Position papers of the Federated Conference on Computer Science and Information Systems, pp. 119–125
DOI: 10.15439/2017F556
ISSN 2300-5963 ACSIS, Vol. 12

A Modular Testbed for Intelligent Meters and their Ecosystem

Jan Wetzlich, Martin Nischwitz, Florian Thiel
Physikalisch-Technische Bundesanstalt,
Germany
Email: {jan.wetzlich, martin.nischwitz, florian.thiel}@ptb.de

Jean-Pierre Seifert
Security in Telecommunications,
Technische Universität Berlin,
Germany
Email: jp.seifert@sec.t-labs.tu-berlin.de

***Abstract*—Modern, intelligent measuring systems are increasingly distributed and networked or even virtualized. In order to guarantee the security of the measurements, security gateways are an effective means of protecting the local sensors and displays from manipulations from public wide area networks. On the other hand this means a complex, tiered eco system, therefore we are setting up a testbed for conducting further research on this topic concerning new innovative security approaches beyond traditional public key infrastructure and their influence on system architectures, secure remote verification and legally conform update mechanisms.**

I. Introduction

THE European Union is facing unprecedented challenges resulting from increased dependence on energy imports and scarce energy resources, and the need to limit climate change. Energy efficiency is a valuable means to address these challenges. It improves the Union's security of supply by reducing primary energy consumption and decreasing energy imports. The conclusions of the European Council emphasised the need to increase energy efficiency in the Union to achieve the objective of saving 20 % of the Union's primary energy consumption by 2020. To achieve this the European Commission has issued the directive 2012/27/EC [7] on energy efficiency which directly addresses energy end-use efficiency and energy services. A main statement is the introduction of intelligent energy meters to increase the awareness of the end-user about its consumption. Furthermore, the aim was formulated in the directive that at least 80 % of consumers should be equipped with intelligent metering systems by 2020. These energy meters are regulated within the framework of legal metrology.

Even only in Germany Legal Metrology covers around 160 million measuring instruments, which are used for business or administrative purposes or in the public interest. They are subdivided into 150 types of equipment, subassemblies and additional equipment. The largest share is attributable to the area of commodity meters, such as electricity, gas, water and heat meters. Other everyday points of contact with Legal Metrology include not only dispensing pumps at petrol stations and scales in the retail trade, but also speed and alcohol meters. The importance of adequate protection against tampering of the software in such measuring instruments can be seen in the proportion of the gross domestic product (GDP) generated by legal measurement: in most industrialized countries, legally relevant measurements are responsible for a share of 4% to 6% of GDP. This corresponds in Germany to an annual turnover of 104 to 157 billion Euros [1]. The consequences of successful manipulation can easily be estimated from these figures. At the same time, Legal Metrology is responsible for around 56% of the federal tax bill. In 2015, some 40 billion Euros was accounted for solely by revenue from the energy tax (electricity / gas / heat / mineral oil) [3].

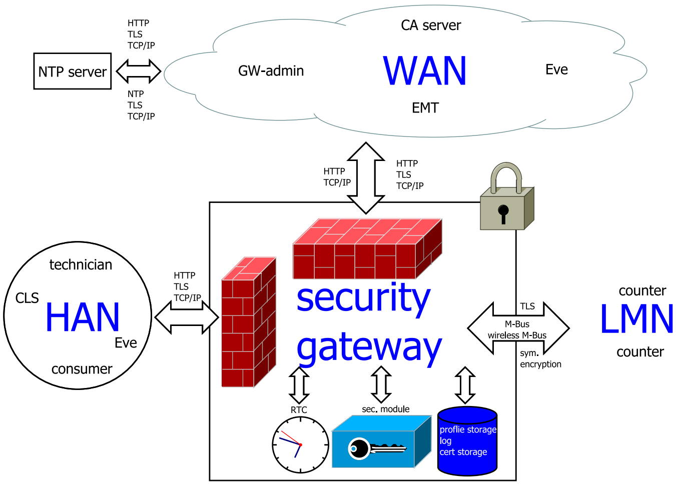


Fig. 1. Common entities in an ecosystem for intelligent meters covering an home area network (HAN) with some controllable local systems (CLS) connected to a wide area network (WAN) with external market participants (EMT) and a local metrological network (LMN) with different counters and meters

Due to the strong trend towards digitalization, the share of software in measurement systems will grow steadily. At the same time, software already accounts for more than half of the development process in some measuring instruments. This evolution is accompanied by virtualization, networks and spacial distribution of sensors, data processing, data storage and monitoring. In Figure 1 a common example for such a system is shown. In order to guarantee the security of the measurements, security gateways are an effective means of protecting the local sensors and displays from manipulations from public broadband networks (WAN). In addition, there

are new technical possibilities for diagnostic tests as well as firmware updates from afar. Therefor a testbed for intelligent measuring systems is being developed at the PTB in cooperation with TU Berlin in order to investigate the associated processes and architectures scientifically.
In section II we discuss the legal framework for intelligent measuring instruments, section III presents the structure of the testbed ecosystem and the approach for the modeling testbed with its components and interfaces and finally section IV discusses targeted research in the field of intelligent measurement systems to be performed using the testbed.

II. Legal Metrology

The central concern of Legal Metrology is to protect and ensure trust in measurements. In this context, Legal Metrology does a lasting contribution to a functioning economic system by simultaneously protecting the consumers.

The International Organization of Legal Metrology (OIML) was set up to assist in harmonising such regulations across national boundaries to ensure that legal requirements do not lead to barriers in trade. Software requirements for this purpose are formulated in the OIML D 31 document [8]. WELMEC is the European committee to promote cooperation in the field of Legal Metrology, for example by establishing guides to help notified bodies (responsible for checking the measuring instruments) and manufacturers implement the Measuring Instruments Directive described below.

A. *Legal European Framework*

Directive 2014/32/EU of the European Parliament and of the Council [6], which is based on Directive 2004/22/EC [5], known as the Measuring Instruments Directive (MID), are directives by the European Union to establish a harmonized European market for measuring instruments, which are used in different member states. The aim of the MID is to protect the consumer and to create a basis for fair trade and trust in the public interest. The directive is limited to ten types of measuring instruments that have a special economic importance because of their number or their 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 analysers. The MID defines basic requirements for these measuring instruments, e.g. the protection against tampering and the display of billing-related readings. Each measuring instrument manufacturer themselves decide which technical solutions they want to apply. Nevertheless, they must prove to a notified body that their instrument complies to the MID requirements. The notified bodies that must be embraced by the manufacturers are denominated by the member states. In Germany, for example, the Physikalisch-Technische Bundesanstalt (PTB) is such a notified body. The PTB is furthermore the German national metrology institute providing additional scientific and technical services, which is why it achieves the demanded technical expertise needed. In general, the combination of technical expertise related to the measuring instruments, competence for the assessment, monitoring of product related quality assurance systems, and experience with European regulations, are required. Additionally, it is of particular importance that the notified body is independent and impartial.

B. *Critical Infrastructure*

Commodity meters for gas, water and electrical energy are concerned to be parts of a critical infrastructure, which results in requirements of a high security level, but also the use of reliable, interoperable and trusted standards like [9].

III. Approach

The main idea is to highly use virtualization so that most parts of the testbed can be done in software. This provides higher flexibility for exchanging parts of the ecosystem and scaling to larger numbers of sensors etc. As a starting point we choose the eco system that is described by the technical directive TR-03109 from the German BSI [4]. In Figure 1 the composition of the ecosystem is shown. Only the gateway itself is implemented as a separate board. The main advantage of the chosen system is the opportunity to downscale this high level security system to use cases, where less security is mandatory or required. On the other side chosen system constitutes of traditional, state of the art concepts and technologies, including e.g. a public key infrastructure (PKI) and stateless webservices. Another side effect is the fact, that [4] will be mandatory for new electrical energy, water, gas and heat meters in Germany in the future, so there will be a huge dissemination of such systems. This means advancement, which can be easily integrated in the testbed or at least in a non disruptive manner, are more likely to be adopted.

A. *Interfaces*

In addition to the network interfaces, UART (TTL, RS232), RS485 / M-Bus, I2C and SPI as well as wireless M-Bus are available in the metrological network. The radio interface is implemented as a physical interface as well as via a channel simulation. With the help of the channel simulations, the system behavior can be investigated in the event of malfunctions and attacks on the wireless interfaces. The implemented simulated distortions include echoes, interference from other users of the ISM band, such as through home automation systems and forced collisions by simultaneous data transmission. For the manipulation of sensor signals and the interruption of physical interfaces, 4 digital to analog converters (DAC) and 16 DIO are available, which can switch further relays. By means of four analog-to-digital converters (ADC), any controllable devices can be tested for their reactions.

B. *Sensors*

The sensors of the measuring system are also simulated, which results in an independence from the measured physical variables. The virtualization approach allows the number of

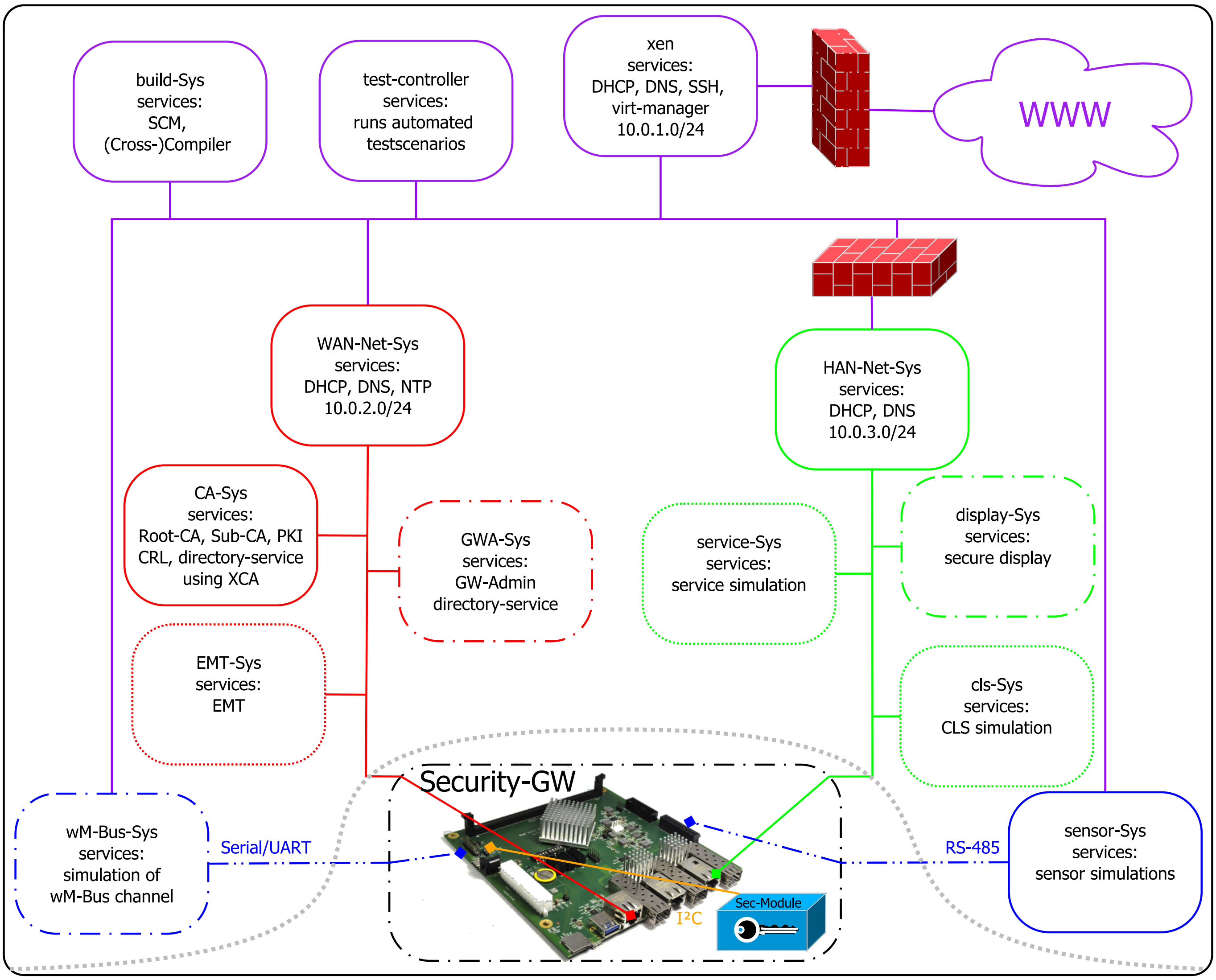


Fig. 2. Network layout of the ecosystem: HAN (green), WAN (red) and LMN (blue) are connected by the security gateway. For testing purposes there is an additional network around the eco system (purple).

sensors to be scaled and combined as desired. The configurable parameters of the basic behavior of the sensor simulation are:

- cyclic measurement data or incrementation rate for accumulative counters
- encryption type (plain/symmetrical AES/asymmetrical RSA or ECC)
- used credentials
- used interface (wireless M-Bus/M-Bus/RS232/I2C/SPI)
- parameters for the channel simulation(sending interval/obstacles)

The second possibility for controlling the sensor simulation is to dynamically manipulate the sensor during the execution of a test scenario. For example, it is possible to set counter readings, change keys, or interrupt the transmission or reception function at the interface to the gateway.

C. *Network topology*

The different networks of the ecosystem consist of wide area network (WAN) and a home area network. The WAN constitutes of a public key infrastructure, the gateway administrator, a system that provides general network services such as DNS, DHCP, NTP, as well as simulated external market participants. The local network also provides general network services with DNS and DHCP, in addition, a secure display, service technician and controllable systems are also connected here. In deviation from [4], there is also the possibility to connect sensors via network interfaces in the metrological network.

D. *PKI*

The initial version of the testbed constitutes of a traditional PKI with a single root certificate authority (root-CA) at the top, a tier with some subsequent CAs and at the bottom different

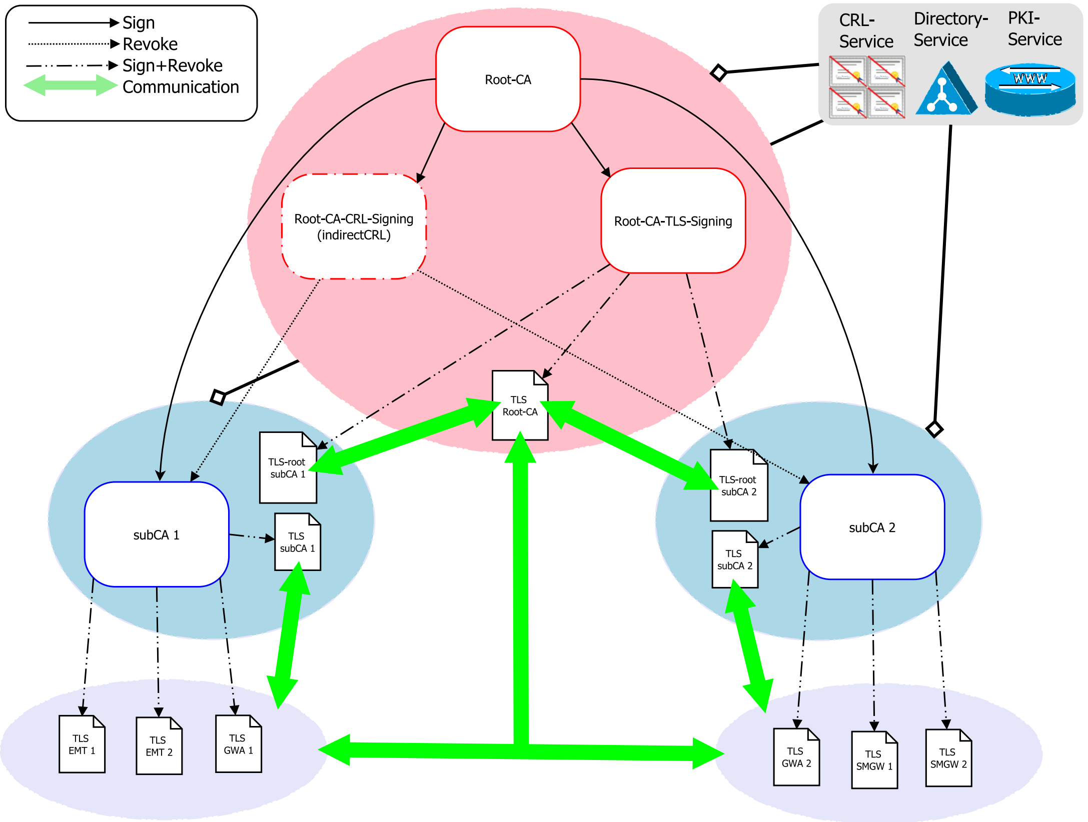


Fig. 3. The hierachy of the implemented PKI.

certificate users e.g. GW admins, security gateways and TLS communication between CAs. The certificates are served via LDAP(s) and can be requested/issued via webservices. Signed certificate revocation list (CRL) are available via HTTP. The hole architecture is shown in Figure 3.

E. Test Automation

Running test scenarios is prepared by the test controller by establishing a defined output state and controlled by calling atomic methods of the test API during the course of the individual scenarios. The test scenarios are implemented for the greatest possible flexibility in Python. Figure 4 shows schematically the structure of the test API for a single component of the ecosystem. The test controller can access all components of the ecosystem, whereby the services and interfaces already provided by the component are addressed preferably - for example, signing requests to the PKI. For more complex or non-existent methods, encapsulated extra test services are used on the component which, in turn, use existing services or interact directly with the ecosystem - for example, sending malicious data or requests or configuring new sensors in the gateway, this involves interactions with the gateway admin service, the gateway and possibly external market participants.
The test services are implemented on the side of the test controller as RESTful Webservices and are also written in Python. The third possible impact of the test controller on the ecosystem is manipulation using the analog and digital inputs and outputs, for example, to selectively switch off physically embedded components of the ecosystem, manipulate them or manipulate sensor inputs.

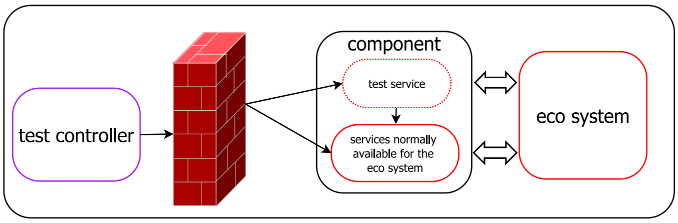


Fig. 4. Scheme of test API

F. GW reference architecture

Based on [2] we chose a microkernel architecture for the security gateway on an ARMv8 board. A major goal of the reference architecture is the development and evaluation of safe methods for remote maintenance of intelligent measuring systems, as well as remote detection and verification.

Advantages: Due to the small-sized trusted computing base (TBC), the integrity of the entire gateway can reliably be ensured and verified by the targeted microkernel architecture with separated minimal systems. Possibly existing security gaps in parts of the software have significantly less impact

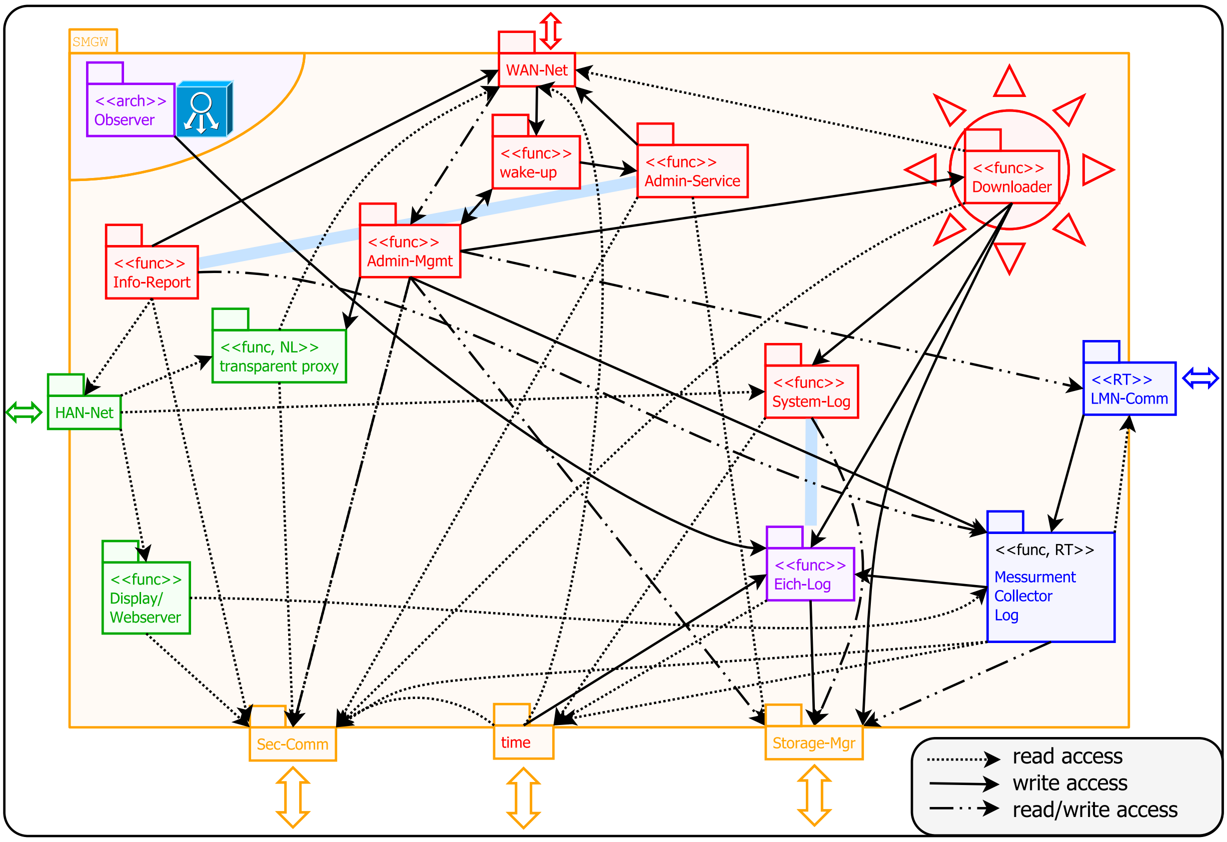


Fig. 5. Reference architecture for security gateway

on the overall system. A further advantage of the modular microkernel architecture is that the BSI TR-03109 (smart meter gateway with CC-certified security modules) can be used to scale the ecosystem as well as the gateway down to less sensitive measuring systems, in order to implement a protection level appropriate to the risk. The provided microkernel variants are, like all other components of the testbed opensource and thus particularly suitable as a reference architecture. In addition, virtualization enables existing applications to be run in a single virtual machine at a fast pace and then to be separated into individual virtual machines later.

Architecture design approach: In Figure 5 a possible partitioning for a security gateway is shown. In this case, conceivable functions, which have similar data streams, are combined into a virtual machine. Mainly these are the following functions:

- management service of the gateway itself
- informational services for the GW admin
- informational services for extern market participants
- informational services for local displays/devices in the HAN
- different system logs for users, admin and market authorities
- measurement data processing

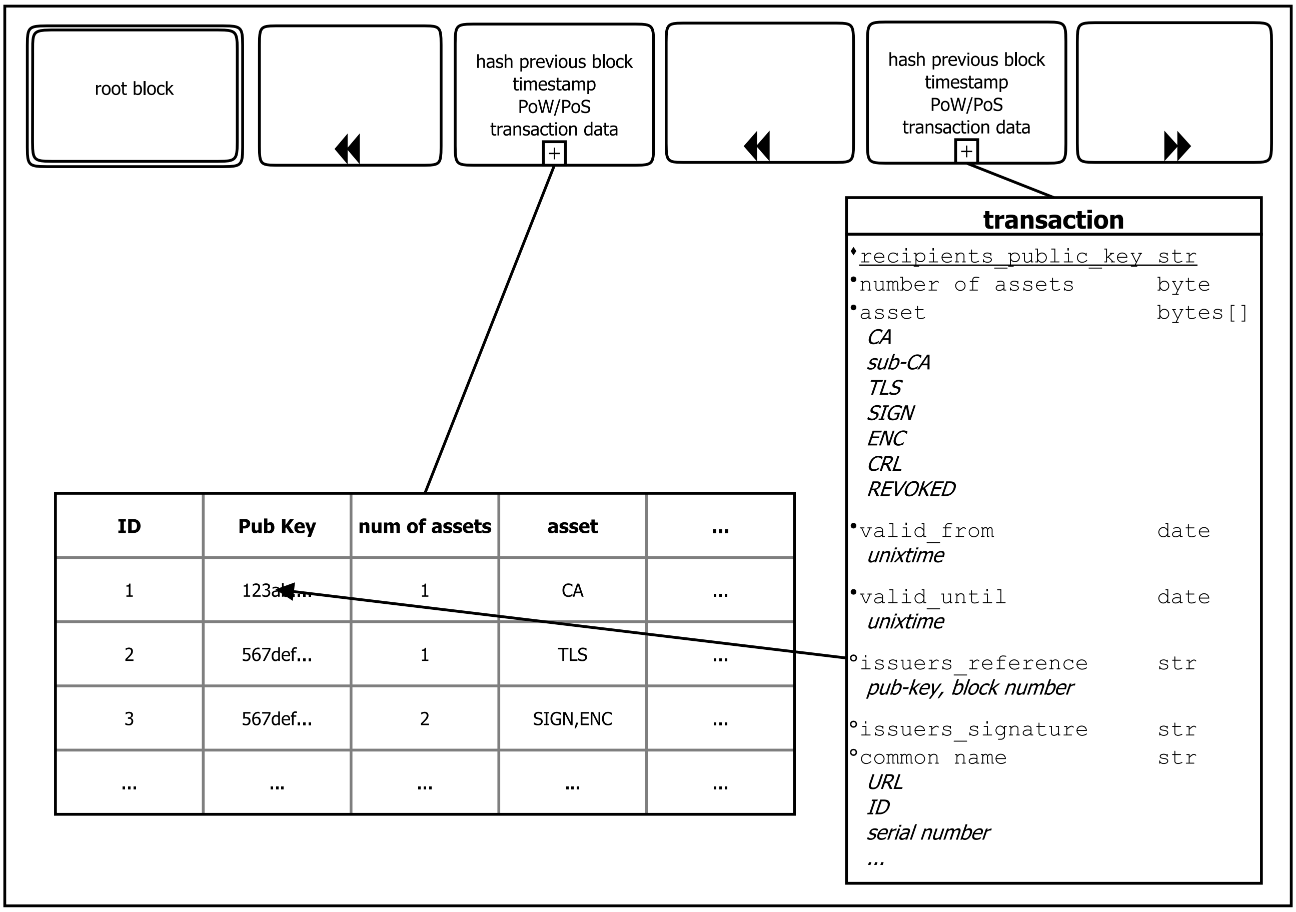
In addition, an observer and a downloader are provided to monitor the integrity of the other virtual machines respectively to update them remotely. It is common in such a microkernel architecture to outsource the operation of hardware interfaces such as persistent storage, network interfaces and other external interfaces into dedicated virtual machines. In Figure 5, this is represented for a gateway with a very high level of protection. With a lower protection requirement, individual virtual machines can be combined, which in turn reduces the hardware requirements for the measuring system.
As a first approach a microkernel of the L4 family was used here, however, due to the paravirtualization used, some adjustments of the drivers are necessary, so that in future work a microkernel will be used, which can use hardware virtualization functions of modern ARMv8 processors, so such modifications won't be needed.

IV. Conclusion and Outlook

The testbed is still work in progress, but main parts like the gateway, sensor simulation and PKI are already implemented. The completion of the testbed will be pursued for the end of the year.

A. Work still to do

The next steps include to develop and evaluate a suitable simulation for a set of controllable devices in the HAN as well as of service technicians in the local network and external market participants in the WAN. The test API can then be finalized and the test scenarios can be implemented.



ID	Pub Key	num of assets	asset	...
1	123ab...	1	CA	...
2	567def...	1	TLS	...
3	567def...	2	SIGN,ENC	...
...	...	...	...	...

Fig. 6. Conceivable transaction scheme for asset granting and id verification using a blockchain.

B. Approaches beyond traditional PKI

The main research focus is to secure the data transfer using alternative approaches to a classical PKI with its limitations. such as Quantum Key Distribution [11] and post-quantum cryptography [12] for encryption, which is secure against quantum computer attacks, and blockchain for authentication without single point of failure.

Main advantages of replacing a traditional PKI by a blockchain are the greater reliability due to the distributed nature of a blockchain, as well as more transparent granting of assets/certificates. An other aspect might be the absence of a root-Key, so there will be no need for redistribution of a root-certificate. As a blockchain is subjected to computational and/or economical power of its node, a public blockchain might not be a suitable solution for a PKI in Legal Metrology, where only certain entities can be trusted to handle grant request with the required fidelity. A setup with a set of nodes limited to authorized participants like in Figure 7 appears to be a more preferable solution.

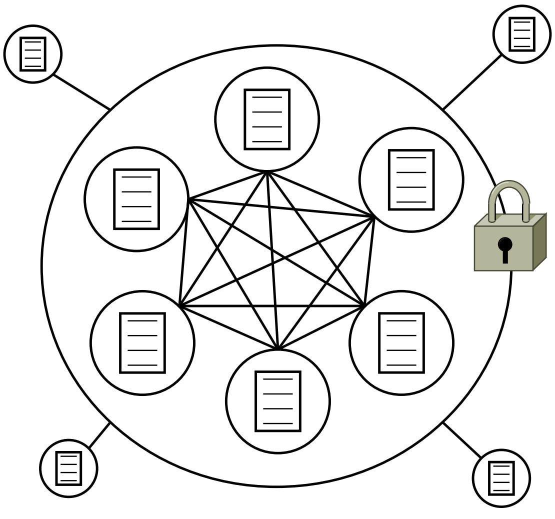


Fig. 7. Node topology for a private blockchain hosting a PKI. Inner nodes are granted to mine/mint transaction blocks outer nodes can only mirror the chain and may request assets to be confirmed by inner nodes

Common blockchains like Bitcoin [13] use a Proof-of-Work to overcome the consensus issue, but this implies huge computational effort and therefore huge energy consumption. Other approaches like Ethereum [16] use more energy-efficient proof of stake, which is usually defined by the possessed amount of an associated currency. This approach also seems to be less than ideal.

A proposed scheme for a blocklayout in a PKI chain is given in Figure 6. We propose to include certificate revocations in the same chain as this will reduce complexity for clients and will give them a starting point for searching for revocations. Also a combination of a blockchain PKI with Physical Unclonable Function (PUF) [18] might be an interesting approach. Interesting and important questions might be:

- How can embedded devices handle the huge amount of data in such a blockchain for authentication?
- Proof-of-Work or an alternative?
- How to integrate PUFs into a blockchain?

C. Further Applications

Further research topics of interest beside approaches beyond traditional PKI focus on new opportunities due to the permanent or at least regular network connection of intelligent measuring systems, such as:

remote verification, remote update: Subsequent investigations will deal in particular with the trustworthy remote partial examination as well as with safe remote software upgrades of intelligent measuring systems. It's expected to develop a legal conform reference method or solution therefore.

smart services: The third object of investigation is research on novel services, which are based on the accumulated data of intelligent measuring systems. For example, methods for predictive maintenance or for identifying attacks on networked measuring systems are conceivable. Here again blockchain approaches for smart contracts might be a suitable solution especially if blockchain technology is already used for PKI.

References

[1] D. Peters, M. Peter, J.-P. Seifert und F. Thiel: A Secure System Architecture for Measuring Instruments in Legal Metrology, published in Computers, Open Access Journal (ISSN 2073-431X), 2015

[2] D. Peters, F. Thiel, M. Peter, J.-P. Seifert, "A Secure Software Framework for Measuring Instruments in Legal Metrology", accepted for IEEE International Instrumentation and Measurement Technology Conference (I2MTC), Pisa, Italy, May 11-14, 2015

[3] N. Leffler and F. Thiel. Im Geschäftsverkehr das richtige Maš. In Schlaglichter der Wirtschaftspolitik, Monatsbericht November, 2013.

[4] BSI TR-03109 Technische Vorgaben für intelligente Messsysteme und deren sicherer Betrieb, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03109/TR03109.pdf?__blob=publicationFile&v=3

[5] Directive 2004/22/EC of the European Parliament and of the Council, March 2004. Official Journal of the European Union.

[6] Directive 2014/32/EU of the European Parliament and of the Council, October 2013. Official Journal of the European Union. doi: 10.3000/19770677.L_2014.096.eng.

[7] Directive 2012/27/EU of the European Parliament and of the Council, February 2014. Official Journal of the European Union. doi: 10.3000/19770677.L_2012.315.eng

[8] General requirements for software controlled measuring instruments, 2008. OIML D 31.

[9] CEN-CENELEC-ETSI Technical Report TR 50572:2011,ICS 33.200; 91.140.01

[10] Oppermann, Alexander and Seifert, Jean-Pierre and Thiel, Florian. 2016. Distributed Metrological Sensors managed by a secure Cloud-Infrastructure, accepted for 18. GMA/ITG Fachtagung, Sensoren und Messsysteme 2016, Nürnberg, 10.-11. Mai, (2016)

[11] P Eraerds, N Walenta, M Legré, N Gisin, and H Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027, 2010.

[12] Daniel J. Bernstein. *Introduction to post-quantum cryptography*, pages 1–14. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[13] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system,âĂİ http://bitcoin.org/bitcoin.pdf.

[14] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi. Certificate validation through public ledgers and blockchains. pages 156–165.

[15] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, and Vladimiro Sassone. Blockchain-based database to ensure data integrity in cloud computing environments. pages 146–155.

[16] Elfriede Sixt. *Ethereum*, pages 189–194. Springer Fachmedien Wiesbaden, Wiesbaden, 2017.

[17] Alexander Chepurnoy. Interactive proof-of-stake. *CoRR*, abs/1601.00275, 2016.

[18] W. Che, F. Saqib, and J. Plusquellic. Puf-based authentication. In *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, pages 337–344, Nov 2015.