "birth certificate". As such, it was taken as a good example for digitisation because it denotes the starting point of a particular instrument's

DOI 10.5281/zenodo.5704676

lifecycle and since it contains basic and relevant information about it.

The *requirements* on an EU DoC are given within the Union harmonisation legislation (usually EU directives) – for the example of a non-automatic weighing instrument, this would be the EU directive 2014/31/EU ("NAWID") [1]. According to Article 14 of this directive, the DoC must contain a statement that the fulfilment of certain essential requirements regarding the object of the declaration has been demonstrated. A detailed list of requirements, such as metrological requirements or requirements regarding the design and construction, is given in Annex I of the directive. Furthermore, the directive regulates the language in which the declaration shall be issued, the content depending on different modules of the conformity assessment procedure that are relevant to the object of the declaration (see [1], Annex II), as well as the structure of the directive (see [1], Annex IV):

EU DECLARATION OF CONFORMITY (No XXXX) (1)

1. *1. Instrument model/Instrument (product, type, batch or serial number);*
2. *Name and address of the manufacturer and, where applicable, his authorised representative;*
3. *This declaration of conformity is issued under the sole responsibility of the manufacturer;*
4. *Object of the declaration (identification of instrument allowing traceability; it may, where necessary for the identification of the instrument, include an image);*

DOI 10.5281/zenodo.5704676

5. *The object of the declaration described above is in conformity with the relevant Union harmonisation legislation;*
6. *References to the relevant harmonised standards used or references to the other technical specifications in relation to which conformity is declared;*
7. *The notified body … (name, number) performed … (description of intervention) and issued the certificate;*
8. *Additional information:*

   Signed for and on behalf of;

   (place and date of issue);

   (name, function) (signature).

In addition, the regulations of the directive ensure that even if the object of the declaration is subject to several Union acts, all respective identifications and publication references shall be drawn in a single EU declaration.

3.2 XML schema for the EU DoC

A digital transformation of processes and data anticipates the requirement to provide machine-readable interfaces for the exchange of all relevant information. The XML implementation for the EU DoC in SmartCom is describing an example for such an interface for non-automatic weighing instruments. A transition towards machine-readable formats has many benefits for users and manufacturers. Digitising the full analogue process leads to machine readable data and thereby obviates the need for manual transcription of data which is inherently error

DOI 10.5281/zenodo.5704676

prone. A further goal is to automate follow-on processes, such as digitisation of the conformity assessment process.

The purpose of this work is to demonstrate how in principle a legal metrology process can be operated in a networking environment. As such, the XML implementation presented here only uses a subset of the full data that would normally be needed for a universally applicable EU DoC format. The digitalisation example developed in this work is for the purposes of a proof of concept only. It is used to demonstrate metrological data transfer between the instrument's stakeholders and can be used only as a prototype for a real application. The example was developed according to the following three assumptions:

- It is based on a practical EU DoC example from the weighing industry.
- It addresses content that would be required by NAWID Annex IV [1] that needs to be machine-readable.
- Where appropriate, it reuses data elements from digital calibration certificates (DCCs) to increase the implementation value.

Figure 1 shows the basic XML structure of the EU DoC example. Element *doc:declarationOfConformity* defines the root element of this structure. The prefix "doc" shows all elements that belong to this structure. These are described in detail in the next sub-sections. For technical experts, an XML Schema Definition file (XSD) and a full XML example is made available, see Annex 8.

DOI 10.5281/zenodo.5704676

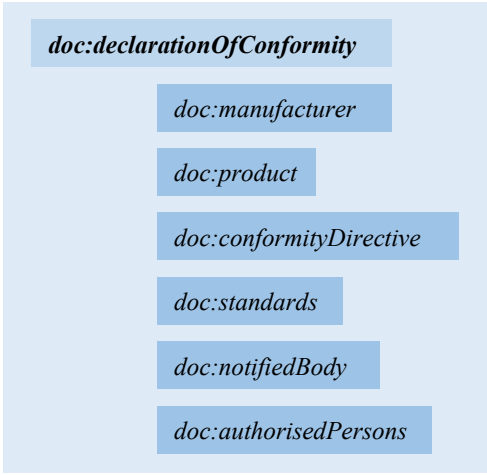


Figure 1 Basic structure of EU DoC XML schema.

3.2.1 Element *doc:manufacturer*

This element provides information on the manufacturer of the instrument for which the EU DoC is issued. It has the following data fields:

- ***doc:name***
  Name of the manufacturer company (mandatory). The name can be provided in various languages.

- ***doc:eMail***
  A contact e-mail address of the company (optional).

- ***doc:phone***
  A phone number to contact the company (optional)

- ***doc:fax***
  A fax number to contact the company (optional)

DOI 10.5281/zenodo.5704676

- ***doc:location***
  An address of the company (mandatory). The address provides sub-fields to provide the country, state, city, street, street number, post code, post office box code, and further information of the company.

3.2.2 Element *doc:product*

Element *doc:product* is used to provide information on the object of the declaration (the instrument). The following product information can be specified with this XML element:

- ***doc:name***
  This element should provide the type name of the object of the declaration (mandatory). The type name can be repeated in various languages. An example of such a type name would be 'Non-automatic weighing instrument' in the scope of the NAWID.

- ***doc:description***
  A text element that can be used to describe the object of the declaration (optional). The description can be provided in various languages.

- ***doc:model***
  Specification of the model of the object of the declaration (mandatory). In the case of a non-automatic weighing instrument, this should be identical to the information of the type examination certificate according to module B (if used) of NAWID.

- ***doc:identifications***
  A list of further identifications for the object of the declaration (mandatory). Identifications can be product, sub-type, batch and/or serial numbers. Each identification

DOI 10.5281/zenodo.5704676

must provide the issuer of the identification (e.g. manufacturer or customer), a value for identification (e.g. serial number) and it can have an optional description.

3.2.3 Element *doc:conformityDirective*

This element provides information on the European Union harmonisation legislation to which the issuer of the EU DoC declares conformity. NAWID is one example for such a legislation. In reality, an EU DoC can address numerous legislation documents. To realise this requirement, each legislation text identifier is enclosed in one statement element in the XML and the statements can be repeated as required. Alternatively, one XML file for each EU DoC under different legislations can be issued.

Each statement has the following fields:

- ***doc:reference***
  Identification of a legislation document. E.g. “2014/31/EU” for the NAWID. A comprehensive list of the existing legislation is available at [6].

- ***doc:declaration***
  A text element that can be used to provide information on the declaration. According to NAWID, mandatory declarations are
  - “This declaration of conformity is issued under the sole responsibility of the manufacturer.” and
  - “The object of the declaration described above is in conformity with the relevant Union harmonisation legislation”

  Declarations can be provided in various languages.

DOI 10.5281/zenodo.5704676

3.2.4 Element *doc:standards*

This element contains information on harmonised standards or other technical specifications which are used in relation to the declaration of conformity. The standards and specifications are provided by a list of statements. Each statement can have the following information:

- ***doc:norm***
  Identification of a harmonised standard or specification, e.g., for NAWID the "EN 45501:2015".

- ***doc:declaration***
  A text element that can be used to provide information on the standard or specification. The field can also be used by the issuer to make its own declarations on the conformity to standards. Declarations can be provided in various languages.

Note: *doc:conformityDirective* and *doc:standards* are based on the identical XML element *doc:statement*.

3.2.5 Element *doc:notifiedBody*

This element for the notified body allows the provision of various information on interventions, such as type examination or approval of the quality management system of the organisation that issues the EU DoC, by a notified body. The element can be repeated multiple times to allow for different notified bodies and interventions of these bodies. The following fields can be specified:

- ***doc:name***
  Name of the notified body and its Nando registered number (mandatory). E.g., "Physikalisch-Technische

DOI 10.5281/zenodo.5704676

Bundesanstalt (PTB KBS, 0102)". The name can be provided in various languages.

- ***doc:certificateNo***
  Number (respectively ID) of the certificate that was issued to the manufacturer by the notified body (mandatory).

- ***doc:description***
  A text element that can be used to describe the background of the certificate that was issued by the notified body and to describe interventions of that body (optional). In the case of the NAWID, important descriptions should address modules B and D as also described in the EU Blue Guide, paragraphs 5.1.7 and 5.1.8 [7]. Other modules are possible depending on the information given in the legislation. The description can be provided in various languages.

3.2.6 Element *doc:authorisedPersons*

This element provides information on the employees (respectively persons) who have been authorised by the manufacturer organisation to issue the EU DoC for the object of the declaration. One or more authorised persons can be specified. Each person is defined by a *doc:respPerson* element with the following fields:

- ***doc:person***
  Mandatory information includes name, e-mail, and address (location) of the responsible person. The data structure has the same format as *doc:manufacturer*. The address (location) is optional in the case that the location of the responsible person is the same as the location of the manufacturer.

DOI 10.5281/zenodo.5704676

- ***doc:description***
  A text element that can be used to describe the authorised person, e.g. “Head of the Laboratory” (optional). The description can be provided in various languages.

- ***doc:role***
  A text element for the role of the responsible person (optional). E.g., “authorised to compile the technical file” or “responsible for production”.

- ***doc:mainSigner***
  A Boolean field to identify whom from the authorised persons is responsible to sign the EU DoC.

DOI 10.5281/zenodo.5704676

4 Data security

Until now, legal metrology regulations from organisations OIML, WELMEC cover measuring instruments working in Local Area Network environments; see [3] for details. Now with the advent of IoT technology this activity will start to move towards communications over Wide Area Networks e.g., internets. There are many documented cases where unprotected communication of technical information over internets has resulted in catastrophic results, for example the attack on the Ukrainian electrical power supply in December 2015 [8]. It is very likely that metrological information will become a target for such attacks, and it is essential that security of this information is considered from the outset this work.

The main cryptographic functions discussed in this paper are based on public key cryptography. The idea behind public key cryptography is using cryptographic keys and specific algorithms for creating and validating digital signatures and encrypting files. The cryptographic keys can be symmetric or asymmetric but since digital signatures are based on using asymmetric keys, this paper focuses on the use of asymmetric key pairs.

An asymmetric key pair consists of a private key that is to be kept private and secure and a public key that could be publicly available, since it is, e.g., used to verify the signatures generated with the corresponding private key. The private and public key are mathematically connected to each other since they are created with specific mathematic algorithms that ensure that the key pair is unique [9].

DOI 10.5281/zenodo.5704676

4.1 Digital signatures and seals

A conventional signature whether electronic or not, is a basic function of communicating authority and trust [10]. Varying from a conventional signature, a digital one can be used to detect unauthorised modifications to the data or document [9].

For creating a digital signature, the Digital Signature Algorithm (DSA) standard specifies that the signature is generated from three discussed components or their products: a private key; hash function, and the ambiguous data or file that is to be signed [9].

A DSA is an algorithm specified in the Digital Signature Standard (DSS) [9]. The algorithm applies the concepts of hash algorithms and public-key cryptography or more commonly known as private-public key pairs.

A hash function is an algorithm that outputs a digest of the original data. This is a one-way algorithm, meaning the operation cannot be reversed. The algorithm is commonly used to check the integrity of the data since every document (depending on the algorithm implementation) has a different hashed value. One of the commonly used hash functions is the SHA-256 algorithm [11].

There are a variety of different algorithms for calculating a signature. For example, such modern algorithms include the Elliptic Curve Digital Signature Algorithm (ECDSA) and the Rivest-Shamir-Adleman (RSA) [9].

Likewise, the signature can be verified using the public key associated with the private key, the hash function used in the signature process, and the data or document that has been signed [9]. The verification operation can be seen as the reverse of the signing operation. Similar to the signature creation, the same hash function is used to compute the

DOI 10.5281/zenodo.5704676

hash of the document or file. In addition, the public key is used to obtain the hash of the original document from the digital signature. If any changes have been made in the original file, the hash of the file will have changed as well. If the hash values are the same, then the signature is valid.

4.2 Data encryption

While digital signatures can be used to ensure the non-repudiation of the data that is shared, they do not secure the confidentiality of the data. This can be solved using encryption. A file can be encrypted using the receiver's public key and a specific encryption algorithm. An encrypted file can only be decrypted with the private key of the receiver. If the sender knows the receiver, the encryption process is relatively simple as the public key can be exchanged relatively easily. If that is not the case, the sender needs to provide a private key to the receiver in a secure manner, which makes the process much more complicated.

4.3 Public key infrastructures

Public key infrastructures (PKI) are essential for an application relying on cryptography and provide a basis for many modern security-based solutions. A PKI signifies a chain of hierarchy consisting of Certificate Authorities (CA) and their issued public-key certificates [12]. These public-key certificates are used to signify the authority who owns the public key by conveying information about them [10].

The establishment of a PKI can be based on a mutual agreement of trust in a specific CA and the PKI in which it is included. For example, when two independent unknown

DOI 10.5281/zenodo.5704676

parties agree that they will trust a specific CA and if the other party has a valid and authentic digital certificate signed by the mutually trusted CA, they can trust each other [12].

A simple representation of a PKI consists of a root CA which is the highest authority of the infrastructure that issues certificates for intermediary CAs. An intermediary CA can issue certificates for lower level intermediary CAs or the end users which can be people, organisations or services.

Therefore, there can be multiple levels of intermediaries in this chain of trust. Each entity in this chain of trust usually has a Certificate Revocation List (CRL) or an address for an Online Certificate Protocol responder (OCSP) specified in the commonly used x.509 certificate's values. These can be used to revoke the certificate's validity. This process model is the basis for most common implementations of a hierarchical PKI. Importantly the PKI method described is easily and quickly scalable on the assumption that there is an existing hierarchy available already [12].

The most well-known PKI is in the modern internet's Transport Layer Security (TLS) which is based on x.509 certificates. In addition to other fields, TLS certificates specify the key usage explicitly [13]. Currently, the Root CAs for all important internet and computing technologies are shipped within most modern operating systems.

4.4 Cryptographic standards, primitives, and protocols (eIDAS)

Electronic identification and trust services (eIDAS) is an EU law that specifies requirements for digital signatures and transactions. The aim of the regulation is to specify secure conduct and interoperability for data in the European

DOI 10.5281/zenodo.5704676

Union. There are a variety of signature standards accepted as being eIDAS compliant for example XAdES which is the eIDAS compliant standard for XML signatures [3]. Producing eIDAS compliant digital signatures provides the capacity to render it legally binding in the EU if all requirements, in addition to the signature algorithms are met.

4.5 Legal frameworks

In this section, we are concerned with the digital signing of the EU declaration of conformity (EU DoC) as defined in EU Decision No 768/2008/EC. However, the same legal regulation applies to any other document that requires a signature. Within Europe eIDAS (electronic IDentification, Authentication and trust Services) is the legal framework described in EU Regulation 910/2014 as of 23 July 2014 [14]. This forms the basis for a digital signature to be accepted across the EU by public entities and companies offering public services.

With respect to this deliverable, the objective is to move to legally binding and digitally signed calibration certificates issued by a signature provider certified by the eIDAS. It should be noted that the EU defines the term *electronic signature* wider than *digital signature*, hence not all *electronic signatures* are legally binding. The EU explains, quote: “A digital signature, on the other hand, refers to a mathematical and cryptographic concept that is widely used to provide concrete and practical instances of electronic signature. The definition given by ETSI TR 119 100 is that of data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. These two concepts should be

DOI 10.5281/zenodo.5704676

distinguished, as all electronic signatures are not necessarily digital signatures [15]."

eIDAS defines three types of electronic signatures: Simple Electronic Signatures, Advanced Electronic Signatures (AdES), and Qualified Electronic Signatures (QES). Qualified Electronic Signatures are embedded into national law of the EU Member State, where the qualified trust service provider is established, and therefore form the appropriate basis for DCCs that needs to be valid within the European Union. From a legal perspective, a single digital signature can be valid for several documents as long as the signer takes the responsibility of the issued signature and is aware of what is being signed.

Nowadays declarations of conformity are issued automatically by the respective systems. This is often a scanned hand-written signature being inserted into the PDF. QES issues based on certificates from a Trust Service Provider (TSP) can be issued also at scale without human intervention and are legally equivalent to hand-written signatures.

From a wider viewpoint, beyond the EU legislation, it becomes more challenging, whether global service providers [16] are accepted as to provide legally binding signatures. This very much depends on the various jurisdictions and international agreements.

DOI 10.5281/zenodo.5704676

5 SmartCom UniTerm

To enable digital online conformity assessment, the UniTerm user interface was developed. In the current section, the goals and requirements on the metrological data transmission on the example of a web terminal, UniTerm, are discussed. Their implementation in the respective user interface using REST as well as *EU DoC service* of the partner project AnGeWaNt are presented. The AnGeWaNt platform, see section 5.2, allows for flexible implementation of software components communicating via REST. The developed *EU DoC Service* performs validation of the XML file with the instrument information against the EU DoC schema, being the core component of the presented online conformity assessment procedure.

5.1 Goals and requirements for data transmission

The workflow of online conformity assessment system consists of the following steps:

- Unified user interface installed on manufacturer device (UniTerm).
- Security concept for the transmission of metrological information outside the restricted environment.
- Data transmission using REST, a well-established architectural style using the HTTP protocol.
- Data storage and exchange using nodes.

DOI 10.5281/zenodo.5704676

- XML-based validation schema, including frameworks of the EU DoC.
- Unified user interface installed on customer device (UniTerm).

The main functionality of the UniTerm is summarised in Figure 2.

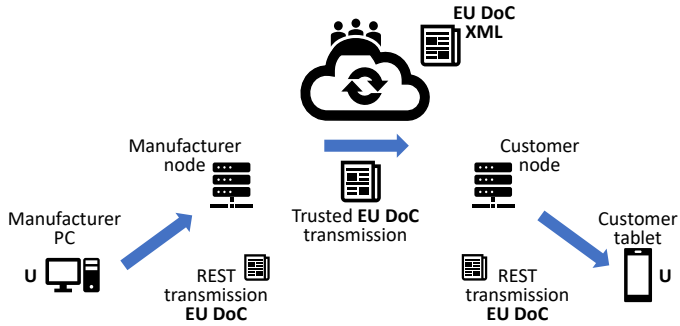


Figure 2 *Flowchart representing UniTerm functionality. Legend: EU DoC (European Declaration of Conformity); U (SmartCom UniTerm) - e.g. browser application for: viewing EU DoC, applying electronic signature to EU DoC and validating signature DoC.*

The above-described concept for online conformity assessment was implemented on the basis of the AnGeWaNt platform [17].

5.2 Platform architecture of AnGeWaNt

The architecture of the AnGeWaNt platform is designed and implemented according to a SOA (Service-oriented architecture) [18]. SOA is a software architecture model which classifies software components as services. Such services are designed as distinct units, stateless, loosely

DOI 10.5281/zenodo.5704676

coupled and can be combined flexibly. These units communicate via a REST protocol. As a central service hub, the platform offers access to all connected infrastructures and their provided services. Its modular approach allows for flexible implementation of new services, as it was realised for the *EU DoC Service* case. To increase flexibility and ease later expandability, the platform employs standardised and harmonised interfaces across all services [19]. The AnGeWaNt platform is written in Java with a relational database, while the vacuum laboratory is written in Clojure with a NoSQL persistence layer behind it.

5.3 REST protocol

Representational state transfer (REST) is a software architectural style that uses a subset of HTTP. It is commonly used to create interactive applications that use web services [20].

An application is said to be RESTful if it conforms to the following six architectural guidelines [21]:

- A client-server architecture consisting of clients, servers, and resources.
- A stateless client-server communication where session state information is stored at the client, not on the server.
- Cacheable data to eliminate client-server interactions.
- A uniform interface between components to transfer information in a standardised, rather than application-specific, form.
- A multilayer system, where client/server interactions are extended to hierarchical layers.

DOI 10.5281/zenodo.5704676

- Code-on-demand, which allows servers to extend a client's functionality by committing executable code.

SOAP is a common alternative to REST to access a web service. REST and SOAP are two different approaches to online data transfer. REST was developed more recently and is often considered the faster alternative in web-based scenarios. REST was implemented in the TraCim system [22] and is applied in the online conformity assessment system UniTerm.

5.4 UniTerm implementation

The SmatCom unified user interface, UniTerm, was developed to enable online conformity assessment for an end-user. In the user interface for UniTerm, the manufacturer fills in the form with the information on the object of the declaration, required for validation. In the next step, the XML file is generated in UniTerm and sent to AnGeWaNt's *DoC Service*. The transmission of metrological information is realised using the REST communication method.

The *EU DoC Service* validates the XML file with the instrument information against the EU DoC schema. Finally, both the manufacturer and the customer can access the certificate and XML file from the UniTerm interface.

DOI 10.5281/zenodo.5704676

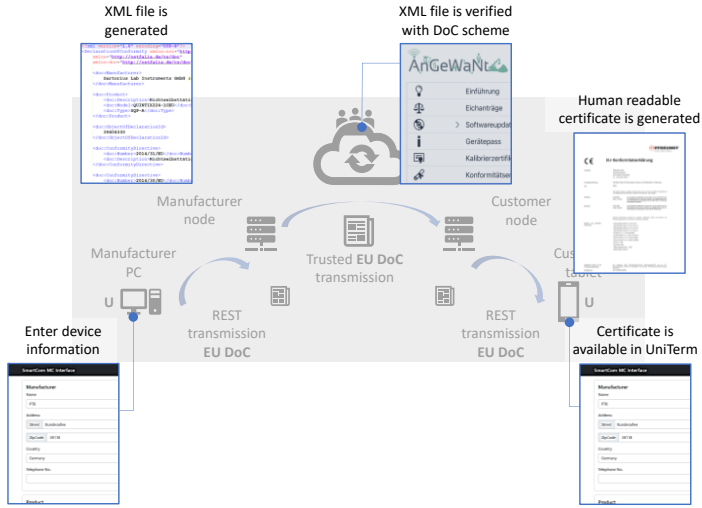


Figure 3 *UniTerm implementation*

Due to the flexibility of the developed *EU DoC Service*, the XSD file (XML schema definition) described above can be easily exchanged. This allows for fast adaption of the verification process to the legal requirements for the current use case of the non-automated weighing instruments as well as process adjustment for other instruments.

For the current demonstrator, for simplicity and time reasons, the security concept, described in Section 4, was not implemented. To implement it, the test environment should be set to test the UniTerm – *EU DoC Service* interaction. External certificate for validation of the security encryption should be used.

DOI 10.5281/zenodo.5704676

6 Summary

Before a product can be placed on the market within the EU, an EU Declaration of Conformity (EU DoC) needs to be produced by the manufacturer. This DoC can therefore be viewed as an example of how information is provided by one of the stakeholders within the life cycle of a device in legal metrology, where communication between several stakeholders is exchanged in several steps. One example for a possible future application is the exchange of data from the owner of the instrument to the weights and measures authorities. The purpose of this document thus has been to describe the concept for the solution of communicating this type of information in a safe and secure manner.

Following on from the earlier SmartCom work developing the Digital Calibration Certificate and Digital SI core outcomes from SmartCom, a technical solution framework for the communication of such legal documentation over networks has been developed. This solution uses XML as the core communication format and security based on a Public Key Infrastructure approach which is in common use throughout the internet and networking security industry.

The concept solution uses REST API technology to communicate with a cloud-based service to provide validation, safe storage and also the ability to connect with other legal metrology cloud-based services potentially at the national and or European level. A UniTerm interface has also been developed that allows the user to input required core data in a simple and easy to use manner.

Two practical demonstrators based on this core concept are discussed in detail in SmartCom deliverables D7 "Report on the validation of a demonstrator for the exchange of dimensional measurements in an end user application, with

DOI 10.5281/zenodo.5704676

a secure logistic data chain including DCCs" and D8 "Report on the validation of a demonstrator for the use of UniTerm in the legal weighing industry".

DOI 10.5281/zenodo.5704676

7 References

[1] European Commission, *Non-automatic weighing instruments (NAWI): Directive 2014/31/EU of the European Parliament and of the Council of 26 February 2014.* [Online]. Available: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/weighing-instruments_en (accessed: Jul. 8 2021).

[2] European Commission, *Measuring instruments (MID): Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014.* [Online]. Available: https://ec.europa.eu/growth/single-market/european-standards/harmonised-standards/measuring-instruments_en (accessed: Jun. 24 2021).

[3] P. Nikander, T. Elo, and T. Mustapää *et al.,* "Document specifying rules for the secure use of DCC covering legal aspects of metrology," in *Zenodo.* Accessed: Jun. 17 2021. [Online]. Available: 10.5281/zenodo.3664211

[4] W3C, *World Wide Web Consortium Extensible Markup Language (XML): W3C Recommendation 26 November 2008.* [Online]. Available: https://www.w3.org/TR/xml/ (accessed: Feb. 19 2021).

[5] European Commission, *New legislative framework.* [Online]. Available: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en (accessed: Jun. 17 2021).

[6] European Commission, *Legislations.* [Online]. Available: https://ec.europa.eu/growth/tools-databases/nando/index.cfm?fuseaction=directive.main (accessed: Jun. 17 2021).

[7] Official Journal of the European Union, *Commission Notice. The 'Blue Guide' on the implementation of EU products rules 2016.* [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016XC0726%2802%29 (accessed: Jul. 8 2021).

DOI 10.5281/zenodo.5704676

[8] K. Zetter., *Inside the Cunning, Unprecendented Hack of Ukraine's Power Grid.* [Online]. Available: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed: Jul. 22 2021).

[9] C. F. Kerry and P. D. Gallagher, *Digital Signature Standard (DSS).* [Online]. Available: https://csrc.nist.gov/publications/detail/fips/186/4/final (accessed: Jul. 8 2021).

[10] Imai H. and Zheng Y., Eds., *Certifying trust: Public Key Cryptography*. Springer Berlin Heidelberg, 1998.

[11] P. Pritzker and W. E. May, *Secure Hash Standard (SHS): National Institute of Standards and Technology.* [Online]. Available: https://csrc.nist.gov/publications/detail/fips/180/4/final (accessed: Jul. 8 2021).

[12] J. Weise, *Public Key Infrastructure Overview.* [Online]. Available: http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf (accessed: Jul. 8 2021).

[13] E. Rescorla, *The Transport Layer Security (TLS) Protocol Version 1.3.* [Online]. Available: https://tools.ietf.org/html/rfc8446 (accessed: Jul. 8 2021).

[14] Official Journal of the European Union, *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.* [Online]. Available: https://eur-lex.europa.eu/eli/reg/2014/910/oj (accessed: Jun. 17 2021).

[15] CEF Digital, *eSignature Overview.* [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/eSignature+Overview (accessed: Jul. 8 2021).

[16] GlobalSign by GMO, *Introducing GlobalSign Digital Signing Service by GMO.* [Online]. Available: https://www.globalsign.com/en/digital-signatures (accessed: Jun. 17 2021).

[17] A. Oppermann, S. Eickelberg, and J. Exner, "Toward Digital Transformation of Processes in Legal Metrology for Weighing Instruments: 15th Conference on

Computer Science and Information Systems (FedCSIS)," in pp. 559–562.

[18] M. Dohlus, M. Nischwitz, A. Yurchenko, R. Meyer, J. Wetzlich, and F. Thiel, "Designing the European Metrology Cloud," *OIML Bulletin*M., vol. 61, no. 1, pp. 8–17, 2020.

[19] A. Oppermann, S. Eickelberg, and J. Exner, Eds., *Digital transformation in legal metrology: An approach to a distributed architecture for consolidating metrological services and data*: Springer International Publishing, 2021.

[20] R. T. Fielding, *Architectural Styles and the Design of Network-based Software Architectures: PhD Thesis*. University of Califonia, Irvine, 2000. Accessed: Apr. 27 2021. [Online]. Available: https://www.ics.uci.edu/~fielding/pubs/dissertation/top.htm

[21] Red Hat, *Integration. REST or SOAP?* [Online]. Available: https://www.redhat.com/de/topics/integration/whats-the-difference-between-soap-rest (accessed: Jun. 2021).

[22] *TraCIM.* [Online]. Available: https://www.ptb.de/emrp/tcim.html (accessed: Feb. 19 2021).

DOI 10.5281/zenodo.5704676

8 Annex: XML Implementation of the EU DoC example

8.1 XML Example

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<doc:declarationOfConformity
  xmlns:doc="http://smartcom.eu/ns/doc"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <doc:manufacturer>
    <doc:name>
      <doc:content>Sartorius Lab Instruments GmbH &amp;amp; Co.
        KG</doc:content>
    </doc:name>
    <doc:eMail>metrology@sartorius.com</doc:eMail>
    <doc:location>
      <doc:street>Otto-Brenner-Strasse</doc:street>
      <doc:streetNo>20</doc:streetNo>
      <doc:postCode>37079</doc:postCode>
      <doc:city>Goettingen</doc:city>
      <doc:countryCode>DE</doc:countryCode>
    </doc:location>
  </doc:manufacturer>

  <doc:product>
    <doc:name>
      <doc:content lang="en">Non-automatic weighing
          instrument</doc:content>
    </doc:name>
    <doc:description>
      <doc:content lang="en">Non-automatic electromechanical
        weighing instrument without lever system
      </doc:content>
    </doc:description>
    <doc:model>model xyz</doc:model>
    <doc:identifications>
      <doc:identification>
        <doc:issuer>manufacturer</doc:issuer>
        <doc:value>0012345678</doc:value>
          <doc:description>
            <doc:content lang="en">Serial No.</doc:content>
          </doc:description>
```

DOI 10.5281/zenodo.5704676

```
    </doc:identification>
  </doc:identifications>
</doc:product>

<doc:conformityDirective>
  <doc:statement>
    <doc:declaration>
      <doc:content lang="en">This declaration of
        conformity is issued under the sole
        responsibility of the manufacturer.”</doc:content>
     </doc:declaration>
  </doc:statement>
  <doc:statement>
    <doc:declaration>
      <doc:content lang="en">The object of the
          declaration described above is in conformity
          with the relevant Union harmonisation
          legislation</doc:content>
    </doc:declaration>
  </doc:statement>
  <doc:statement>
    <doc:reference>2014/31/EU (ELI:http://data.europa
          .eu/eli/dir/2014/31/oj)</doc:reference>
    <doc:declaration>
      <doc:content lang="en">Non-automatic weighing
            instruments</doc:content>
    </doc:declaration>
  </doc:statement>
  <!-- Additional statements can be added to provide
    further legislation documents -->
</doc:conformityDirective>

<doc:standard>
  <doc:statement>
    <doc:declaration>
      <doc:content lang="en">Products manufactured in
        compliance with harmonised standards benefit from
        a presumption of conformity with the corresponding
        essential requirements of the applicable
        legislation.doc:content>
    </doc:declaration>
  </doc:statement>
  <doc:statement>
    <doc:declaration>
      <doc:content lang="en">The product is manufactured
        in compliance with the following harmonised
        standards.doc:content>
    </doc:declaration>
```

DOI 10.5281/zenodo.5704676

```
    </doc:statement>

    <doc:statement>
      <doc:norm>EN 45501:2015</doc:norm>
    </doc:statement>
    <!-- Additional statements can be added to provide
      further standards -->
  </doc:standard>


  <doc:notifiedBody>
    <doc:name>
      <doc:content>Physikalisch-Technische Bundesanstalt(PTB
        KBS, 0102)</doc:content>
    </doc:name>
    <doc:certificateNo>DE-18-NAWID-PTB013
      </doc:certificateNo>
    <doc:description>
      <doc:content lang="en">The notified body mentioned
        above performed a type examination and issued the EU
        Type Examination Certificate with the here given
        certificate number. NAWID Module B.</doc:content>
    </doc:description>
  </doc:notifiedBody>

  <doc:notifiedBody>
    <doc:name>
      <doc:content>Physikalisch-Technische Bundesanstalt(PTB
        KBS, 0102)</doc:content>
    </doc:name>
    <doc:certificateNo>DE-M-AQ-PTB158</doc:certificateNo>
    <doc:description>
      <doc:content lang="en">The notified body mentioned
        above recognized the quality management system of
        the manufacturer and issued the approval certificate
        for the quality management system with the here
        given certificate. NAWID Module D.</doc:content>
    </doc:description>
  </doc:notifiedBody>


  <doc:authorisedPersons>
    <doc:respPerson>
      <doc:person>
        <doc:name>
          <doc:content>Dr. M. Mustermann</doc:content>
        </doc:name>
        <doc:eMail>mustermann@company.de</doc:eMail>
```

DOI 10.5281/zenodo.5704676

```
      </doc:person>
      <doc:description>
        <doc:content lang="en">Head of International
          Certification Management</doc:content>
      </doc:description>
      <doc:role>Person authorised to compile the technical
        file</doc:role>
      <doc:mainSigner>true</doc:mainSigner>
    </doc:respPerson>
    <doc:respPerson>
      <doc:person>
        <doc:name>
          <doc:content>Lieschen Mueller</doc:content>
        </doc:name>
        <doc:eMail>Mueller@company.de</doc:eMail>
      </doc:person>
      <doc:description>
        <doc:content lang="en">Head of the Production
          Department</doc:content>
      </doc:description>
      <doc:role>Responsible for the production</doc:role>
      <doc:mainSigner>false</doc:mainSigner>
    </doc:respPerson>
  </doc:authorisedPersons>
  </doc:declarationOfConformity>
```

8.2 XML Scheme Definition (XSD)

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<xs:schema xmlns:xs=http://www.w3.org/2001/XMLSchema
        xmlns:doc=http://smartcom.eu/ns/doc
        targetNamespace="http://smartcom.eu/ns/doc"
        elementFormDefault="qualified">
  <xs:annotation>
    <xs:documentation>This XSD contains data elements form
        the XML DCC (https://www.ptb.de/dcc). Modifications
        of the original elements were made and declared in
        the XSD in an appropriate form.</xs:documentation>
  </xs:annotation>

  <xs:element name="declarationOfConformity">
    <xs:complexType>
      <xs:sequence>

<!-- 1. Manufacturer of instrument (use of DCC contactType)
-->
```

DOI 10.5281/zenodo.5704676

```
<xs:element name="manufacturer" type="doc:contactType"/>

<!-- 2. Product (item) subject to declaration (adoption of
dcc:item without manufacturer, equipmentClass and
descriptionData) -->
<xs:element name="product">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="name" type="doc:textType"/>
      <xs:element name="description" type="doc:textType"
        minOccurs="0"/>
      <xs:element name="model" type="xs:string"
        minOccurs="0"/>
      <xs:element name="identifications"
        type="doc:identificationListType"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- 3. Underlying conformity directives (based on
dcc:statement) -->
<xs:element name="conformityDirective"
  maxOccurs="unbounded" >
  <xs:complexType>
    <xs:sequence>
      <xs:element name="statement"
        type="doc:statementMetaDataType"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- 4. Underlying standards for conformity (based on
dcc:statement) -->
<xs:element name="standard" maxOccurs="unbounded">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="statement"
        type="doc:statementMetaDataType"
        maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- 5. Notified body where description element allows to
define the actions. -->
<xs:element name="notifiedBody" maxOccurs="unbounded">
  <xs:complexType>
```

DOI 10.5281/zenodo.5704676

```
    <xs:sequence>
      <xs:element name="name" type="doc:textType" />
      <xs:element name="certificateNo" type="xs:string" />
      <xs:element name="description" type="doc:textType"
        minOccurs="0"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

<!-- 6. Authorized persons from the manufacturer
organization (based on dcc:respPerson) -->
<xs:element name="authorisedPersons">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="respPerson"
        type="doc:respPersonType" maxOccurs="unbounded"/>
    </xs:sequence>
   </xs:complexType>
  </xs:element>
 </xs:sequence>
</xs:complexType>
</xs:element>

<!-- complex types adopted from DCC (without ID attributes)
-->
<xs:simpleType name="stringISO639Type">
  <xs:restriction base="xs:string">
    <xs:pattern value="[a-z]{2}"/>
  </xs:restriction>
</xs:simpleType>
<xs:simpleType name="stringISO3166Type">
  <xs:restriction base="xs:string">
    <xs:pattern value="[A-Z]{2}"/>
  </xs:restriction>
</xs:simpleType>
<xs:complexType name="stringWithLangType">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="lang" type="doc:stringISO639Type"
        use="optional"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="textType">
  <xs:sequence>
    <xs:element name="content" type="doc:stringWithLangType"
      maxOccurs="unbounded"/>
```

DOI 10.5281/zenodo.5704676

```
  </xs:sequence>
</xs:complexType>
<!-- modification compatible with dcc definition:
descriptionData element removed -->
<xs:complexType name="contactType">
  <xs:sequence>
    <xs:element name="name" type="doc:textType"/>
    <xs:element name="eMail" type="xs:string"
      minOccurs="0"/>
    <xs:element name="phone" type="xs:string"
      minOccurs="0"/>
    <xs:element name="fax" type="xs:string" minOccurs="0"/>
    <xs:element name="location" type="doc:locationType"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="locationType">
  <xs:choice maxOccurs="unbounded">
    <xs:element name="city" type="xs:string"/>
    <xs:element name="countryCode"
      type="doc:stringISO3166Type"/>
    <xs:element name="postCode" type="xs:string"/>
    <xs:element name="postOfficeBox" type="xs:string"/>
    <xs:element name="state" type="xs:string"/>
    <xs:element name="street" type="xs:string"/>
    <xs:element name="streetNo" type="xs:string"/>
    <xs:element name="further" type="doc:textType"/>
  </xs:choice>
</xs:complexType>
<xs:complexType name="identificationListType">
  <xs:sequence>
    <xs:element name="identification"
      type="doc:identificationType" maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="identificationType">
  <xs:sequence>
    <xs:element name="issuer">
      <xs:simpleType>
        <xs:restriction base="xs:string">
          <xs:enumeration value="manufacturer"/>
          <xs:enumeration value="calibrationLaboratory"/>
          <xs:enumeration value="customer"/>
          <xs:enumeration value="owner"/>
          <xs:enumeration value="other"/>
        </xs:restriction>
      </xs:simpleType>
    </xs:element>
    <xs:element name="value" type="xs:string"/>
```

DOI 10.5281/zenodo.5704676

```
    <xs:element name="description" type="doc:textType"
      minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<!-- modification: only used norm, reference and declaration
element from dcc type -->
<xs:complexType name="statementMetaDataType">
  <xs:sequence>
    <xs:element name="norm" type="xs:string" minOccurs="0"/>
    <xs:element name="reference" type="xs:string"
      minOccurs="0"/>
    <xs:element name="declaration" type="doc:textType"
      minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<xs:complexType name="respPersonType">
  <xs:sequence>
    <xs:element name="person"
      type="doc:contactNotStrictType"/>
     <xs:element name="description" type="doc:textType"
       minOccurs="0"/>
     <xs:element name="role" type="xs:string"
       minOccurs="0"/>
     <xs:element name="mainSigner" type="xs:boolean"
       minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
<!-- modification of dcc element: removed
descriptionData -->
<xs:complexType name="contactNotStrictType">
  <xs:sequence>
    <xs:element name="name" type="doc:textType"/>
    <xs:element name="eMail" type="xs:string"
      minOccurs="0"/>
    <xs:element name="phone" type="xs:string"
      minOccurs="0"/>
    <xs:element name="fax" type="xs:string" minOccurs="0"/>
    <xs:element name="location" type="doc:locationType"
      minOccurs="0"/>
  </xs:sequence>
</xs:complexType>
</xs:schema>
```

DOI 10.5281/zenodo.5704676

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.5704676