DOI 10.5162/sensoren2016/P7.5

Distributed Metrological Sensors managed by a secure Cloud-Infrastructure

Alexander Oppermann[1], Dr. habil. Florian Thiel[1]
[1]Physikalisch-Technische Bundesanstalt (PTB), Fachbereich 8.5 „Metrologische Informationstechnik“,
Abbestr. 2-12, 10587 Berlin, Deutschland
Alexander.Oppermann@ptb.de, Florian.Thiel@ptb.de

Abstract

In recent years Cloud Computing has seen a lot of improvement in terms of security, stability and maturity thus it should be able to meet the demands and requirements of critical infrastructures and well-regulated areas. This paper focuses on a secure and modular approach for a cloud infrastructure that conforms to the Measuring Instrument Directive of the European Union while preserving the advantages and benefits of cloud computing for corporations and consumers. The legitimate, secure and protected flow of measurement data are key challenges of this work by utilizing homomorphic encryption the authors respond to these challenges and counter the main attack vectors of cloud computing at the same time.

Keywords: Cloud Computing, Trusted Cloud, Internet of Things, Homomorphic Encryption, Legal Metrology

Introduction

In recent years Cloud Computing has seen a lot of improvement in terms of security, stability and maturity. Nowadays one can raise the research question if cloud computing is mature enough to meet the demands and requirements of critical infrastructures and well-regulated areas. According to Gartner [10], Cloud Computing technology is now in the stage of trough of disillusionment and thus becoming more interesting for companies to be considered for profitable industrial appliances.

For this reason there are demanding approaches from manufacturers who want to utilize cloud computing for their business concepts in the area of legal metrology. They want to take advantage of a virtualized and easy scalable infrastructure, in order to store data externally or, e.g. externalize complete software processes and to put them into the cloud (For more information refer to the section Research Scenarios). Through virtualization and externalization measuring instruments and sensors will be reduced in cost as well as in size. In the near future only rudimentary sensors will be common with a tiny processing and communication unit that will provide easy access to an open network, e.g. the Internet (cf. [1]).

All measurement devices in Europe are subject to legal control and have to pass a conformity assessment by a notified body, in order to assure that they meet the essential requirements of the Measuring Instrument Directive 2014/32/EU (MID) [2]. Additionally to this directive other documents like the WELMEC “Software” guide [3] or the OIML guide [4] which help to support this process by offering technical guidance to implement the essential requirements. The development of new standards, validation and recommendations for cloud computing will be part of further research and will in return enhance the guidance documents (cf. [1]).

This development will have a big impact on all market participants, i.e. the manufacturer, the user, the end-user, notified bodies and market surveillance. Subsequently the new role and duties of the Cloud Service Provider, as well as the legal impact, have to be determined.

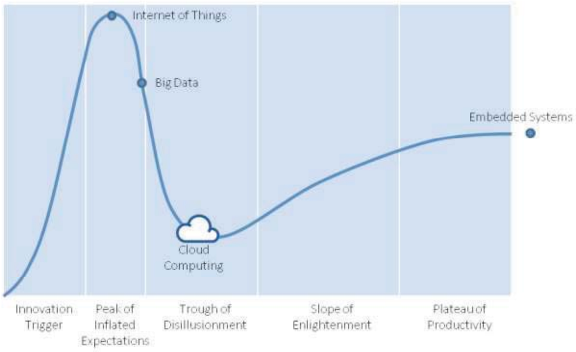

Figure 1: Gartners Hype Cycle from 2014 [10]. Embedded Systems already left the chart.

The remainder of this paper is structured as follows: Section *Legal Metrology* outlines how this field is organized; Section *Secure Cloud Infrastructure* gives a brief outlook of a secure cloud architecture and describes homomorphic encryption; Section *Research Scenarios* explains the use cases and its benefits for legal metrology.

Legal Metrology

The main motivation of legal metrology is the assurance of correct measurements and the preservation of public trust in them. Furthermore, legal metrology plays a key role in order to guarantee the operation of the economic system while protecting the customer simultaneously.

The scope of legal relevant measuring instruments comprises commercial, administrative purposes and public interest. In Germany over 100 million legally relevant meters are in use (c.f. [11]). The large majority of these are deployed as commodity meters for water, gas, electricity or heat. Aside from these operational areas legal relevant applications are scales, e.g. in supermarkets, petrol pumps and the traffic control with its meters for alcohol and speed.

The main issue of all these measuring instruments is that neither the user nor the affected person can verify the measurement result without depending on the accuracy and official calibration of these measuring instruments.

The *International Organization of Legal Metrology* (OIML) intents to harmonize regulations transnational worldwide and to decrease trade barriers due to legal requirements. The software requirements for legal measuring instruments are addressed in the document OIML D 31 (cf. [4],[12]).

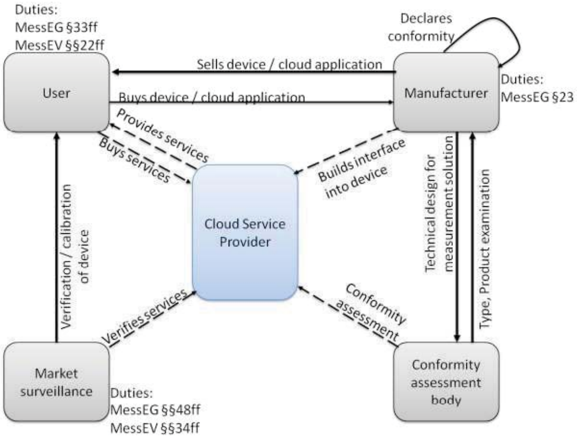

Figure 2: Overview of the different actors their roles, schedule of responsibilities and duties in legal metrology. The cloud service provider role has to be determined.

On the European level the European committee also known as WELMEC will harmonize the regulations for legal metrology. Notified Bodies (private or public departments to validate measuring instruments) within Europe and manufacturers that implement the Measuring Instrument Directive (MID) are being supported by the committee and their published guides [12].

Cloud Service Provider

In legal metrology are four main roles (Conformity assessment body, manufacturer, user, market surveillance) established (see Figure 2). Through Cloud Computing there will be an additional role introduced, which is not yet clearly defined with its duties and its relationships to the other market participants. The requirements and guidelines for a Cloud Service Provider in the field of legal metrology have to be determined in order to comply with the legal demands. This will be part of the future work. There are four conceivable scenarios for the Cloud Service Provider: The manufacturer can host the cloud services in house (i.e. on-premise-solution); the user implements the on-premise-solution; either the manufacturer or the user has a subcontractor which provides the cloud service functionality (i.e. off-premise solution).

Measuring Instrument Directive

The establishments of common European Standards for measuring instruments are the goal of the European directive (2014/32/EU, [2]) better known as the Measuring Instrument Directive (MID). To enable fair trade, trust in public interest and to protect the consumer are further objectives of the MID.

The MID comprises ten types of measuring instruments that are of special interest and importance to the economy due to their widespread or cross-border use. These are: water meters, gas meters and volume conversion devices, active electrical energy meters, heat meters, measuring systems for the continuous and dynamic measurement of quantities of liquids other than water, automatic weighing instruments, taximeters, material measures, dimensional measuring instruments, and exhaust gas analyzers. In the annex of the directive there are definitions, fault tolerances and specific requirements outlined for each type of the prior mentioned measurement instruments. The specific requirements involve, e.g. basic tamper protection and a display for measurement data [2].

If the manufacturer wants to put a new measuring instrument on the market, he has to declare the conformity with the MID based on the assessment by a Notified Body in Europe (cf. Figure 2). The *Physikalisch-Technische Bundesanstalt* (PTB) is a Notified Body in Germany and also the German national metrology institute that acts as an interface between scientific research and economic interests. Additional areas of activities are gaining technical expertise related to measuring instruments, conformity assessment, monitoring of product related quality assurance systems and advising with European regulations.

WELMEC

WELMEC is a body, which consists of the European Free Trade Association (EFTA) and national authorities responsible for legal metrology, like the PTB. The WELMEC Committee contains members from 37 countries and has eight WELMEC Working Groups (WG) with WG7 responsible for software matters as well as publishing the WELMEC 7.2 *Software Guide*. The current version is WELMEC 7.2 Issue 6 and was released this year. It includes additionally a guideline for manufacturers to implement a risk analysis for their measuring instruments.

The WELMEC 7.2 Software Guide provides a comprehensive view of software security with particular regard to measuring instruments. Achieving software security in conjunction with compliance of the software related part demanded by the MID is the main goal of the guide, if followed. The numerous examples and rules of the guide ease that process for Notified Bodies and manufacturers.

Segregation of legally relevant and legally non-relevant software segments is highly recommended when planning software modules for secure measuring instruments. The main challenge is that the legally relevant part may not be affected by the legally non-relevant part. Protected interfaces help to assure that unwanted interchange of information is prevented. The modularization of software will simplify and speed up the update routine as well as the process for manufacturer and Notified Bodies alike. WELMEC 7.2 Software Guide designates legally relevant modules through contributions to or influence on measurement data. Examples include displaying data, protecting data, saving data, identifying the software, executing downloads, transferring data, and checking of received or stored data (see [3]).

Secure Cloud Infrastructure

In this work an external cloud service provider is assumed, i.e. a third party, off-premise solution, and three research scenarios are being developed, i.e. externalization of storage, externalization of processing and complete virtualization of a measurement device, in order to test the feasibility of cloud computing in conjunction with regulated area like legal metrology.

A reference architecture is developed and suggested, which enforces security by separation through the use of virtualization and containers. Peters [5] already proved a design concept for embedded systems by using a separation kernel and virtualized compartments to ensure the usual software security requirements for general purpose operating systems [6], [7]. This design concept facilitates software updates and patches without the need of going through the process of recertification and subsequently reduces costs for manufacturers and others alike.

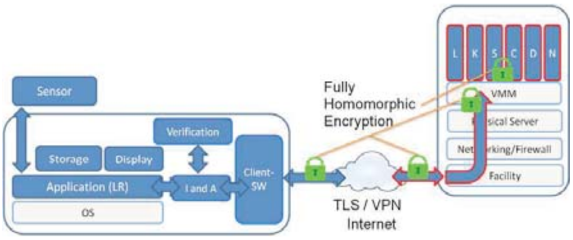

Figure 3: Legal Cloud Framework: Measurement Device and Cloud Architecture secured via TLS and homomorphic encryption. L: Legally relevant VM, K: Key & Signature Manager, S: Storage Manager, C: Connection Manager, D: Download Manager, N: legally non-relevant VM

One aspect of this work is to determine the modalities for contract design between manufacturers, cloud service provider and user. Until today there is lack of understanding how the responsibilities are handled and regulated between these partners.

Cloud Computing solutions accumulate and concentrate always large amounts of data and therefore generate attention and demand for legal and illegal data access. The robustness, redundancy and high-availability are the main focus when designing a secure cloud infrastructure. Of further importance is the constant match of the real world with the deduced threat model. This leads to latest security requirements for the cloud architecture.

Furthermore new approaches are investigated which will solve two main threats in cloud computing (refer to Figure 8, R1 and R8) and thus increases trust in these complex technologies. Firstly, to avoid an insider attack

DOI 10.5162/sensoren2016/P7.5

by an illicit system administrator. A benevolent system administrator role is unprovided for legal metrology and consequently everyone has to be distrusted initially. Data integrity, data security and data privacy can be hardly provided with classical approaches, if the cloud service provider is considered untrustworthy. From a security viewpoint, this leads to an exceptionally interesting challenge.
Secondly, to ensure that an unallowed communication between two virtual machines (VM) is impossible and to secure the processing within a VM (see Figure8, R1). This will enhance the security in case of a malicious VM in the cloud, which tries to overcome data restriction policies.
In order to tackle these two pressing issues and therewith guarantee privacy and integrity of measurement data, the possibility of using cloud applications, which take advantage of fully homomorphic encryption (FHE) [8] will be elaborated. Chechulina et al. [9] proposed a promising approach and used FHE successfully to execute secure database operations on encrypted data.

Homomorphic Encryption

Rivest, Adleman and Dertouzos invented the crypto system RSA [13] and described the possibility of homomorphic encryption [14] in 1978. The distinctive feature about homomorphic encryption is that it enables mathematical operations on already encrypted data without decrypting it first. In 2009 Gentry were able to prove that a crypto system exists which holds both properties that are addition and multiplication. The first fully homomorphic crypto system based on ideal lattices [15] was presented to the world. One year later Gentry constructed a fully homomorphic scheme from a “bootstrappable” somewhat homomorphic scheme (c.f. [16]) by using only modular arithmetic.

Categories of homomorphic schemes

Homomorphic schemes are very different and thus do not always share the same properties. Armknecht et al. [17] identified attributes (correctness for decryption and evaluation, compactness) of homomorphic schemes that enable a correct classification of the miscellaneous schemes. They determined that a scheme is composed of four steps that are generation of keys (Gen), encryption (Enc), evaluation of the cipher text (Eval) and decryption (Dec).
Armknecht et. al defined three classifications, but for this work are only the principal two important to be mentioned:

A *Somewhat Homomorphic scheme* δ (Gen, Enc, Eval, Dec) features correct decryption and correct evaluation. No rule exists for compactness. With each homomorphic operation the cipher text can grow in length.

A *Fully Homomorphic scheme* δ (Gen, Enc, Eval, Dec) features compactness, correctness and the scheme itself is a set of all circuits. This implies that the scheme can evaluate any given circuit regardless of the size.

Utilizing fully homomorphic encryption

Using fully homomorphic encryption within the measuring instrument increases data security and integrity for the transportation and the processing of measurement data in the cloud (see Figure 3).
The principal attack vectors (compare Figure 8, especially R1+R8) will be decreased immensely by implementing homomorphic encryption algorithm that performs operations on encrypted data. Data cannot be changed without difficulty and a lot of effort by a malicious insider, nor is spying of processed data possible by an infected or corrupted VM. While reducing the most important endangerments for utilizing cloud computing in a well-regulated area, another goal is achieved that is to nullify innovation hindrances by avoiding special requirements for measuring instruments that employ cloud computing. Moreover, cloud service providers have no need to deploy special hardware for their servers in order to satisfy particular security demands and facilitate trust in cloud computing platforms.

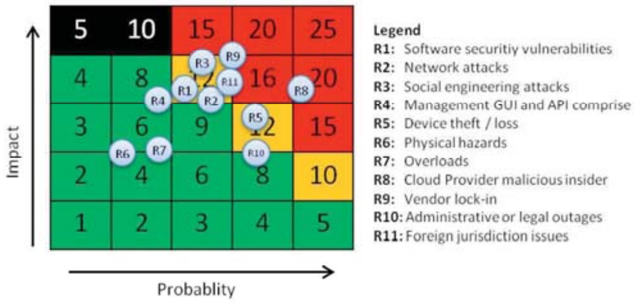

Figure 4: ENISA Risk Analysis Cloud Computing from [21], with additional information of R8 malicious insider [22]

- 🟩 Minor Impact
- 🟨 Signifcant Impact
- 🟥 Major Impact
- ⬛ High Imact, low probability

Challenges with fully homomorphic encryption

The vast majority of homomorphic encryption schemes exist only theoretically [17] on paper instead of as implementations. A huge challenge is still the rather long computation time for most systems. Elaborating, testing and evaluating existing implementations like HElib, FHEW, HomomorphicEncryption R Package [18] and NTRU based implementation (cf. [19]) will be part of the future work.

Research Secenarios

This chapter gives an overview of the research scenarios and use cases which are created to outline the long term goal of a fully virtualized measuring instrument that meets the legal and software-security requirements for measuring instruments. The scenarios are derived from industry demands and reflect the current need for - above all legally conform - cloud computing solutions.

Fully Virtualized Measuring Instrument

This use case scenario objective is to have only a physical senor and a module for data acquisition and communication left in the field with the rest of the measuring instrument transferred to the cloud. To guarantee data integrity and security the communication module has to cryptographically sign the data before sending them off to the cloud.

In the cloud each module will be separated in different virtualized compartments to avoid wanted or unwanted manipulation of the virtual machines among themselves, e.g. processing and storage for measurement data are separated. Further services legally relevant or not are also detached from the rest. In case of a manipulation a virtual machine can be shutdown rapidly and replaced by a new one without losing a lot of time in maintenance and downtime. As in Figure 4 indicated the display is detached from the measuring instrument. Hence, the display will be implemented as a software service so that market participants are able to access measurement data from their favorite device. Achieving conformity with the MID is very challenging at the moment but with regard of cost efficiency this scenario is the most promising one.

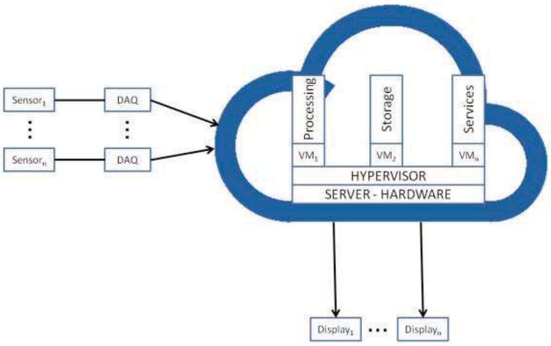

Figure 5: Research Scenario: Fully virtualized measuring instrument with everything moved to the cloud except the physical sensor, data acquisition and communication module.

Measuring Data Export

In contrast to the prior use case the measuring instrument is fully implemented in hardware and can be sealed and verified as a calibrated measuring instrument, which is in accordance with the German Verification Act (Mess- und Eichgesetz/Mess- und Eichverordnung (MessEG/EV)).

As indicated in Figure 5 the real world data will be acquired by the sensor and then passed on to the measuring instrument where the data is processed and the result is determined. The measurement data will be cryptographically signed before sent to the cloud storage. The measuring data is now accessible by authorized market participant and can be retrieved through a secure software based display service. The displayed data can be verified by the initially created cryptographically secured hashes. The signed data is an additional tool to prevent tampering of measurement data.

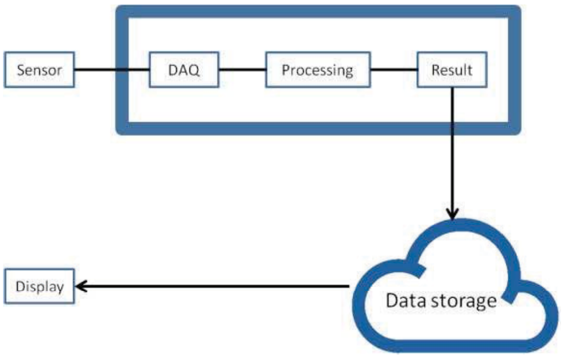

Figure 6: Cloud storage solution. Processing of data happens in a sealed measuring instrument. Results are sent to the cloud storage.

Measuring Algorithm and Parameter Export

This scenario is similar to the prior use case for data measuring and data acquisition, but before passing the data on to the processing step the measuring instrument has to register and connect to the cloud platform. Hence, the measurement algorithm and additional parameters has to be downloaded to be able to proceed with the processing of the measurement data. The main goal of this scenario is to prevent product imitation and to protect intellectual property of the manufacturer, who outsources their production lines into uncertain environments. Cloud computing acts exemplarily as a prevention strategy for intellectual property theft and downgrades the measurement device into a "dumb" device. In Figure 6 the display is connected directly to the measurement instrument but it is possible like in prior scenario to distribute the measurement result to the cloud and implement a software based display service.

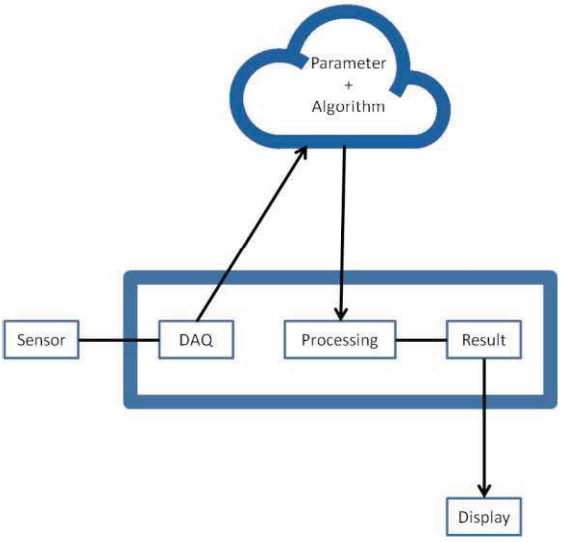

Figure 7: Cloud Computing as an approach to decrease product imitation by moving intellectual property into the cloud.

A moderately different approach to achieve conformity with the MID, and to enable a cloud computing solution for measuring instruments, is to separate the legally relevant and non-legally into different software modules, therewith to move the non-legally part to the cloud platform. The processing and legally relevant determination of the measurement result resides within the sealed and verifiable calibrated measuring instrument. The measurement data will be cryptographically signed and transported to the cloud, where the manufacturer can provide services to enhance the user experience. The measurement data is accessible by a software based display service as described in prior use cases.

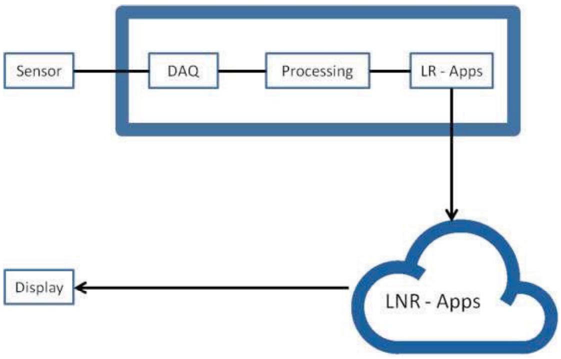

Figure 8: Processing and legal-relevant part stays in a sealed measuring instrument and the legal-non-relevant part is moved to the cloud.

Conclusion and Future Works

This paper introduced and outlined the field of legal metrology its characteristics and requirements. The initial work in the field of virtualization in legal metrology [5] is the foundation for this research work, since most of the requirements of the MID and the WELMEC 7.2 Software Guide are already addressed. The cloud computing platform environment has different needs and this will alter the framework to meet the legal requirements on its highest protection level. The challenge is to keep the technical advantages and benefits of a cloud computing solution while reaching conformity with the MID and the software security requirements.

The next steps will be to implement that framework on an Openstack Cloud platform and therewith show the feasibility. Further will be the proposed framework measured in its performance and robustness. Black and white hat testing will be performed to measure the effectiveness of the security measures.
The configuration, analysis and evaluation of the fully homomorphic schemes will also be part of the future work. It has to be proven that the data and algorithm can be effectively secured against tampering and attacks. Further the execution time for encryption, decryption and mathematical operations on encrypted data have to be determined and optimized. Finally as it is required by this year by the MID [20] a risk analysis has to be performed for the cloud platform.

References

[1] Thiel, F., Esche, M., Peters, D., and Grottker, U.. "Cloud Computing in Legal Metrology." 17th International Congress of Metrology. EDP Sciences, 2015.

[2] Directive 2014/32/EU of the European Parliament and of the Council from 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of measuring instruments (2014). Available for download from: http://old.eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2014:096:0149:0250:EN:PDF.

[3] WELMEC Guide 7.2: Software Guide (Measuring Instruments Directive 2004/22/EC), available for download at www.welmec.org.

[4] Organisation Internationale de Métrologie Légale (OIML), General requirements for software controlled measuring instruments, OIML D-31, (2008)

[5] Peters, D., Peter, M., Seifert,J.-P. and Thiel, F.. A Secure System Architecture for Measuring Instruments in Legal Metrology. In MDPI Computers, 4(2), 61 – 86, 2015

[6] Thiel, F., Grottker, U., Richter, D., The Challenge for legal metrology of Operating Systems Embedded in Measuring Instruments, OIML BULLETIN, 52 (LII), pp. 7-16, ISSN 0473-2812, (2011)

[7] Thiel, F., Grottker,U., Hartmann, V., Richter,D., IT Security standards and legal metrology – a Validation, EPJ Web of Conferences, Vol. 77, 00001, p.1-6, DOI 10.1051/epjconf/20147700001, ISSN 2100-014X (2014)

[8] Gentry, C.. *A fully homomorphic encryption scheme*. Diss. Stanford University, 2009.

[9] Chechulina,D., Shatilov, K., Krendelev, S.. Fully Homomorphic Encryption for Secure Computations in Protected Database, FedCis 2015, p.125 – 131

[10] Rivera, J ; Meulen, R Van d.. Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business. In: Retrieved March 31 (2014), S. 2015

[11] Leffler, N. and Thiel, F. (2013). Im Geschäftsverkehr das richtige Maß - Das neue Mess- und Eichgesetz, Schlaglichter der Wirtschaftspolitik. Monatsbericht; Bundesministerium für Wirtschaft und Technologie (BMWi).

[12] Kochsiek, M. and Odin, A. (2001). Towards a global measurement system: Contributions of international organizations. OIML Bulletin, 42(2):14–19.

[13] Rivest, R. L., Shamir, A., and Adleman, L. (1978). Amethod for obtaining digital signatures and public key cryptosystems. Communications of the ACM, 21(2):120–126.

[14] Rivest, R. L., Adleman, L., and Dertouzos, M. L. (1978).On data banks and privacy homomorphisms. Foundations of secure computation, 4(11):169–180.

[15] Gentry, C. et al. (2009). Fully homomorphic encryption using ideal lattices. In STOC, volume 9, pages 169–178.

[16] Van Dijk, M., Gentry, C., Halevi, S., and Vaikuntanathan, V. (2010). Fully homomorphic encryption over the integers. In Advances in cryptology–EUROCRYPT 2010, pages 24–43. Springer.

[17] Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., J¨aschke, A., Reuter, C. A., and Strand, M. (2015). A guide to fully homomorphic encryption.

[18] Aslett, L. J. M., Esperanc¸a, P. M., and Holmes, C. C. (2015). A review of homomorphic encryption and software tools for encrypted statistical machine learning. Technical report, University of Oxford.

[19] Rohloff, K. and Cousins, D. B. (2014). A scalable implementation of fully homomorphic encryption built on ntru. In Financial Cryptography and Data Security,pages 221–234. Springer.

[20] Esche, M. and Thiel, F. (2015). Software risk assessment for measuring instruments in legal metrology. In Computer Science and Information Systems (Fed-CSIS), 2015 Federated Conference on, pages 1113–1123. IEEE.

[21] Dekker, M.A.C. and Liveri, D. (2015). Cloud Security Guide for SMEs - Cloud computing security risks and opportunities for SMEs. In European Union Agency for Network and Information Security (ENISA), 2015, DOI 10.2824/508412

[22] Dupré,L. and Haeberlen, T. (2012). Cloud Computing Benefits, risks and recommendations for information security. In European Union Agency for Network and Information Security (ENISA), 2012