17th International Congress of Metrology, 16001 (2015)
DOI: 10.1051/metrology/201516001

Cloud Computing in Legal Metrology

F. Thiel , M. Esche, D. Peters and U. Grottker

Physikalisch-Technische Bundesanstalt (PTB), Abbe Str. 2-12, 10587 Berlin, Germany

Résumé. L'informatique en nuage (ou *"cloud computing"*) est un paradigme qui englobe une vaste palette de réalisations techniques, son but principal étant d'offrir un accès transparent à des ressources partagées à un grand nombre d'usagers, sans interactions nécessaires de la part de l'opérateur de ces ressources. Compte tenu des avantages des services dématérialisés, il est fort probable qu'on les retrouve bientôt également dans le secteur réglementé de la métrologie légale. Dans cet article, nous résumerons les définitions pertinentes ainsi que les architectures de référence décrivant les systèmes en nuage. Nous identifierons également les menaces principales touchant actuellement les nuages informatiques. En outre, nous donnerons un aperçu des travaux de normalisation en cours visant à garantir la sécurité de ces systèmes. Nous développerons et éluciderons plusieurs exemples dans lesquels il serait acceptable d'utiliser cette technologie dans le contexte de la métrologie légale. Ces exemples peuvent être considérés comme des suggestions pour l'élaboration à venir d'exigences informatiques en métrologie légale.

1 Introduction

Unlike the Internet, cloud computing is still at a comparatively early stage, giving Europe a chance to act to ensure being at the forefront of its further development and to benefit on both the demand and the supply side through wide-spread cloud use and cloud provision. A study undertaken for the European Commission in 2012 estimates, that the public cloud would generate € 250 billion in Gross Domestic Product (GDP) in 2020 with cloud-friendly policies in place against € 88 billion in the "no intervention" scenario, leading to extra cumulative impacts from 2015 to 2020 of € 600 billion. This translates into the creation of 2.5 million extra jobs [1], [2]. A future focus on cloud systems (Fig. 1) and applications thereof are often seen as the next logical step that consumers and providers of IT infrastructure will take based on existing technology. The main advantage lies, of course, with the central aim of cloud computing: improving the user's quality of service without him having to understand the technological background. The most important technology supporting this trend is virtualization [4] which allows for the allocation of resources on demand while providing more flexibility through dynamic use of existing infrastructure. Since this trend will eventually also reach the legal metrology sector, this paper intends to identify potential use cases for cloud technology and legal hurdles associated with their implementation in regulated market sectors. This may also provide a basis for this context on which Notified Bodies can rely when performing conformity assessment of cloud-based systems.

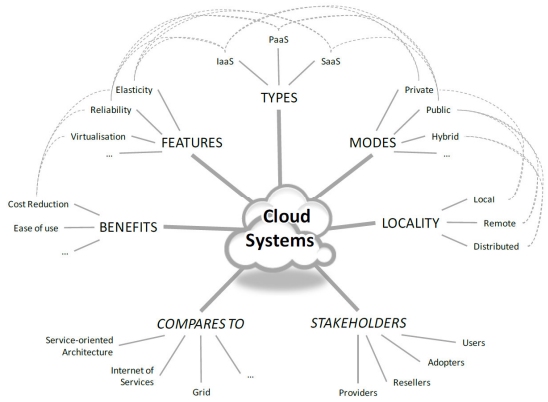

Fig. 1: Non-Exhaustive view on the main aspects forming a Cloud-System [3].

The remainder of the paper is structured as follows: Section 2 will highlight the future importance and possible benefits of the use of cloud systems in legal metrology. Relevant definitions and reference architectures to describe these systems will be summarized in Section 3. Afterwards, Section 4 further focuses on the top IT security threats cloud computing is currently encountering. The standardization efforts undertaken for cloud systems on the European level will be discussed in Section 5. For each of these standards the respective impact on legal metrology will be outlined. On

[a] Corresponding author: florian.thiel@ptb.de

that basis two acceptable examples of the utilization of cloud technology in legal metrology will be developed and explained in Section 6, where Infrastructure as a Service (IaaS) and Software as a Service (SaaS) are applied. These examples intend to provide an insight showing which direction the future development of IT related requirements should probably take in order to manage the increasingly sophisticated IT components and simultaneously not to overburden legal metrology authorities. Section 6 summarizes the paper and provides a conclusion.

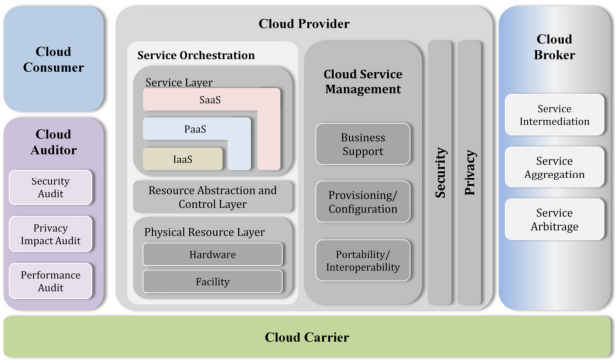

Fig. 2: Overview of the NIST cloud computing reference architecture [10].

2 Cloud Computing and Measuring Instruments

Unsurprisingly, with the advantages of Cloud Computing at hand, there are good prospects that this technology will find its way into measuring systems subject to legal control. Marketing concepts from manufacturers of measuring instruments who are active in legal metrology are already on the table utilizing several aspects cloud systems offer. These approaches make use of virtualized infrastructure to, e.g. remotely store legally relevant measurement data or to transfer the whole processing software into the "cloud", i.e. onto an external server. The latter solution makes the software at the individual measurement instrument available simply as a virtualized component which, e.g. makes the update procedures very simple for a large number of instruments and could simplify the work of the market surveillance authorities if they intend to test instruments remotely. Another application is to store only the part of the software which contains the intellectual properties of the manufacturer in the cloud as an anti-counterfeiting measure.
Therefore, the local instrument may be reduced to its core physical sensor combined with a miniaturized communication unit which provides the access to an open network, e.g. the Internet. This concept will reduce costs remarkably and will also encourage the miniaturization of sensors, which furthermore supports technologies such as those proposed in the digital agenda for Europe 2020 [5].
During the process of conformity assessment of measuring instruments, these systems have to meet the requirements of the Measuring Instruments Directive 2014/32/EU (MID) [6]. Several helpful guidelines have been developed [7][8] to support this process. Currently, the tailoring of essential requirements to all kinds of IT components, including validation recommendation, predominates. Complementary to this procedure, the practice of increasingly relying on international standards which cover essential requirements will be followed. To see if these guidance documents or related standards are fit for dealing with Cloud Computing or whether they need amendments, reaching a mutual understanding by using the same definitions and architectural designs will be of great help.

3 Prominent Definitions

Cloud computing is a developing concept undergoing frequent changes which is thus not fixed by definition. Nevertheless, the US National Institute of Standards and Technology (NIST) has provided a number of concept definitions in [9], which highlight important aspects of cloud systems, allows comparison between different solutions possible and may serve as a basis for a discussion about what cloud computing actually is and how it can be used.

According to the NIST definition, the cloud is first divided into a physical layer and an abstraction layer, see Figure 2. The physical layer encompasses all hardware resources, whereas the abstraction layer covers all software components used in conjunction with the physical layer. According to [9] cloud technology serves the purpose of providing network access by means of a shared number of both physical and abstract components such as networks, servers, applications, and provided services. The great advantage of the cloud lies in the transparency of these components to the actual user and the minimum amount of interaction required of the cloud provider.

3.1 Essential characteristics

In the publication [9] by NIST, five main characteristics, that set cloud computing apart from other technologies, were originally defined. These will be briefly revisited here.

1. *On-demand self-service:* The end user can at any time acquire as much computing capability as needed without having to consult individual service providers.
2. *Rapid elasticity:* Resources allocated to a user can be quickly scaled to fit current needs and can be released again immediately after use.
3. *Measured service:* To provide fair quality of service to all users of the cloud, resource usage can be optimized and controlled automatically. This ensures that both service provider and user receive a maximum of transparency.

4. *Broad Network access:* Since all services are provided over the network by making use of standardized protocols and interfaces, they can be used by a wide variety of different client devices ranging from mobile phones to laptops and workstation computers.
5. *Resource pooling:* Since the user has no control over which specific resources are made available to him, the provider can pool his resources and allocate them flexibly to multiple users if needed.

Hamada et al. [4] identified a sixth characteristic which shows some helpful properties in the context of legal metrology, e.g. for the assessment of conformity by notified bodies and market surveillance. The work of both parties could greatly profit from certificates issued by other entities supporting the auditability of cloud configurations.

6. *Auditability and certifiability:* Hamada et al. suggest that all cloud services should keep logs concerning the correct realization of policies. Such policies may, for example, be rules or regulations that the cloud provider needs to comply with.

3.2 Service Models:

Based on the reference architecture shown in Figure 2, cloud computing can be seen as a stack of services that are layered on top of each other. The stack provides a means of differentiating the degree of freedom that a cloud user has in realizing his solutions. The following three service models can be frequently found in the literature. Exact definitions are, for example, given again in [9].

Software as a Service (SaaS): In this scenario, the consumer receives access to certain applications offered to him by the cloud provider. The consumer is unaware of both the underlying software stack and the exact hardware. Access to the cloud application may either be through web-based services such as a browser or through a specific application programming interface (API). In both cases, the user has no influence on the underlying hardware and software components such as protocol stacks, the operating system, memory or network configurations etc.

Platform as a Service (PaaS): A next step in giving the consumer more flexibility consists of allowing him to run his own applications on top of the cloud provider's platform. Compared to the SaaS scenario, only the application itself is removed from the provider's control and handed to the consumer. All other components such as available libraries and services are beyond the control of the user. Again the underlying infrastructure should be completely transparent to him. A minimal degree of control may be exerted over the configuration of the environment in which the application runs.

Infrastructure as a Service (IaaS): This scenario corresponds to the case where a consumer rents hardware infrastructure to run his own software on top of it. This may cover everything from the underlying operating system, storage units, the network configuration, libraries as well as tools and applications. Consequently, the cloud provider's control responsibilities are in this case significantly lower than for PaaS and SaaS. For the service dependent activities of the parties see Figure 3.

Service Models	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Installs, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud system.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

Fig. 3: Service model dependent activities of the Cloud Consumer and Cloud Provider [11].

3.3 Scope of Control between Provider and Consumer

The selected service model has an impact on the control the user has over the resources available to him. Similarly, with a lesser degree of influence by the user, more control can be exerted by the provider himself. Both facts are visually represented in Figure 4. With a changing degree of control, legal responsibilities for both parties involved with maintenance and use of the cloud also change. A detailed analysis of the responsibilities of both provider and consumer may be found in [10].

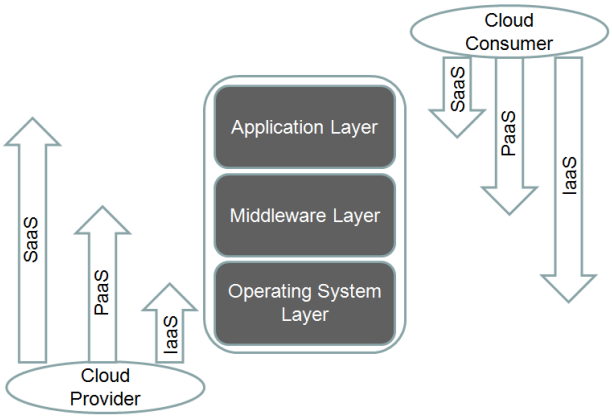

Fig. 4: Control responsibilities depended on the service model [10].

For legal metrology, it is essential that different service models lead to different responsibilities as indicated above. In the case that a manufacturer uses services from a cloud provider, the user is nonetheless accountable for the security. Therefore the contract between both parties

should incorporate necessary certificates, security standards used etc. The notified body could support the manufacturer during the contract design.

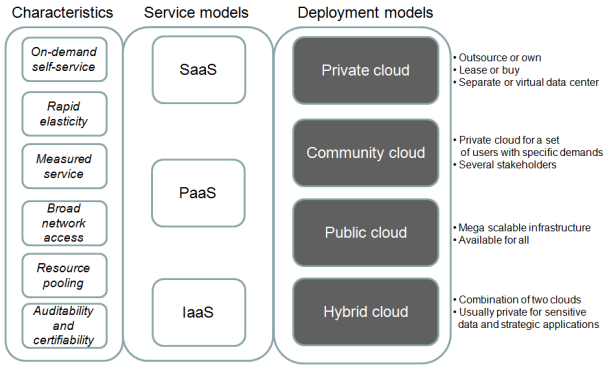

Fig. 5: Cloud characteristics, service models and deployment models.

3.4 Usage Models

A usage or deployment model specifies both the legal ecosystem in which the cloud resides as well as its size and possible access scenarios. The following four general terms have been coined in [10] and will here be interpreted specifically for the field of legal metrology.

Private cloud: The term *private cloud* refers to an infrastructure that is reserved exclusively for use by one single customer. Depending on the actual physical location of the hardware, [10] here differentiates between *on-site private clouds* and *outsourced private clouds*. The first of both cases could be especially appealing to market surveillance bodies, since it allows for on-site checks of the used infrastructure. If a third-party provider operates the cloud, contractual obligations between provider and user become of interest. This will be discussed further in Section 6.

Community cloud: This scenario shares several common properties with the *private cloud* solution. The cloud infrastructure is, however, made available for use not by one customer, but by a group of consumers with common objectives. Again, the location of the cloud can be on the premises of a customer (*on-site community cloud*) or it can be operated as an *outsourced community cloud*. The driving paradigm behind the community cloud is the sharing of both common cloud resources and the resources of the community partners.

Public cloud: A public cloud's business model differs significantly from those of the previously introduced scenarios. Here, a provider makes his cloud infrastructure available to an arbitrary set of customers. The cloud services are thus sold to the general public and are accessible over the Internet.

Hybrid cloud: The term hybrid cloud describes an amalgamation of at least two of the above scenarios. These preserve their separate identities but are linked by standardized protocols and data formats that allow for porting of both data and applications among the different cloud models employed.

For a visualized summary of the characteristics, the service and the deployment models see Figure 5.

Based on the selected usage model, the relevant threats to the functionality of the cloud can be identified originating both from within the intended user group and from possible malicious outsiders.

4 Top Threats to Cloud Computing

According to the responsibilities laid down for the consumers in legal metrology, they also have to concern themselves with the risks associated with Cloud Computing. If there are no adequate security mechanisms, one consequence could be the loss of control over systems for which the customer is directly responsible. Therefore, it becomes necessary to take a closer look at the current risk landscape associated with the cloud. A recent study by the Cloud Security Alliance (CSA) [12] lists the following nine major threats to cloud security:

1. *Data Breaches*
2. *Data Loss*
3. *Account Hijacking*
4. *Insecure Interfaces and APIs*
5. *Denial of Service*
6. *Malicious Insiders*
7. *Abuse of Cloud Services*
8. *Insufficient Due Diligence*
9. *Shared Technology Issues*

A detailed evaluation of these threats and a presentation of adequate countermeasures may be found in [13]. From the above list it should become clear, that cloud computing is a technology that can easily come under attack and for which general purpose exploits can probably be obtained without difficulty. Since metrological security and resistance to manipulations are part of the essential requirements in the MID, the manufacturer of a measuring device has to show that moving metrological functionality to the cloud essentially poses no greater risk of invalidating the essential requirements than having the functionality physically located on a distinct device.

An adequate level of security is thus required while trying at the same time not to overburden the innovative potential of the manufacturers and of the providers of cloud services. According to the European Measuring Instruments Directive 2014/32/EU [6], which regulates activities in the field of legal metrology, an adequate analysis and assessment of the risk(s) associated with an instrument must be carried out by the manufacturer when submitting a system or device for conformity assessment to a Notified Body. In such an analysis the above threats

have to be taken into account to convince the notified body that the essential requirements cannot corrupted.

In [14], the authors describe a risk assessment method for measuring devices based on the ISO/IEC standards 27005 [15], 15408 [16], and 18045 [17]. The method uses a reproducible risk probability score derived from the Common Criteria vulnerability analysis as detailed in [16]. Calculating a risk score requires a formal description of assets, threats, threat agents and system vulnerabilities, see Figure 6. Details on the generic derivation of assets and threats may be found in [14]. With the help of that approach a method is in place to evaluate the risk associated with innovative IT solutions in legal metrology which can be easily applied to cloud computing scenarios, too.

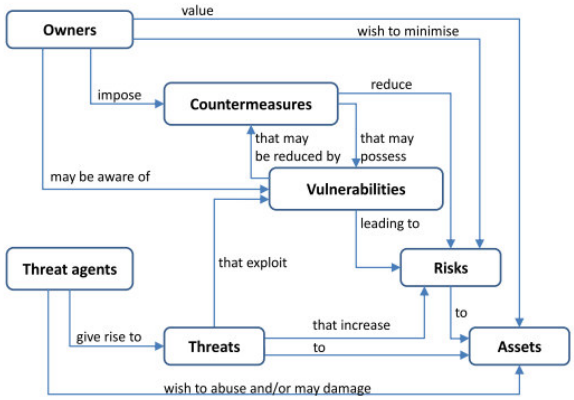

Fig. 6: The elements relevant to IT risks and their relationships according to ISO 15408:2005 (Common Criteria) [16].

5 European Standardization for CC

In legal metrology the application of standards by the manufacturers to cover essential requirements is common practice. To identify such standards for cloud computing is helpful for building a knowledge base for the notified bodies to assist the manufacturer during the type approval process. Furthermore, the legal aspect of shared responsibility between the cloud provider and the cloud customer as shown in Figure 4 must be considered since the modalities for contract design between these partners are unclear today.

Both initiatives for standardization and legal aspects have been initiated on the European level and their status is described in the following section.

The European Commission's communication on the European cloud strategy describes one key action for standardization in this context [2]: to identify a list of necessary standards that ensure data security, interoperability as well as data portability. Tasked with this action is the European Telecommunication Standards Institute (ETSI) which has recently launched the Cloud Standards Coordination (CSC) initiative [18].

For the identification of relevant standards one may also refer to the NIST Cloud Computing Standards Roadmap [11]. In addition, the NIST Cloud Computing Standards Roadmap Working Group provides an extended inventory of standards relevant to Cloud Computing [19]. The activities by NIST are very likely to influence the European initiatives as well.

The aim of the European cloud computing strategy is to develop model contract terms that would regulate issues not covered by the Common European Sales Law such as:

- *data preservation after termination of the contract,*
- *data disclosure and integrity,*
- *data location and transfer,*
- *ownership of the data,*
- *direct and indirect liability,*
- *change of service by cloud providers,*
- *subcontracting*

These model contract terms are a prerequisite for the approval of cloud-based measuring systems since responsibilities defined for the market players in legal metrology need to be covered by these contracts whenever responsibilities and resources are shared.

6 Cloud Solutions for legal metrology

In the following section, some examples of cloud services, which could become important in legal metrology, will be discussed. We assume an external cloud service provider, i.e. the off-premises solution rather than the on-premises one. The latter would entail fewer constrains, since it is under complete control of the manufacturer. The whole cloud system stack consists of the facility, the networking part including the firewall, the physical server, the virtual machines, the utilized operating system, the storage device, and the web server (s. Figure 7). It seems obvious that the whole stack needs to be evaluated. This requires a significant number of tests and an extensive system analysis. Therefore, aiming for a more effective procedure, solutions are preferred that do not require this task.

To understand cloud computing risks, it is important to look at the relationships between the cloud computing models. IaaS is the foundation of all cloud services, with PaaS building upon IaaS, and SaaS upon PaaS, as shown in Figure 2. Hereby, not just the capabilities are inherited, but also the information security issues and associated risks.

Three important cloud configurations and their security issues regarding legal requirements that have to be resolved will now be identified.

6.1 Infrastructure as a Service:

In general, IaaS provides enormous extensibility with few application-like features. This means less integrated security capabilities and functionality beyond protecting the infrastructure itself. This model requires that operating systems, applications, and content be managed and secured by the cloud consumer.
The simplest application of IaaS is the one which just uses external hardware to store measurement data, like a dropbox (s. Figure 6).

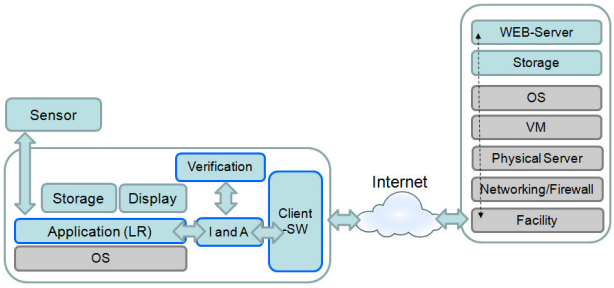

Fig. 7: IaaS: utilizing external memory as infrastructure in the Cloud. (I: Integrity, A: Authenticity, OS: Operating System, VM: Virtual machine, LR: legally relevant)

Assuming that integrity and authenticity of the data are ensured, there is no need to evaluate the complete system stack. Applying state of the art signature algorithms ensures these requirements. Hereby, the data sent to the cloud should be encrypted first or at least signed by the measuring instrument with its private key. In this scenario, the cloud system can be regarded as a black box, because it cannot modify the data without detection.

If the market surveillance authorities intend to carry out their tests via the Internet, i.e. decide to access the data in the cloud remotely and not on the instrument itself, the keys of the instrument must be derived from a Public Key Infrastructure (PKI) to guarantee the correctness of the public key. In that case, each measuring instrument and its data can be authenticated by a unique set of public and private key.

A challenge that still arises in this context is that availability cannot be guaranteed. If a certain billing action is questioned, and the data needed cannot be retrieved from the cloud, the responsibility lies with the user of the measuring instrument. Nevertheless, it can be argued that the data in a cloud is normally better secured (by backup systems) than on a single measuring instrument.

6.2 Platform as a Service

PaaS models a system, where the cloud provider delivers a computing platform, typically including operating system, programming language execution environment, database and webserver. It seems unlikely that such a service finds a realistic application in legal metrology. Nevertheless, in the general definition, PaaS lies on top of IaaS and adds a middleware to the Cloud. This extends to security features. So the additional middleware can be used to add security functionality to the scenario described in Section 6.1. Hereby, the middleware could be used to access the distributed storage devices. Of course, the same challenges concerning availability arise.

6.3 Software as a Service

The last example aims at the transfer of the processing software from the instrument into the cloud (s. Figure 8). This is generally known as using Software as a Service.

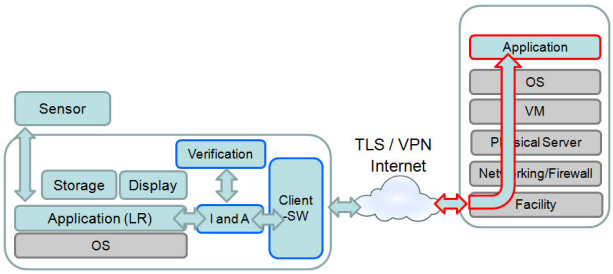

Fig. 8: SaaS: Software application transferred in the Cloud. (I: Integrity, A: Authenticity, OS: Operating System, VM: Virtual machine, LR: legally relevant). TLS: Transport Layer Security VPN: virtual private network.

The aim is to reduce this complex system into a well known one, e.g. the “desktop” solution. The connection to the application in the cloud should be done via an internet tunnel, e.g. constructing a virtual private network (VPN) with the help of the Transport Layer Security (TLS) protocol.

6.3.1 Trusted Software as a Service

The downside of SaaS regarding legal metrology is that the cloud infrastructure itself cannot be trusted. It will probably be difficult to convince the Notified Body that the application is running in a secure environment which protects its keys from the underlying framework in the cloud. The protection of the keys is crucial, because if the keys are accessible to an illicit part of the framework, they can be used to create trusted input and output for the measuring instrument. To prevent this from happening, trust in the infrastructure could be achieved through three points:

- *Risk analysis and assessment*
- *Contract design*
- *Third party cloud certificates*

According to legal requirements, the examination of the technical design of an instrument is sufficient for the assessment of conformity. Further measures are the design of civil contracts between manufacturer and cloud service provider and the use of third party cloud-certificates, e.g. on security measures.

The manufacturer could be obliged to set up a contract with the cloud service provider about issues such as listed

in chapter 5. In this scenario, the cloud service provider becomes a sub-contractor. Furthermore, certificates about applied security and emergency standards should be requested to establish the Notified Body's trust in the design.

Certificates of third parties are accepted within the legal requirements. National IT Security organization like NIST or the German BSI give guidelines on cloud-certification and contract design (i.e. service level agreement (SLA)). Nevertheless it should be noted, that exact procedures and rules concerning legal metrology are yet to be stipulated, so the points mentioned in this section should be seen as guidelines.

The Sealed Cloud [20], for example, is a patented technology, that enables data centers to be secured in a way that processed data and content cannot be accessed by the operator. A consortium, consisting of the Fraunhofer Institute for Applied and Integrated Security (AISEC) as well as the companies Uniscon and SecureNet develops this technology for the Trusted Cloud program of the Federal Ministry of Economy and Energy in Germany (BMWi). Another example, also developed by the Trusted Cloud program is Tresor [21]. Tresor targets the health care domain, with the goal of secure and trusted electronic transfer of patient data from one medical facility to another.

From the software side, new and upcoming technologies like the Intel Software Guard Extensions (SGX) [22] could help the cloud provider to establish trust. Intel SGX is a set of new CPU instructions that can be used by applications to set aside private regions of code and data that cannot be modified by other software including the underlying virtual machine monitor or the operating system.

In all cases, the cloud servers should interact with the instrument in some kind of “handshaking” mode. Handshaking, i.e. challenge-handshake, in this regard means the mutual authentication of two systems or software parts to validate the identity of the originator of the connection upon connection or any time later by cryptographic means.

Additionally, remote attestation for clouds is an interesting aspect, which for example can be realized by the Intel OpenAttestation SDK (OAT) [23]. Remote attestation services are critical for implementing security solutions in the cloud. This can be achieved through remote attestation servers, as described in [23]. Here, all the metrics related to the virtual machines (VM) and their status are maintained and compared with earlier states of successful service deployment through a standalone attestation server that makes sure that only expected programs with expected configuration files are loaded inside the expected VM and only the VM with the expected software stack is running.

6.3.2 A Suggested Framework:

A measure that enforces security by separation is, as already mentioned, the use of virtualization. An example is given in [24] that uses a separation kernel and virtualized compartments but in a single measuring instrument not in a cloud. By doing so the usual requirements on the operating system apply [25], [26]. Even software updates and patches for the operating system can be installed without a need for re-certification. The suggested architecture, which can be deployed by the manufacturer in cooperation with the cloud provider, scales well with the legal requirements, and enforces security by virtualization. In Figure 9, the approach from [24] can be seen, but it is here adapted to the requirements for cloud systems.

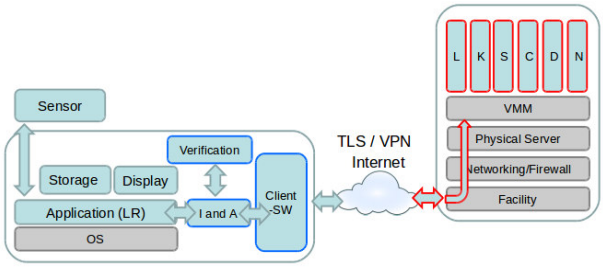

Fig. 9: SaaS Framework: Securing Software through virtualization. (I: Integrity, A: Authenticity, LR: legally relevant, VMM: Virtual Machine Monitor, L: legally relevant VM, K: Key & Signature Manager, S: Storage Manager, C: Connection Manager, D: Download Manager, N: non-legally relevant VM)

In this framework, legally relevant tasks (tasks that are needed for the measurement purpose) are separated from non-legally relevant ones by putting them in different VMs, the N VM (non-legally relevant VM) and the L VM (legally relevant VM).

The rest of the basic cloud-framework consists of four basic virtual machines that help to fulfill the legally relevant functions, like storing keys (K VM), storing data (S VM), supervising communication (C VM) and managing software updates (D VM).

This modular system architecture scales well, because the virtual machines can just be copied, multiplied and dynamically swapped from server to server, whenever more or less computations are needed. It is even possible to swap out non-legally relevant task (N VMs) to a public cloud which is not subject to legal control.

For this solution the manufacturers, which create the software stack for SaaS, need to have complete access to the cloud. They should be responsible for the underlying hardware together with the cloud provider. Trust can again be achieved by the points listet in Section 6.3.1.

7 Conclusion

According to Gardner's 2014 Hype Cycle for Emerging Technologies, Cloud Computing has nearly reached the "Trough of Disillusionment" [27]. It is therefore expected that in the next two to five years the industry will develop and implement realistic strategies for the use of Cloud Computing in legal metrology. Since the notified body shall keep itself apprised of any changes in the generally acknowledged state of the art [6], the technology enabling Cloud Computing and the security threats, which this technology could encounter, should be of vital interest to notified bodies. This is especially important since the solutions adopted in the pursuit of the essential requirements shall take account of the intended use of the instrument and any foreseeable misuse thereof [6]. This paper intended to give notified bodies guidance in this field by summarizing the relevant definitions and reference architectures that describe cloud systems. It further focused on the top IT security threats cloud computing is currently facing. Standardization efforts undertaken for such systems have also been discussed. On that basis two acceptable examples of the utilization of cloud technology in legal metrology (Infrastructure as a Service and Software as a Service) were developed and explained.

8 Acknowledgements

The authors are grateful to the colleagues of the department 8.5 *Metrological Information Technology* of Physikalisch-Technische Bundesanstalt for helpful discussions and critical remarks.

References

[1] IDC, "Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up", (2012).
Available for download from:
http://cordis.europa.eu/fp7/ict/ssai/docs/study45-d2-interim-report.pdf

[2] Unleashing the Potential of Cloud Computing in Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2012) 529,
Available for download from:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012DC0529

[3] The future of Cloud Computing, Opportunities for European Cloud Computing Beyond 2010.
Available for download from:
http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf, European Commission (2010)

[4] M. Hamadaqa, and L. Tahvildari, Cloud Computing Uncovered: A Research Landscape, Adv. In Computers, Vol.86, pp. 41–85. ISBN 0-12-396535-7, (2012)

[5] DIGITALEUROPE's Vision 2020.
Available for download from:
http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=157&PortalId=0&TabId=353

[6] 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.

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

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

[9] P. Mell, T. Grance, NIST Special Publication 800-145, The NIST Definition of Cloud Computing, September 2011.
Available for download from:
http://www.nist.gov/itl/cloud/publications.cfm

[10] NIST SP 500-292 NIST Cloud Computing Reference Architecture, (2011)
Available for download from:
http://www.nist.gov/itl/cloud/publications.cfm

[11] NIST Special Publication 500-291 version 2, NIST Cloud Computing Standards Roadmap, July 2013,
Available for download from:
http://www.nist.gov/itl/cloud/publications.cfm

[12] Cloud Security Alliance, "The Notorious Nine Cloud Computing Top Threats in 2013" 2013,
Avaliable from:
https://cloudsecurityalliance.org/research/top-threats/

[13] C. M. R. da Silva et al., Systematic Mapping Study On Security Threats in Cloud Computing (IJCSIS) International Journal of Computer Science and Information Security,Vol. 11, No. 3, March 2013
Available for download from:
http://arxiv.org/ftp/arxiv/papers/1303/1303.6782.pdf

[14] M. Esche and F. Thiel, Software Risk Assessment for Measuring Instruments in Legal metrology, submitted to Federated Conference on Computer Science and Information Systems (FedCSIS), (2015)

[15] "ISO/IEC 27005:2011(e) Information technology - Security techniques - Information security risk management," International Organization for Standardization, Geneva, CH, Standard, June 2011.

[16] "ISO/IEC 15408:2012 Common Criteria for Information Technology Security Evaluation," International Organization for Standardization, Geneva, CH, Standard, September 2012, Version 3.1 Revision 4.

[17] "ISO/IEC 18045:2012 Common Methodology for Information Technology Security Evaluation," International Organization for Standardization, Geneva, CH, Standard, September 2012, Version 3.1 Revision 4.

[18] ETSI Cloud Standards Coordination, Final Report 2013. Available for download from: http://www.etsi.org/images/files/Events/2013/2013_CSC_Delivery_WS/CSC-Final_report-013-CSC_Final_report_v1_0_PDF_format-.PDF

[19] NIST Inventory of Standards Relevant to Cloud Computing. Accessible via: http://collaborate.nist.gov/twiki-cloudcomputing/bin/view/CloudComputing/StandardsInventory

[20] Uniscon GmbH – The Web Privacy Company, A Reliable Data Center Excluding Provider Access to Client Data, Available from: https://www.idgard.de/en/sealed-cloud-white-paper-en/

[21] TRESOR – Trusted Ecosystem for Standardized and Open cloud-based Resources, Available from: http://www.cloud-tresor.com/

[22] Ollie Whitehouse, Intel Software Guard Extensions (SGX): A Researcher's Primer, Available from: https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/january/intel-software-guard-extensions-sgx-a-researchers-primer/

[23] U. Shanmugam, L. Tamilselvan, U. Nandhini, and Dhinakaran, Attestation for Trusted Computing to Assure Security in Cloud Deployment Services, International Journal of Information and Electronics Engineering, Vol. 2, No. 4, July 2012

[24] D. Peters, M. Peter, J.-P. Seifert , F. Thiel, A Secure System Architecture for Measuring Instruments in legal metrology, published in Computers Open Access Journal (ISSN 2073-431X) doi:10.3390/computers4020061,(2015)

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

[26] F. Thiel, U. Grottker, V. Hartmann, D. Richter, 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)

[27] Gartner's 2014 Hype Cycle for Emerging Technologies**,** Accessible via: http://www.gartner.com/newsroom/id/2819918