International Journal of Electrical, Electronic and Communication Sciences
ISSN: 2517-9438
Vol:12, No:5, 2018

System Security Impact on the Dynamic Characteristics of Measurement Sensors in Smart Grids

Yiyang Su, Jörg Neumann, Jan Wetzlich, Florian Thiel

Abstract—Smart grid is a term used to describe the next generation power grid. New challenges such as integration of renewable and decentralized energy sources, the requirement for continuous grid estimation and optimization, as well as the use of two-way flows of energy have been brought to the power gird. In order to achieve efficient, reliable, sustainable, as well as secure delivery of electric power more and more information and communication technologies are used for the monitoring and the control of power grids. Consequently, the need for cybersecurity is dramatically increased and has converged into several standards which will be presented here. These standards for the smart grid must be designed to satisfy both performance and reliability requirements. An in depth investigation of the effect of retrospectively embedded security in existing grids on it's dynamic behavior is required. Therefore, a retrofitting plan for existing meters is offered, and it's performance in a test low voltage microgrid is investigated. As a result of this, integration of security measures into measurement architectures of smart grids at the design phase is strongly recommended.

Keywords—Cyber security, performance, protocols, security standards, smart grid.

I. Introduction

NOWADAYS, the need to integrate renewable energy sources into power grids has led to a move away from centrally managed passives grids towards active distribution grids where energy is fed into the grid at the low voltage (LV) and middle voltage (MV) levels. However, knowledge of the topology and power flow of such grids is limited. In order to provide the necessary information for grid observation and control, a network of sensors is installed in the gird. The information communication between sensors and monitoring or control systems may be vulnerable to malicious cyber attacks [1]. In the previous project JRP ENG04 SmartGrid [2] the LV grid elements were the focus of the analysis. The problems in each grid region are very similar. Electrical grids consist of critical elements and components which need to be protected against manipulations and threats. An analysis of grid architectures was performed by the authors, during which all components, actors, roles, methods, effects/influences, and interactions were taken into account. The main result was the realization that manipulations of many apparently insignificant components probably have the same influence on security as the manipulation of only one significant component. Therefore, any cryptographic infrastructure has to take into account that many single elements of the same kind (e.g. simple measurement sensors, state indicators, etc.) have the same influence on the grid security as a complex one (e.g. data acquisition systems, grid control center). Furthermore, a security concept was developed by the authors. In general, this concept proposed to apply data authenticity and integrity on the application layer between end-to-end communicating entities in the LV grids.

Y. Su, J. Neumann, J. Wetzlich and F. Thiel are with Physikalisch-Technische Bundesanstalt (PTB), Berlin, Germany (e-mail: yiyang.su@ptb.de, joerg.neumann@ptb.de, jan.wetzlich@ptb.de, florian.thiel@ptb.de).

However, in metrology applications other security objectives such as prevention of eavesdropping, playback and spoofing in LV grids should also be accounted. Additionally, some critical control signal and measurement data should be protected from repudiation. This can ensure that the data can be audited in the future. Furthermore, integration of security measures into measurement architectures of LV girds will affect the end-to-end information transmission behavior between different grid entities. This may even impact the performance of the grids. Additionally, dynamic control systems for smart grids are becoming a focus of ongoing research. The observation and control of LV grids require highly dynamic measurements. Accurate information about latency and reaction time for each end-to-end-communication relation is one of the most important issues for grid stability. The impact of system security on the dynamic characteristics of measurement sensors will be assessed within this paper.

The remainder of this paper is organized as follows. In Section II different standards and guidances are analyzed in order to find appropriate application layer protocols to realize the security concept. Section III provides detailed information on the implementation of our experimental measurement systems. Section IV presents two test circumstances and their numerical results. Section V introduces some of the research that is related to our work. Finally, Section VI concludes the paper and describes the future challenges.

II. Appropriate Standards for Adaption

In this section potential standards, whose application layer protocols can be used over the TCP/IP protocol stack, are investigated. In addition, data security specification of these protocols are analyzed whether they can provide data authenticity, integrity, as well as non-repudiation on application layer between end-to-end entities.

A. IEC 61850-8-1, IEC 62351-3/4

IEC 61850-8-1 [4] provides a mapping of ACSI (Abstract Communication Service Interface, IEC 61850-7-2) to MMS

(Manufacturing Message Specification, ISO 9506) and ISO/IEC 8802-3 frame. The MMS services and protocol are specified to operate full TCP compliant communication profiles. However, this comes without its own security measures. The security of IEC 61850-8-1 relies on IEC 62351-3 and -4.

IEC 62351-3 defines how to secure TCP/IP-based protocols through constraints on the specification of the messages, procedures, and algorithms of Transport Layer Security (TLS) [3]. Authenticity and confidentiality can only be achieved by using appropriate cipher suites for TLS and also conjunction the states of applied certificates with TLS.

IEC 62351-4 divides the security mechanism into two profiles: T-Profile addresses the protection of information transmissions over TCP/IP through TLS (referring to IEC 62351-3) while A-Profile addresses the protection for the application layer. The latter only provides authentication during the connection establishment using MMS association.

B. IEC 62056-5-3, Green Book

IEC 62056-5-3 [5] specifies the DLMS/COSEM application layer in terms of structure, services and protocols for COSEM clients and servers, and defines how to use the DLMS/COSEM application layer in various communication profiles. Additionally, this part also addresses the security for data access and transport. The data access security provides three authentication mechanisms: Lowest Level, Low Level, and High Level Security authentication. Only by using High Level Security authentication the client and the server can identify each other. The data transport security describes an authenticated encryption for DLMS Application Layer Protocol Data Unit (APDU) using cipher suite AES-GCM. This cipher suite provides authenticity and integrity.

Green Book (Ed. 8.1) [6] is published by the DLMS User Association (UA). Several new features regarding functionality, efficiency, and security are added while keeping full backwards compatibility. Besides above mentioned security mechanisms, additional security protection types are added into the data transport security. In particulate, the new type General-Signing that applies asymmetric methods to provide authenticity, integrity and non-repudiation for DLMS APDUs is added. This type comprises:

- Tag: A unique value is given to identify the type of APDU.
- Additional fields: These contains transaction-id, sender, recipient, date-time, and a flexible field can hold additional information concerning protection.
- Content: It is used to store the DLMS APDU and needs to be protected.
- Signature: It is calculated based on the additional fields and the content and provides authentication as well as protection against manipulation of the data.

C. IEC 62056-62, Blue Book, SELMA

IEC 62056-63 and Blue Book [8] published by DLMS UA specifies the COSEM interface classes. An object oriented model of a meter is provided. The information of an object is organized in attributes. They describe the characteristics of an object by means of attribute values. The first attribute in any object is the logical_name, which is used as identification of the object based on Object Identification System (OBIS) code. In order to either examine or modify the values of the attributes a number of getter and setter methods are provided by an object. Objects that share common characteristics are generalized as interface class. In SELMA [9] class interfaces containing signed attributes are provided such as Signed Daily Profiles, Signed Captured Objects, and Signed General Data. For example, the class Signed Data contains an attribute named signed_data. This attribute comprises meter related information, measurement data, and authentication parameters, which contains a time stamp, certificate identification, and a digital signature. The ideal is that measurement data is always combined with a digital signature such that the data's authenticity as well as it's integrity can always be verified.

D. Signing HTTP Messages

The Hypertext Transfer Protocol (HTTP) is defined by the W3C. It is a stateless application level request/response protocol with extensible semantics as well as self-descriptive message payloads that is suitable for flexible interaction with network based hypertext information systems. It is widely used on the Internet.

At present, Signing HTTP Messages [7] is still a work in progress document of the Internet Engineering Task Force (IETF). This document specifies an additional HTTP Signature Header mechanism that can be used to authenticate the sender of a message and ensure that particular headers have not been modified during transmission. This header comprises:

- keyId: An opaque string that can be used to look up the component required to validate the signature.
- algorithm: A specification of the digital signature algorithm that is used when generating the signature.
- headers (optional): This parameter is used to specify the list of HTTP headers. If this parameter is not specified, implementations must operate as if the 'Date' header is provided.
- signature: The signature of the message. It is generated using an asymmetric method and encoded to base64 string.

E. XML Security

The Extensible Markup Language (XML) is designed to store and transport data, as well as to be flexible and self-descriptive. It specifies a set of rules to encode the data that is readable for human and machine. The plain text format provides a software- and hardware-independent way of processing data.

The W3C states that preventing the manipulation of data in XML format requires integrity, authentication, and privacy. XML Encryption and XML Signature are provided to address these security objectives. XML Encryption allows the encryption of any data with symmetric and asymmetric algorithms. The cipher data may be contained or identified (via a URI reference) by an XML Encryption EncryptedData

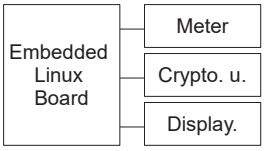

Fig. 1 Retrofitting a meter

element. XML Signature uses asymmetric methods to provide information integrity and non-repudiation. The generated signature can be enveloped within the same XML document or detached over data external.

III. Experimental Implementation

Based on the analysis above, DLMS/COSEM, SELMA, Signing HTTP Messages, and XML Security are suitable for the implementation to provided the end-to-end security. A secure communication system is proposed as that the TLS is used to provide authentication between the DAS and meter, as well as confidentiality for exchanged data. On the application layer the exchanged data such as command and measurement data will be signed with digital signatures by the DAS and meter using their own private key, respectively. The integrity and non-repudiation of the application data can be provided on this layer. A PKI can be used to issue certificates and provide certificate status.

Such system has been implemented in our research, which is used to investigate the impact of the system security on the practical performance. To realize this system, firstly a digital power meter is retrofitted and combined with an embedded Linux board. Then, a DLMS/COSEM server application and a web service server application on the Linux board are implemented. Also two appropriate DAS applications are implemented on a computer respectively. Finally, a X.509 PKI to issue certificates and offer Online Certificate Status Protocol (OCSP) for providing the revocation status of applied certificates is established. Detailed implementation information is given in the following sections.

A. Retrofitted Meter

Most of the existing meters have none of the required security measures. A retrofitting plan for a meter is proposed as shown in Fig. 1. The meter is combined with an embedded Linux board. The cryptographic unit offers asymmetric cryptographic algorithm to generate digital signatures for security features on the application layer. The display is used for local monitoring.

For our experimental implementation, two different embedded Linux boards are selected:

- Hardware A: Raspberry Pi B+, CPU: ARM1176JZF-S @ 700 MHz single-core, Memory: 512MB;
- Hardware B: CubieTruck, CPU: ARM Cortex-A7 @ 1 GHz dual-core, Memory: 2GB.

Furthermore, the power meter PAC3200 is selected, which can communicate with the boards via Modbus TCP and consists of a built-in display. For the cryptographic unit we use the smart card Infineon SLE66 which provides Elliptic Curve Digital Signature Algorithm (ECDSA) with curve parameter P-192. Multiple meters are retrofitted for laboratory and field testing.

B. Implementation of DLMS/COSEM

An experimental version of DLMS/COSEM logical name referencing system is implemented by using C. During the implementation, different electrical data measured by the power meter PAC3200 are mapped into unique OBIS codes. Two COSEM interface classes are used to represent the measurement data: one is the interface class Register, which is not protected by any security features (defined in [8]), another is the interface class Signed General Data, which signs measurement data with a digital signature (defined in [9]). The actual digital signature is generated by using the smart card. In order to compare the performance of the digital signing process using the smart card, an additional a software signing function (ECDSA, curve parameter P-256) is implemented by using the OpenSSL library version 1.0.2h [12]. Finally, xDLMS APDUs such as Get-Request, Get-Response, Set-Request, Set-Response, and General-Signing are implemented. These can be used to simulate the following use cases:

I Non-authenticatable Get-Request and non-authenticatable Get-Response: The DAS sends a Get-Request APDU to request the attribute value of one Register object. Then, the meter returns the attribute within a Get-Response APDU.

II Authenticatable Get-Request and authenticatable measurement data: The DAS sends a General-Signing APDU, which wraps a Get-Request APDU that requests the attribute signed_data of one Signed General Data object. Then the meter verifies the signature of the General-Signing APDU. If the signature is valid, the meter returns the attribute within a Get-Response APDU. If the signature is invalid, the meter returns nothing.

C. Implementation of the Web Service

Considering the recommendation of [13], a RESTful web service is established by using web.py framework [14]. In this web service, the access to COSEM objects is mapped to RESTful verbs and Uniform Resource Identifiers (URIs). Furthermore, the COSEM data type and data structure is mapped to XML. As before, signatures can be generated by using the smart card or via software. Similar use cases as described in the previous section can also be simulated with this web service.

I Non-authenticatable HTTP GET and non-authenticatable XML file: The DAS sends a HTTP GET without the Signature header field to request the attribute value of one Register object. Then, the meter returns the attribute within a XML file without XML Signature protection.

II Authenticatable HTTP GET and authenticatable XML file: The DAS sends a HTTP GET with the Signature header field to request the attribute value of one Register object. Then, the meter returns the attribute within a XML file with XML Signature protection.

TABLE I
APPLIED CIPHER SUITES

Key exchange	Signature	Encryption	Hash
(C1)TLS_ECDHE_	ECDSA_	WITH_AES_128_CBC_	SHA256
(C2)TLS_ECDHE_	ECDSA_	WITH_AES_256_CBC_	SHA384
(C3)TLS_ECDHE_	ECDSA_	WITH_AES_128_GCM_	SHA256
(C4)TLS_ECDHE_	ECDSA_	WITH_AES_256_GCM_	SHA384

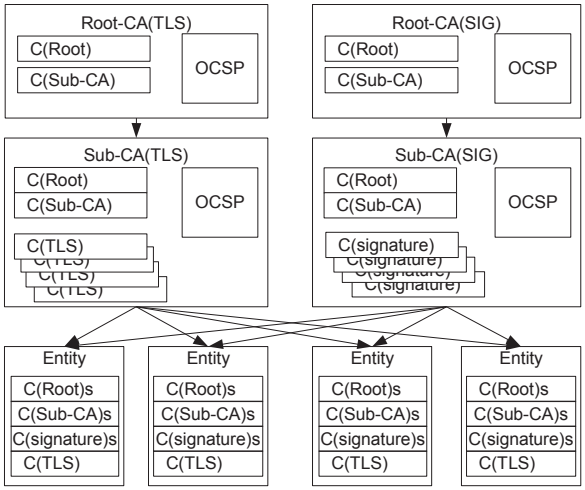

Fig. 2 Architecture of the PKI

D. Implementation of TLS

The OpenSSL library (1.0.2h) is used to implement TLS1.2. Considering forward security, authentication, hash function, encryption, Message Authentication Code (MAC) and current recommendations from different institutes the selected cipher suites are displayed in Table I. The TLS handshake process in our experiment has been configured as that the DAS and meter must identify each other. In addition, after a successful handshake the revocation status of applied certificates must be checked.

E. Implementation of PKI

The EJBCA [10] is chosen as CA software to provide various PKI services. The architecture of the PKI is shown in Fig. 2.

The PKI consists of two separate X.509 Root-CAs as the most trustworthy instance, two X.509 Sub-CAs that issue certificates for end entities. The DAS and meter store their own certificates for TLS respectively. During a TLS handshake the DAS sends its certificate to the meter and vice versa. In contrast to the certificates used for TLS, the certificates used for the signatures, which contain the public key for verifying the signature of the received data on the application layer, will not be exchanged between the meter and DAS. More precisely, the meter's signature certificate is installed in the DAS and vice versa. Considering the proposition of [11] the applied signature algorithms and curve parameters for CAs are displayed in Table II.

TABLE II
SIGNATURE ALGORITHMS AND CURVE PARAMETERS FOR CAS

CA	Signature algorithm	EC parameter
Root-CA	ecdsa-with-SHA384	P-384
Sub-CAs	ecdsa-with-SHA256	P-256

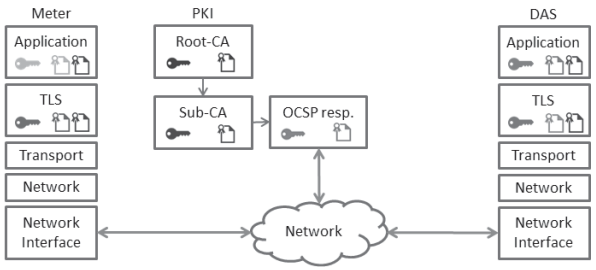

Fig. 3 Communication network for meter, DAS, and PKI

TABLE III
LATENCY OF CONNECTION ESTABLISHMENT IN LABORATORY

Process	Symbol	Latency HW A [ms]	Latency HW B [ms]
TCP HS	t_{TCP_hs}	1.1	0.9
TLS HS P-256	t_{TLS_hs}	125.6	68.8
TLS HS P-384	—"—	157.3	90.7
TLS HS P-521	—"—	221.8	128.5
OCSP (meter)	t_{OCSP_m}	92.2	38.6
OCSP (DAS)	t_{OCSP_c}	23.9	23.9
TLS SR	t_{TLS_sr}	21.4	6.7

IV. EXPERIMENTAL RESULT AND EVALUATION

One of the main aims of our research is to evaluate the performance of the implemented measurement system and to examine whether by applying secure measures the system can still achieve the performance requirements of the smart grid or not. The test was performed in two circumstances: in the laboratory and in the field. A simplified communication network for meter, DAS, and PKI is shown in Fig. 3. Detailed information are stated in the following sections.

A. Laboratory Testing

In the laboratory testing the meters, DAS and OCSP responder can communicate with each other in a local network. First the latency of a TCP handshake is measured. Then the latency of al TLS handshake is measured. Different temporal EC domain parameters such as P-256, P-384, as well as P-521 are applied for the calculation of DH parameters during the TLS handshake to access the performance. Furthermore, The full verification of the TLS certificate chain is set. Additionally, the latency of the OCSP response is measured from the DAS and also from the meter. In this test, all related certificates are valid. Then the latency of session resumption (SR) is measured, which uses the secret information from the previous session to avoid a full TLS handshake. The test was performed with Hardware A and Hardware B. The test results are displayed in Table III.

Without applying TLS, the latency of a TCP Handshake is 1.1 ms for Hardware A and 0.9 ms for Hardware B. When

TABLE IV
LATENCY OF ONE REQUEST WITH A DLMS/COSEM SERVER IN THE LABORATORY

Signature	Cipher	Latency HW A [ms]	Latency HW B [ms]
None	None	4.9	4.6
SC P-192	C1	271.2	251.4
—"—	C2	272.1	253.6
—"—	C3	270.6	251.3
—"—	C4	271.3	251.1
SW P-256	C1	38.8	22.2
—"—	C2	38.2	26.3
—"—	C3	37.1	23.8
—"—	C4	37.7	23.1

using the TLS handshake and OCSP certificate status checking for the connection establishment, the latency for preparing a secure communication between the DAS and meter can be calculated according to (1).

$$t_{sum} = t_{TCP\_hs} + t_{TLS\_hs} + MAX(t_{OCSP\_m}, t_{OCSP\_c}) \quad (1)$$

Hence, at least 239.9 ms and 118.9 ms are required to establish a secure connection with Hardware A and Hardware B, respectively. Similarly, when While applying TLS session resumption for rebuilding the secure communication channel between the DAS and meter, the required time can be calculated according to (2).

$$t_{sum} = t_{TCP\_hs} + t_{TLS\_sr} \quad (2)$$

Hence, it requires 22.5 ms to rebuild the connection with Hardware A ms and 7.6 ms with Hardware B.

Next, the data communication for the use cases described in Sectioin III-B with a DLMS/COSEM server is investigated. Without using TLS and signatures, the latency of a Get-Request is 4.9 ms for Hardware A and 4.6 ms for Hardware B. When applying cipher suite _AES_128_CBC_SHA256 (C1) for encryption and the smart card for signing Get-Response APDU in the meter, the latency for the Get-Request is 271.2 ms for Hardware A and 251.4 ms for Hardware B. However, when applying TLS with the same cipher suite and ECDSA software (P-256) for signing the Get-Response in the meter, the latency for the Get-Request service is 38.8 ms for Hardware A and 22.2 ms for Hardware B. Further test results using other cipher suites are displayed in Table IV.

At last the data communication for the use cases described in Section III-C using a web service is investigated. The results are displayed in Table V. When comparing the results for these tests, the computing power of the hardware strongly influences the performance in terms of latency of the TLS handshake, the OCSP certificate status check, the data encryption and decryption, as well as the signature generation and verification.

B. Field Testing

In the field testing, the meters are installed in the test micro grid at the EFZN [15] in Goslar and the DAS as well as the OCSP responder are installed at the PTB in Berlin such that

TABLE V
LATENCY OF ONE REQUEST WITH A WEB SERVICE IN THE LABORATORY

Signature	Cipher	Latency HW A [ms]	Latency HW B [ms]
None	None	480.5	127.9
SC P-192	C1	766.4	389.0
—"—	C2	768.7	393.4
—"—	C3	766.3	392.4
—"—	C4	777.6	391.7
SW P-256	C1	514.1	149.7
—"—	C2	516.8	150.5
—"—	C3	515.3	150.6
—"—	C4	516.5	149.8

TABLE VI
LATENCY OF CONNECTION ESTABLISHMENT IN THE FIELD

Process	Symbol	Latency HW A [ms]	Latency HW B [ms]
TCP HS	t_{TCP_hs}	12.3	11.4
TLS HS P-256	t_{TLS_hs}	143.7	83.7
TLS HS P-384	—"—	178.4	107.4
TLS HS P-521	—"—	248.2	150.3
OCSP (meter)	t_{OCSP_m}	103.4	43.2
OCSP (DAS)	t_{OCSP_c}	23.9	23.9
TLS SR	t_{TLS_sr}	25.6	9.7

TABLE VII
LATENCY OF ONE REQUEST WITH A DLMS/COSEM SERVER IN THE FIELD

Signature	Cipher	Latency HW A [ms]	Latency HW B [ms]
None	None	14.2	13.8
SC P-192	C1	281.6	259.7
—"—	C2	281.3	261.2
—"—	C3	279.3	259.6
—"—	C4	280.3	260.2
SW P-256	C1	45.9	27.7
—"—	C2	45.2	31.7
—"—	C3	46.7	28.8
—"—	C4	44.7	28.0

they can communicate with each other via Internet. The same tests as during laboratory testing are applied. The latency of the connection establishment is displayed in Table VI. As can be seen from the results, the latency for most processes is increased during the field testing due to the fact that all data has to be routed through the Internet. The only exception is the latency of the ocsp request from DAS which remains same. This is due to the fact that the OCSP responder and the DAS are still in the same local network. Overall, the latency to establish a secure connection is increased to 259.4 ms for Hardware A and 138.3 ms for Hardware B. Finally, the latency for the request using a DLMS/COSEM server or a web service is also increased during the field testing. The corresponding values can be found in in Table VII and VIII, respectively.

C. Evaluation and Discussion

Different smart meter applications require various sampling time and tolerate a certain latency. According to [16] applications such as consumption awareness and cost estimation defines maximum sampling time 15 min and

TABLE VIII
LATENCY OF ONE REQUEST WITH A WEB SERVICE IN THE FIELD

Signature	Cipher	Latency HW A [ms]	Latency HW B [ms]
None	None	492.3	136.4
SC P-192	C1	778.3	400.3
—"—	C2	780.1	402.8
—"—	C3	779.6	401.4
—"—	C4	778.3	401.8
SW P-256	C1	526.9	157.3
—"—	C2	528.3	158.2
—"—	C3	527.4	159.0
—"—	C4	527.6	157.8

maximum acceptable latency 1 h, realtime power curve visualization defines maximum sampling time 1 s and maximum acceptable latency 1 s, etc. The required the sampling time of other applications is from 1 s to 15 min, and for the acceptable latency it is from 1 s to 1 h. Our results show that, using the current testing scenarios, available hardware, selected cipher suites, and proposed secure measures, the acceptable latency of data acquisition can be satisfied.

Forward-secrecy cipher suites by conducting an ephemeral elliptic curve Diffie-Hellman (ECDHE) key exchange as reported in Table I are used in our experiment. A distinct ECDH key is generated by every handshake. The long-term private keys of the meter and DAS are only used for authentication. But in practice the connections between the meter and DAS potentially have longer, or even "permanent" durations. Without completing a new full handshake or reusing a previous session it will weaken the forward security benefit of these cipher suites. A full TLS handshake with key exchange and both side authentication must be periodically performed in order to provide the forward security. During the TLS handshake the certificates can also be checked for their revocation status by using OCSP. The full TLS Handshake and checking for certificate revocation status are all time consuming. If this happens at a non-appropriate time may undermine the performance of the data transfer between meter and DAS. A prior risk assessment and data transfer behaviors must be analyzed in order to provide suitable time schedules for the re-handshake.

V. RELATED WORK

For smart grid communication technology, there are several papers that provide a comprehensive survey of communication protocols in smart metering, e.g. [17] and [18]. The performance evaluation done in [19] points out that it is feasible to build a smart meter using a low cost, low performance open source platform with asymmetric cryptography features (16 seconds for delivering a measurement). Then, authors in [20] conduct an experiment to measure the total time to transfer MMS Request between clients and servers while using TLS. The results show that the performance constraints specified by IEC 61850 can be satisfied by using their hardware and cipher suites. Finally, authors in [21] state a lighter version authentication by using HMAC.

VI. CONCLUSIONS

The integration of security measures into an existing grid could influence it's dynamic behavior.Therefore, in our research we implemented a DLMS/COSEM and a web service measurement system incorporating signatures and TLS as security measures and evaluated the performance of the systems. The results show that the current acceptable latency for the data acquisition can be satisfied if a proper implementation of the security measures is chosen. Hence, we have offered a retrofitting plan, accordingly. However, additional security measures such as periodic session renegotiation and certificate revocation status checking should be considered to maintain a high level of security. For future research, it may be worthwhile to incorporate a larger sensor network into an actual power grid in order to evaluate the performance under more harsh conditions.

REFERENCES

[1] The Smart Grid Interoperability Panel - Cyber Security Working Group, Guidelines for Smart Grid Cyber Security, NISTIR 7628 (2010).
[2] Final Publishable JRP Report, ENG04, SMARTGRID, Metrology for Smart Electrical Grids, EURAMET, 2015.
[3] RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, T. Dierks, E. Rescorla, 2008.
[4] IEC 61850, Part 8-1, Specific Communication Service Mapping (SCSM) - Mapping to MMS (ISO 9506-1 and ISO 9506-2) and ISO/IEC 8802-3, 2004.
[5] IEC 62056, part 5-3, Electricity metering data exchange - The DLMS/COSEM suite - DLMS/COSEM application layer, 2016.
[6] Green Book Edition 8.1, DLMS/COSEM - Architecture and Protocols, DLMS User Association, 2015.
[7] M. Cavage, M. Sporny, Signing HTTP Messages, draft-cavage-http-signature-06, https://web-payments.org/specs/source/http-signatures/, last access April 2017.
[8] Blue Book Edition 10, COSEM - Identification System and Interface Classes, DLMS User Association, 2015.
[9] N. Zisky. et al, PTB-Bericht IT-12 Das SELMA-Projekt: Konzept, Modelle, Verfahren, 2005.
[10] EJBCA - Open Source PKI Certificate Authority, last ccess April 2017.
[11] Technische Richtlinie BSI TR-03116, Kryptographsche Vorgaben für Projekt der Bundesregierung, Teil 3: Intelligente Messsysteme, 2016.
[12] OpenSSL Cryptography and SSL/TLS Toolkit, https://www.openssl.org/.
[13] Technische Richtline BSI TR-03109-1, Anforderungen an die Interoperabilität der Kommunikationseinheit eines intelligenten Messsystems, 2013.
[14] Web framework for Python, http://webpy.org/.
[15] Energy Research Centre of Niedersachsen, https://www.efzn.de/.
[16] M. Kuzlu, M. Pipattanasomporn, et al, Communication network requirements for major smart grid applications in HAN, NAN and WAN, Computer Networks, 67, 74-88, 2014.
[17] Feuerhahn, Stefan, et al. "Comparison of the communication protocols DLMS/COSEM, SML and IEC 61850 for smart metering applications." Smart Grid Communications (SmartGridComm), 2011 IEEE International Conference on. IEEE, 2011.
[18] Hoffmann, Stefan G., Robin Massink, and Gerd Bumiller. "New security features in DLMS/COSEM- A comparison to the smart meter gateway." Innovative Smart Grid Technologies-Asia (ISGT ASIA), 2015 IEEE. IEEE, 2015.
[19] G. Kalns, S. Nadjm-Tehrani, et al, Trading off latency against security in open energy metering infrastructures. Proceedings of The 4th International Symposium for Industrial Control Systems and SCADA Cyber Security (ICS-CSR). 2016.
[20] KHALED, Omar, et al. Analysis of Secure TCP/IP Profile in 61850 Based Substation Automation System for Smart Grids. International Journal of Distributed Sensor Networks, 2016, 12. Jg., Nr. 4, S. 5793183.
[21] Anantharaman, Prashant, et al. "I Am Joe's Fridge: Scalable Identity in the Internet of Things. " Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 2016 IEEE International Conference on. IEEE, 2016.