Secure Integration of DER into Smart Energy Grid and Smart Market

Steffen Fries, Rainer Falk
Corporate Technology
Siemens AG
Munich, Germany
e-mail: {steffen.fries|rainer.falk}@siemens.com

Henry Dawidczak, Thierry Dufaure
Energy Management
Siemens AG
Berlin, Germany
e-mail: {henry.dawidczak|thierry.dufaure}@siemens.com

Abstract—**The integration of decentralized energy resources and loads into the smart energy grid and into smart market is gaining more importance to cope with the increasing demand on energy while reducing load on the energy transmission network that is not affected by energy exchange between local generation and consumption. Characteristic for the involved control systems is the data exchange between intelligent electronic devices (IEDs), which are used to monitor and control the operation. For the integration Decentralized Energy Resources (DER), these IEDs provide the data for obtaining a system view of connected decentralized energy resources – DER. Based on this system view a set of DER, realizing a Virtual Power Plant (VPP), can be managed reliably. In substation automation, the standard IEC 61850 is used to enable communication between similar IEDs to control the central energy generation and distribution. This standard being enhanced with features and mappings to enable its application also for DER. One problem to be solved here is the integration of IEDs residing on a customer network, most likely to be operated behind Firewalls and Network Address Translation (NAT). The solution required must ensure end-to-end secured communication between DER and control center also over public networks. Here, adequate IT security measures are a necessary prerequisite to prevent intentional manipulations, affecting the reliable operation of the energy grid. This paper investigates into currently available security measures and utilizes them to propose a secure communication architecture for DER integration. The described solution is currently proposed within the International Electrotechnical Commission (IEC) for enhancements of the energy automation communication standard IEC 61850. Besides that, this paper also investigates into open issues related to the secure integration of DER.**

Keywords–security; device authentication; firewall; decentralized energy resource, substation automation; smart grid; smart Market, IEC 61850, IEC 60870-5, IEC 62351, XMPP

I. INTRODUCTION

DER, i.e., renewable energy sources like solar cells or wind power, are becoming increasingly important to generate environmentally sustainable energy and thus to reduce greenhouse gases leading to global warming. Integrating DER into the current energy distribution network poses great challenges for energy automation: DER need to be monitored and controlled to a similar level as centralized energy generation in power plants. Widely distributed communication networks are required for exchanging control communication. Multiple DER may also be aggregated on a higher architecture level to form a so-called virtual power plant. Such a virtual power plant can be viewed from the overall energy automation system in a similar way as a common centralized power plant with respect to energy generation capacity. But due to its decentralized nature, the demands on automation and communication necessary to control the virtual power plant are much more challenging.

Furthermore, the introduction of controllable loads on residential level requires enhancements to the energy automation communication infrastructure as used today. Clearly, secure communication between a control station and DER equipment or energy loads of users as well as with decentralized field equipment must be addressed. Standard communication technologies based on IEC 61850 [1], which are used today for substation automation, cannot directly be applied and need enhancements. An abstract view of the setup used as base for the security discussion is shown in Figure 1.

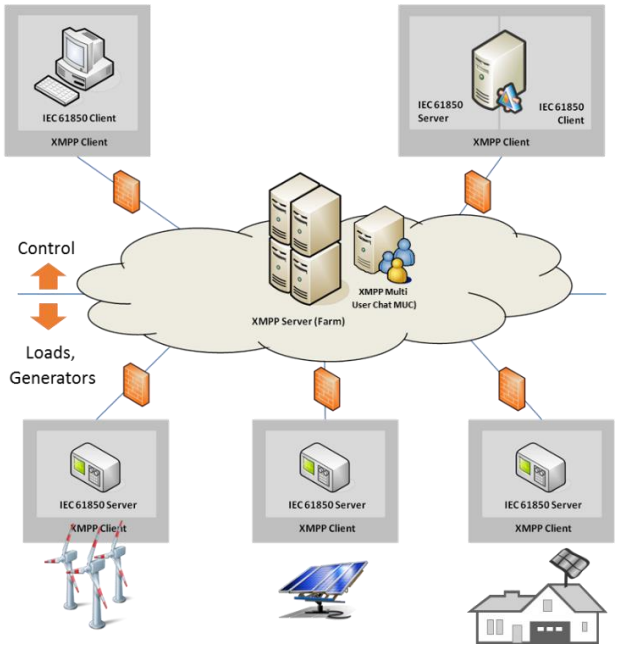

Figure 1. DER Integration based on IEC 61850 over XMPP

 ISBN: 978-1-61208-414-5

Figure 1 depicts the integration of DERs into the Smart Grid and Smart Market. The lower part of the figure shows the distributed generators and loads, which shall be managed by the control function shown in the upper part. The control function may be located at a Distribution Network Operator (DNO), a VPP operator, or a smart energy market operator. Also shown are typical security infrastructure elements – Firewalls – which shield the different sub-networks. Communication is realized by applying IEC 61850 transmitted over the eXtensible Message and Presence Protocol (XMPP) [1][2]. XMPP is a well-known protocol standardized in the Internet Engineering Task Force (IETF) as RFC 6120 and is used for instance in chat applications. It supports Firewall and NAT traversal and also device registration and discovery. As XMPP, IEC 61850 itself is a client-server protocol. In the scenario shown in Figure 1, the IEC 61850 server part resides at the DER sides. Thus, a direct connection to control the DER may not be possible due to blocked inbound connections at the Firewall of the network the DER is connected to. This is the part where XMPP is utilized, as the XMPP client resides on the DER and starts establishing a connection with the XMPP server, which can used to facilitate the IEC 61850 communication.

The remaining part of the paper is organized as following: Section II provides an introduction to IEC 61850 and also investigates into missing parts for the integration of DER into Smart Grids. Section III analysis the security requirements and also potential security measures, by applying existing technology as far as possible. Section IV discusses the resulting security approach, which is also proposed for standardization. Section V concludes the paper and provides an outlook for further work.

Note that this paper targets the identification of existing security means as well as existing gaps for the concept of secure DER integration. Implementations as proof of concept are not finished, yet.

II. IEC 61850 OVERVIEW

A. The IEC 61850 principles

While the first edition of the IEC 61850 series [1], published in 2003 focused on standardizing communication between applications within a Substation Automation Domain, the second edition published in 2010 extends its domain of application up to the Power Utility Automation System. The IEC 61850 series specifies:

- An Abstract Communication Service Interface (ACSI),
- A semantic model based on an object oriented architecture,
- Specific Communication Service Mappings (SCSM),
- A project engineering workflow including a configuration description language (SCL) based on the XML language.

Using the IEC 61850 philosophy, i.e., decoupling the IEC 61850 object model and associated services from the communication technologies allows the standard to be technology independent, that is, specifying new technologies when a set of new requirements is being processed by the standardization body without modifying the system architecture. Services in IEC 61850 include:

- Client and Server communication within the scope of a Two Party Application Association (or session), for discovering, controlling and monitoring objects implemented in the device model,
- Peer to peer communication within the scope of a Multicast Application Association, for providing a unidirectional information exchange from one source to one or many destination.

The IEC 61850-8-1 SCSM part has specified the mapping of IEC 61850 object model and associated services to MMS (ISO 9506 series [3]). While IEC 61850-8-1 SCSM has proven to be a very efficient communication technology within the substation, i.e., within a private network, new challenges appear with the integration of the DERs. A current effort in the standardization has gathered the requirements for an IEC 61850 SCSM to Web Protocols.

Public network/infrastructure are neither administered by the DER owners nor by the control function operator; the use of public network represents therefore a major change in comparison to the way IEC 61850 Systems and communication have been deployed within the substation.

The gathered requirements [4] show also that the response times are less critical than they are in the substation environment. Both the number of devices connected to the Smart Grid as well as the dynamic changes of the system (continuous integration of new resources) encourage the use of a technology that supports the volatility of the system.

The decision criteria used in the standardization committee lead to elect XMPP [5] technology as a network layer in the SCSM.

B. The XMPP principles

XMPP is a communication protocol enabling two entities (XMPP clients) to exchange pieces of XML data called stanzas. As shown in Fig.1, both the DERs (IEC 61850 servers) and the VPP or DNO control center (IEC 61850 client) are then exposed as XMPP clients. They are not directly connected together but can exchange XML messages over the XMPP server(s) they are connected to. Each XMPP client is responsible for initiating a TCP/IP connection to the XMPP server of the domain the XMPP client belongs to. The XMPP servers are located in the WAN and their location can either be statically configured in the DERs or can be discovered by the DERs via DNS-SRV records [6].

Since DERs will be located behind (most of the time unmanaged) firewalls, the XMPP servers cannot reach/connect to them (requirement – blocked inbound connection); nevertheless DERs can reach/connect to the XMPP server of their domain over the stateful firewall of their infrastructure.

 ISBN: 978-1-61208-414-5

As soon as the TCP/IP connection to its XMPP server is established, each XMPP client starts a bi-directional XML stream with its XMPP server.

Each XMPP client has a unique system identifier, a so-called JIDs, whose format is quite similar to the well-known mail addresses format: entity@domain.tld.

Communication between XMPP clients occurs over the XML streams, each client has negotiated with their XMPP server, the server acting then as router forwarding the message exchange.

The XMPP series define three different XML message formats called stanza. Similar to the mail message, each stanza contains an attribute "from" (from="JID of the source of the message") and an attribute "to" (to="JID of the destination of the message"). The message formats are:

- of type <iq> (dedicated for request/response exchange - solicited service),
- of type <message> (dedicated for push-exchange - unsolicited communication),
- or of type <presence> (dedicated for presence announcement).

C. Mapping of IEC 61850 to XMPP

The current draft of IEC 61850-8-2 foresees XER encoding of MMS using following mapping of the services to the XMPP stanza:

- request/reponse services will be mapped to the <iq> stanza (e.g., initiate-RequestPDU, initiate-ResponsePDU, writeRequestPDU, …)
- reporting services will be mapped to the unsolicited <message> stanza (e.g., informationReportPDU, …).

Through the mapping of MMS to XMPP the MMS defined security measures are directly applicable as outlined in the next section.

The XMPP standard provides protocol extensions (so called XEPs [7]), i.e., optional technical specifications to solve additional communication requirements. The developments of the specifications are hosted and coordinated by the XMPP foundation [8]. For example, the XEP-0045 specifies the Multi-User Chat (MUC) environment, with which XMPP clients can exchange messages in the context of an administrated room. The IEC 61850 multicast application association defined the abstract model could easily be mapped to a moderated room, where the moderator is the publisher of the unidirectional information, and the subscribers are dynamically invited to join the room in which the information is being published.

III. Security Considerations

This section investigates into IT security requirements and maps them to existing security measures.

A. Security Requirements

Security requirements targeting the integration of DER into a power system architecture are typically derived from a given system architecture like the one shown in Figure 1 and use cases describing the interactions of the components. Hence, the main focus here is placed on the investigation of the communication relations and data assets exchanged between the components. Table I below provides the most relevant data assets.

TABLE I. Data Assets

Asset	Description, example content	Security relation
Customer related information	Customer name, identification number, schedule information, location data, electrical network topology data	Effects on customer privacy
Meter Data	Meter readings that allow calculation of the quantity of electricity consumed or supplied over a time period.	Effects on system control functions and billing (and thus also privacy)
Control Commands	Actions requested by one component. These may include Inquiries, Alarms, Events, and Notifications.	Effects on system stability and reliability and also safety
Tariff Data	Utilities or other energy providers may inform consumers of new or temporary tariffs as a basis for purchase decisions.	Effects on customer privacy and competition

Data exchange of this information can be performed using hop-to-hop, end-to-end, and multicast communication, depending on the context and the involved entities. Based on Figure 1 the following trust assumptions are assumed:

- DER resource (XMPP client on IEC 61850 server) belongs to DER owner
- DER control (XMPP client on IEC 61850 client/server) belongs to DNO or 3rd party grid service
- XMPP server may belong to DNO or 3rd party grid service provider
- Trust relation between DER resource owner and DNO (e.g., based on contract)
- XMPP server operator trusted regarding resource discovery and message transfer (not handling!)

These trust assumptions for the data exchange lead to base security requirements enumerated in Table II below:

TABLE II. SECURITY REQUIREMENTS

	Security requirements
R1	End-to-middle source authentication ensures peers are properly identification and authentication. It is required between XMPP client and XMPP server or between XMPP servers. Note that here it may target mainly component authentication.
R2	End-to-end source authentication ensures peers are properly identification and authentication. It is required between IEC 61850 client and server instances. This authentication goes across the XMPP server ("application layer") and may be bound to a dedicated instance running on the IEC 61850 host.

 ISBN: 978-1-61208-414-5

	Security requirements
R3	End-to-middle integrity protection to ensure that data in transit has not been tampered with (unauthorized modification) between the XMPP client and XMPP server.
R4	End-to-end integrity protection to ensure that data in transit has not been tampered with (unauthorized modification) between the IEC 61850 client and server instances. Based on the different communication relations, the protection needs to support a) unicast: peer-to-peer related communication b) multicast: group based communication (via the MUC)
R5	End-to-middle confidentiality protection to ensure that data in transit has not been accessed (read) in an unauthorized way between the XMPP client and XMPP server.
R6	End-to-end confidentiality protection to ensure that data in transit has not been accessed (read) in an unauthorized way between the IEC 61850 client and server instances. Based on the different communication relations, the protection needs to support a) unicast: peer-to-peer related communication b) multicast: group based communication (via the MUC)

Mapping the enumerated requirements to the base architecture from Figure 1 is depicted in Figure 2 below.

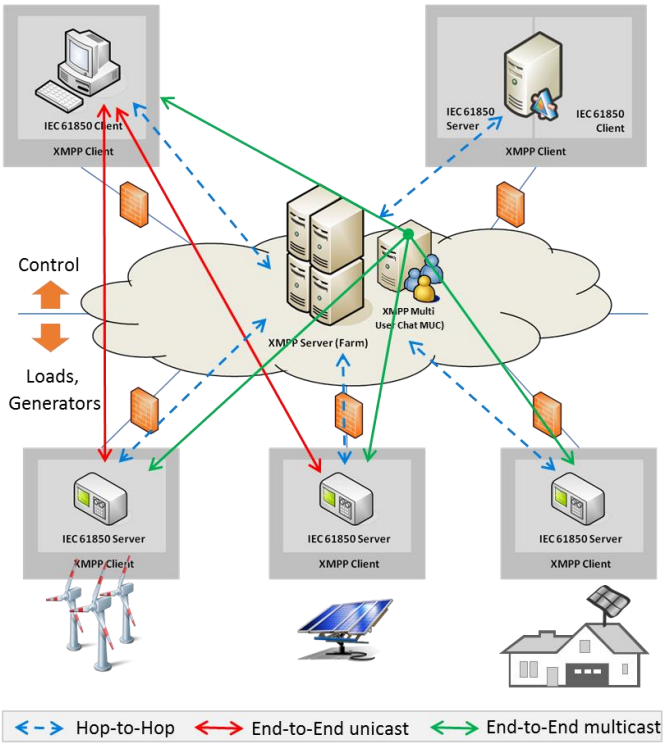

Figure 2. Security Relations for DER Integration

The consequent next step is the mapping of existing security measures to the base requirements to identify a target system architecture and also potential missing pieces.

B. *Mapping of exisiting Security Measures*

The following subsections map the security requirements to existing security measures, to discuss their applicability.

1) *Security Options in XMPP*

XMPP as defined in RFC 6120 and shown in Figure 3 already considers the following integrated security measures:

- Transport layer protection using Transport Layer Security(TLS, RFC 5246, ref. [9]), allows for
  - Mutual authentication of involved peers
  - Integrity protection of data transfer
  - Confidentiality protection of data transfer

  Depending on the chosen cipher suite, the application of this security mean addresses the security requirements R1, R3, and R5.
- XMPP peer authentication with two options
  - Rely on TLS authentication (addresses R1), or
  - Using the separate Simple Authentication and Security Layer (SASL) authentication (in XMPP [10], addresses R1) to authenticate users.

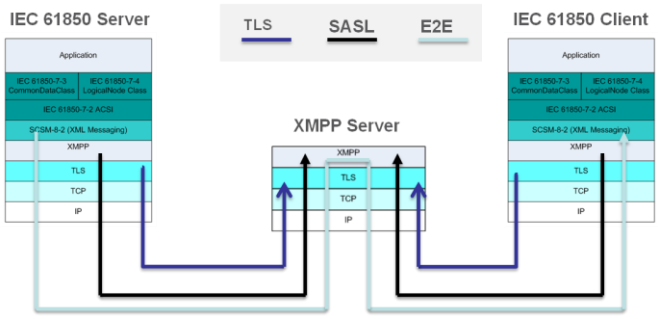

Figure 3. XMPP Security Options

Note that the XMPP security features target the communication between a XMPP client and XMPP server in the first place. Additional means to address end-to-end security support (between XMPP clients) on higher protocol layers are being available or discussed. Examples are:

- RFC 3923 [11] describes end-to-end signing and object encryption utilizing basically S/MIME. This approach addresses the security requirements R2, R4a, and R6a by applying asymmetric cryptography on a per message base. This may influence performance.
- The IETF draft draft-miller-xmpp-e2e [12] describes end-to-end object encryption and signatures between two entities with multiple devices. This addresses the situation, where some end points for a given recipient may share keys, some may use different keys, some may have no keys and some may not support encryption or signature verification at all. The draft defines a symmetric key table that is managed via three mechanisms that enable a key to be pushed to an end point, to be pulled from an originator or negotiated. If applicable it addresses R4a and R6a.

2) *Security in IEC 61850*

The working group IEC TC 57 WG15 is responsible for maintaining and evolving different security mechanisms applicable to the power systems domain. Here, IEC 62351 [13] has been defined, which is meanwhile split into 13 different parts with different level of completeness. Mainly

four parts are within scope for the further discussion of security mechanisms, which help to protect XMPP communication. Note that three parts are already available as technical standard (TS), but are currently being revised and updated, while the fourth one is defined in edition 1.The parts referred to are:

- IEC 62351-3: Profiles including TCP/IP: This part basically profiles the use of TLS and is referenced from part 4, 6, and 9.
- IEC 62351-4: Profiles including MMS: This part is currently in revision. The current document defines protection of MMS messages on transport and application layer. The application layer provides only limited protection as it does only allow for an authentication during the initial MMS session handshake without a cryptographic binding to the remaining part of session. As new scenarios arise, involving intermediate devices, this protection is no longer sufficient. Hence, IEC 62351-4 is being revised to enhance the protection of MMS traffic with additional application layer security profiles. Now, MMS session integrity and confidentiality protection is provided as depicted in Figure 4:

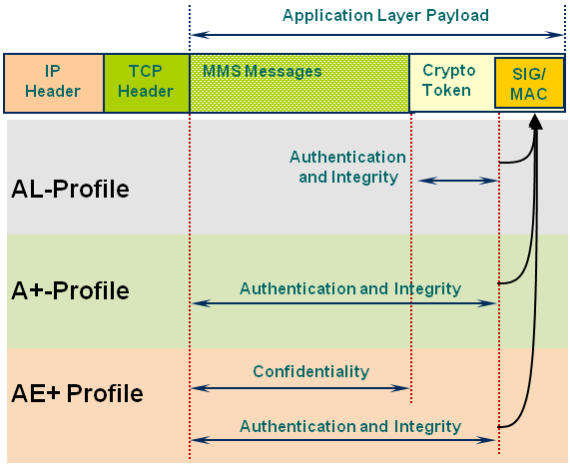

Figure 4. IEC 62351-4 A-Profile enhancements

This approach can be leveraged for the transport over XMPP to address R2, R4a and R6a.

- IEC 62351-6: Security for IEC 61850: This part targets the protection of Ethernet multicast communication exchanges in substations. The applied security measure bases on digital signatures and is currently being reworked to address performance shortcomings. It will be enhanced to allow for a group security approach utilizing symmetric cryptography. This approach can also be leveraged to realize for the secure integration of DER addressing R4b and R6b.
- Draft IEC/TS 62351-9: Cyber security key management for power system equipment: This part focuses on the base key management of asymmetric key material like X.509 certificates and corresponding private keys, but also symmetric keys applicable for group communication. For the latter, the IETF defined "Group Domain of Interpretation", RFC 6407 [14], is used to provide the key material for IEC 62351-6.

IV. PROPOSED COMMUNICATION SECURITY APPROACH

Based on the discussed trust assumptions, the security requirements and the security means in Section III, the following measures are proposed as base for a secure communication architecture to enable the secure integration of DER systems into the Smart Grid. The measures are distinguished into unicast and multicast communication. Also identified are open issues, which have to be addressed.

A. *Unicast security means*

For unicast communication, the security requirements can be fulfilled by the security means described in the sequel. Both hop-to-hop and end-to-end security are required to fulfill the security requirements.

Mutual authentication, session integrity and confidentiality of an XMPP-based client, -server, or server-server communication are protected (hop-to-hop security from IEC 61850 point of view). This fulfills the requirements R1, R3, and R5. The TLS security protocol as specified in RFC 6120 (XMPP Core) is applied, using the cipher suites and settings defined in IEC/IS 62351-3 defining a SSL/TLS profile for protecting TCP based IEC 61850 traffic. The credentials used for authentication are X.509 certificates of the involved peers. The verification of XMPP client or XMPP server certificates requires that the root certificate of the issuing certificate authority (CA) is available at the other peer. Most likely the CA has a relation to the DNO or another 3rd party grid service provider.

End-to-end authentication, integrity, and confidentiality can be achieved by applying the draft IEC/IS 62351-4 MMS secure session concept as stated in section 2) utilizing the AE+ profile to address R2, R4a, and R6a.

Open at this point in time is if there is a distinction between the transport layer authentication and the application layer authentication in terms of utilized credentials. Using the same credentials for both may require access lists of allowed XMPP clients (DER resources) for the XMPP server upfront provided by the DNO (as blacklist or white list).

B. *Multicast security means*

For multicast communication, the multicast distribution point is the MUC, residing at the XMPP server side. Multicast communication is protected only hop-to-hop between MUC and XMPP clients. Here, the solution defined in IEC 61351-6, i.e., the application of a group key for multicast communication, in conjunction with IEC 62351-9 defining the group key distribution, can be re-used directly to address security requirements R2, R4b and R6b.

The realization of the group key management is open, i.e., which entity generates the group key, and distributes it to the clients. Based on the given requirements, and the trust assumptions, the group key generation would be performed at the DNO side, while the group key distribution would be performed using the MUC of the XMPP architecture. This

 ISBN: 978-1-61208-414-5

distributed key management certainly requires a protected end-to-end transport of the group key to avoid that the XMPP server operator has access to this sensitive information. Further information about multicast authentication can also be found in [15].

V. IDENTIFIED OPEN ISSUES

As stated in the previous section, open issues have been identified regarding the credentials used for the peer authentication (hop-to-hop, and end-to-end) in unicast communication, and also regarding the mapping of certain multicast security related functions to the various involved entities. Another issue besides the selection of the authentication credential relates to the performance of peer authentication of XMPP clients towards the XMPP server. It has to be determined, which entity performs the authentication and access control. Different options have been identified:

- Option 1: The XMPP server performs the client authentication locally, using a locally available access control list. The access control list can be provided by the DNO, or by another 3rd party grid service provider over a secure configuration protocol.
- Option 2: The DNO, or another 3rd party grid service provider, performs the authentication, and access control check remotely, based on a redirection from the XMPP server. Frameworks like OAuth [16]could be involved here
- Option 3: While the authentication is performed locally by the XMPP server, the access control check is performed remotely.

These topics require further research, and will have to be included in future standardization work.

Based on a threat and risk analysis, the options for using single credential or different credentials for hop-to-hop, and end-to-end security, have to be compared in the specific application context. This is the basis to make a well-founded design decision. It has to be defined whether the choice can be left to the energy operator to provide flexibility for both options. If all peers authenticate using X.509 certificates, and corresponding private keys, the creation, and distribution of these operational certificates needs to be defined from a process, and also a technical point of view. The standard IEC 62351-9 (targeting key management) provides guidance here, but the involved peers need to be identified, and their responsibility needs to be described for all use cases at a fine granularity to assure interoperability.

Further issues requiring future research are the management of multicast membership: Which entity is determining which XMPP client is allowed to participate in which MUC multicast room. How is the multicast key distribution being performed? It could be performed independently from the MUC, or alternatively using the MUC for distribution of the (encrypted) multicast key.

VI. CONCLUSIONS AND OUTLOOK

This paper proposes security measures for the integration of DER systems into Smart Energy Grid and Smart Market, utilizing and combining mostly existing, or security means currently defined by different standardization organizations. The process for the definition of a standardized security solution is currently ongoing within the IEC.

Open issues requiring further research have been identified, and possible directions for defining a suitable solution have been outlined. While open issues lie in the technical domain, they have dependencies also in the operational domain as security management operations have to be aligned with general operational use cases. The means to address have not been decided yet and need further research.

It is envisioned to provide an implementation in the next step as proof of concept for the applicability of the proposed security approach.

REFERENCES

[1] ISO 61850-x: Communication networks and systems for power utility automation, http://www.iec.ch/smartgrid/standards/ [retrieved: Jan. 2015]

[2] "Efficient Energy Automation with the IEC 61850 Standard Application Examples", Siemens AG, December 2010, http://www.energy.siemens.com/mx/pool/hq/energy-topics/standards/iec-61850/Application_examples_en.pdf [retrieved: Dec. 2014].

[3] ISO 9506: Industrial Automation Systems – Manufacturing Message Specification.

[4] IEC TR 61850-80-3: Mapping to Web Protocols – Requirement Analysis and Technology Assessment

[5] P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, https://tools.ietf.org/html/rfc6120 [retrieved: Jan. 2014].

[6] A. Gulbrandsen, P. Vixie, and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, http://tools.ietf.org/rfc/rfc2782.txt [retrieved: Jan. 2015].

[7] XMPP Protocol extensions: http://xmpp.org/xmpp-protocols/xmpp-extensions/ [retrieved: Jan. 2015].

[8] XMPP foundation: http://www.xmpp.org [retrieved: April. 2015]

[9] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, Aug. 2008, http://tools.ietf.org/html/rfc5246 [retrieved: Jan. 2015].

[10] A. Melenikov and K.Zeilenga, "Simple Authentication and Security Layer (SASL)", RFC 4422, http://tools.ietf.org/html/rfc4422 [retrieved: Jan. 2015].

[11] P. Saint-Andre, "End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)", RFC 3923, https://tools.ietf.org/html/rfc3923 [retrieved: Jan. 2015].

[12] M.Miller and C.Wallace, "End-to-End Object Encryption and Signatures for XMPP", Draft, https://datatracker.ietf.org/doc/draft-miller-xmpp-e2e/ [retrieved: Jan. 2015].

[13] IEC 62351-x Power systems management and associated information exchange – Data and communication security, http://www.iec.ch/smartgrid/standards/ [retrieved: Jan. 2015].

[14] B. Weiss, S. Rowles, and T. Hardjono, "The Group Domain of Interpretation", RFC 6407, Oct. 2011, http://tools.ietf.org/html/rfc6407 [retrieved: Jan. 2015].

[15] S. Fries and R. Falk, "Efficient Multicast Authentication in Energy Environments", Proc. IARIA Energy 2013, March 2013, ISBN 978-1-61208-259-2, pp. 65-71, http://www.thinkmind.org/download.php?articleid=energy_2013_3_30_40056 [retrieved Dec. 2014].

[16] OAuth - OAuth 2.0 authorization framework, http://oauth.net/ [retrieved Jan. 2015].

 ISBN: 978-1-61208-414-5