Decentralized Energy in the Smart Energy Grid and Smart Market – How to master reliable and secure control

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 reliable integration of decentralized energy resources and loads into the smart energy grid and into a smart energy market is gaining more importance to cope with the increasing energy demand and the installation of renewable energy sources. Ideally, the load on the energy transmission network shall not be affected by direct energy exchange between local generation and consumption within a distribution network. Characteristic for the involved control systems is the data exchange between intelligent electronic devices (IEDs) that are used to monitor and control the operation. For the integration of Decentralized Energy Resources (DER), these IEDs provide the data for obtaining a system view of connected (decentralized) energy resources. This system view builds the base to manage a Virtual Power Plant (VPP) by combining a number of DER, reliably. In substation automation, the standard IEC 61850 is used to enable communication between IEDs to control the central energy generation and distribution. This standard is being enhanced with web services, features and mappings to support its application also for DER. One difference to the classical application in substations is the integration of IEDs residing on a customer network, most likely to be operated behind Firewalls and Network Address Translation (NAT). Nevertheless, end-to-end secured communication between DER and control center also over public networks must be ensured to maintain a consistent security level. 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 the currently proposed security measures for the communication architecture for DER integration. In addition to the original paper, the contributions to the International Electrotechnical Commission (IEC) for enhancements of the security for the standard IEC 61850 are elaborated more deeply with the focus not only on pairwise connections but also for multicast communication. Besides that, this paper also investigates into open issues related to the secure integration of DER.**

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

I. INTRODUCTION

As described in [1], renewable energy sources like the sun or wind power are becoming increasingly important to generate environmentally sustainable energy and thus to reduce greenhouse gases leading to global warming. Integrating these decentralized energy resources (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 to keep the stability of the power network frequency. As DER are typically geographically dispersed, widely distributed communication networks are required for exchanging control communication not only between the DER and the control center but also between DER. 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 controlled 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. It allows network operators to control more fine grained the amount and time of energy consumption. This is typically supported by mechanisms provided by a smart energy market allowing the exchange of information about energy prices and demand. Clearly, secure communication between a control station and DER equipment or energy loads of users as well as with decentralized field equipment must be achieved to avoid unauthorized access or manipulation of the data exchanged. Standard communication technologies based on IEC 61850 [2], which are used today for substation automation, cannot directly be applied and need enhancements.

Figure 1 below depicts the integration of DER into the Smart Grid and Smart Market from an abstract view. 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. All peers are connected via a communication network and shielded by firewalls to avoid unauthorized inbound or outbound connections. The control function may be located at a Distribution Network Operator (DNO), a VPP operator, or a smart energy market operator.

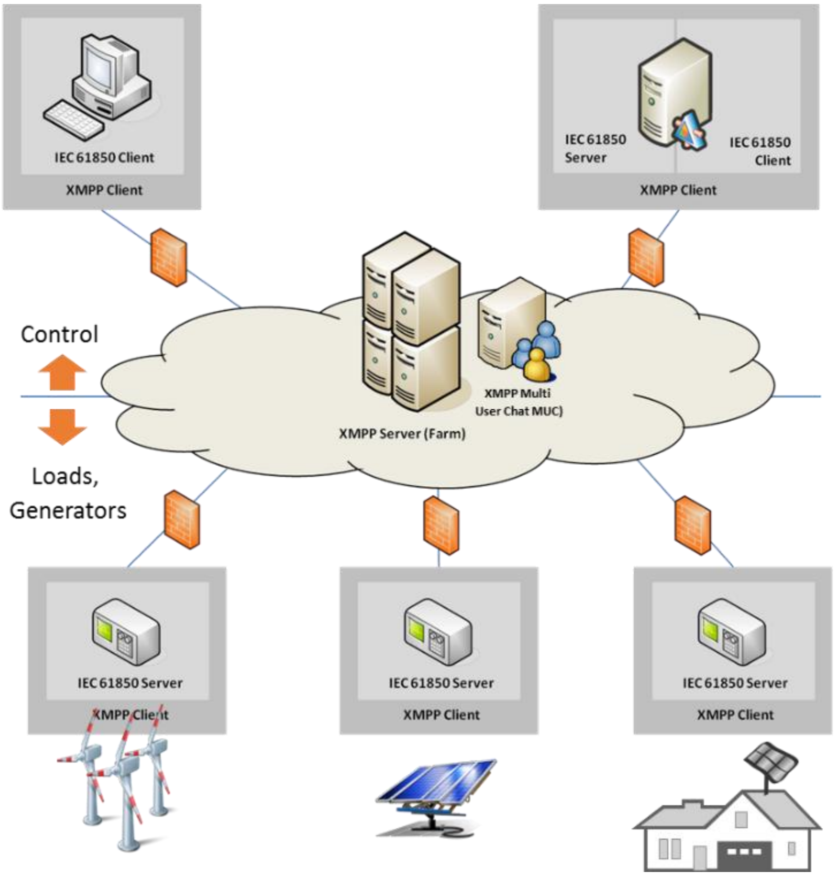

Figure 1. DER Integration based on IEC 61850 over XMPP

For the description of use cases in a smart grid environment the so called traffic light concept has been introduced by the regulation. This concept subdivides use cases into three different scenarios. The green phase allows using all market mechanisms, while yellow and red traffic light scenarios are defined by electrical network constrains due to problems like critical power unbalancing or power flow congestion in the electrical network.

The requirements of communication between DNO and DER Systems regarding for instance transfer times may differ compared to a pure market-driven use cases. It may be necessary to request a larger number of DER systems to change their generating or consuming power in a short time with a high priority. Group communication can be a required option for such use cases.

Grouping (sometimes called clustering) is a function of the DER management that consists in defining and using lists of DER systems by special characteristics (e.g., size of power, location in the topology of the network, type of connected DER units). Groups are created by each DER management entity for a special purpose. Using groups for a fast communication can require special means of the communication protocol.

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][3]. 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, that can be used to facilitate the IEC 61850 communication.

Note that this paper is an extended version of [1] that describes the environment in more detail, and also takes recent advancements in the definition of the IEC standard as well as the underlying scenarios and technology into account. The remaining part of this 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 I discusses the resulting security approach, which is also proposed for standardization. Compared to [1], this section is enhanced with the discussion of multicast communication security. This functionality has been identified in the original paper as being required to better control a larger number of IEDs individually, but provides a combined view at the control center level. Section V concludes the paper and provides an outlook for further work.

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 have not been finished, yet.

II. IEC 61850 Overview

A. The IEC 61850 principles

While the first edition of the IEC 61850 series[2], 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 (see also [3]).

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 destinations.

The IEC 61850-8-1 SCSM part has specified the mapping of IEC 61850 object model and associated services to the Manufacturing Message Specification (MMS, ISO 9506 series [4]). 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 DER. A current effort in the standardization has gathered the requirements for an IEC 61850 SCSM to Web technologies.

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 [5] 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 the election of XMPP [6] 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 DER (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 DER or can be discovered by the DER via DNS-SRV records [7].

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

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 (Jabber Identification), 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

IEC/CDV 61850-8-2 foresees XER encoding of MMS using following mapping of the services to the XMPP stanza:

- request/response 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, …)
- monitoring of association connectivity will use the <presence> stanza

The monitoring of the IEC 61850 association connectivity is a crucial part in an XMPP environment as the two ends of the IEC 61850 two party associations are not directly connected with means of a TCP socket. The XMPP Server monitors the connectivity to each of the two XMPP Clients, and informs the remaining one with mean of a presence (unavailable) stanza when the other end has disconnected (e.g., due to communication outage).

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

D. *Additional XMPP feautures for solving system management use cases*

The XMPP standard provides protocol extensions (so called XEPs [8]), i.e., optional technical specifications to solve additional communication requirements (e.g., group communication). The developments of the specifications are hosted and coordinated by the XMPP foundation [9]. 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.

XEP-0030 specifies an XMPP protocol extension for a generic Service Discovery, with which XMPP clients can discover services associated to a domain (support of MUC, time synchronization scheme, security actors, …) or to a given XMPP Client (support of MUC, support of service discovery, support of additional XEPs). To fulfill the plug and play requirements of a secured Smart Grid environment, XMPP Service Discovery offers an alternative to DNS-SRV records within a domain, having trusted entities (XMPP Server of the domain, or XMPP Clients) responding to service discovery requests. XEP-0060 specifies an XMPP protocol extension for a generic Publish-Subscribe functionality: an XMPP client can be configured to create a node onto the XMPP server, in which it will publish information for subscribers. With means of the Service Discovery protocol extension, XMPP Clients can discover the publish nodes and can request a subscription to them. Publish-subscribe model can be useful for publishing tariff data.

III. Security Considerations

This section describes IT security requirements that are connected with the reliable operation of a smart energy grid. The security requirements are mapped to standardized IT security measures.

A. *Security Requirements*

Security requirements targeting the integration of DER into power system architectures are typically derived from a given system architecture like the one shown in Figure 1, and from use cases describing the interactions of the components. Also, further security requirements may be posed through national regulations, depending on the country the DER integration is done. These regulations specifically target the privacy protection of end user related information.

The main focus in the context of this document 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	Name, identification number, location data, schedule information, 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, billing, and customer 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 competition and customer privacy as tariff depends on consumption.

Data exchange of this information typically depends on the underlying system architecture and may comprise hop-to-hop, end-to-end, or multicast communication, depending on the context and the involved entities. To determine the connected security requirements, the trust relations between the different entities are essential. Based on Figure 1 the following trust relations 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 service (not processing!)

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 identified and authenticated. 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 identified and authenticated. 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.
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 shown in Figure 1 is depicted in Figure 2 below. Note that the figure shows the unicast communication as well as potential multicast communication relations.

Based on the trust assumptions and the enumerated security requirements in Table II, the consequent next step is the investigation into existing security measures to evaluate their effectiveness to cope with the base requirements. These security measures are used to identify a first target system security architecture and also potential missing pieces. For the missing pieces, target architecture specific security measures have to be defined. The following subsections map the existing measures based on standardized solutions and also investigating into enhancements of the considered standards.

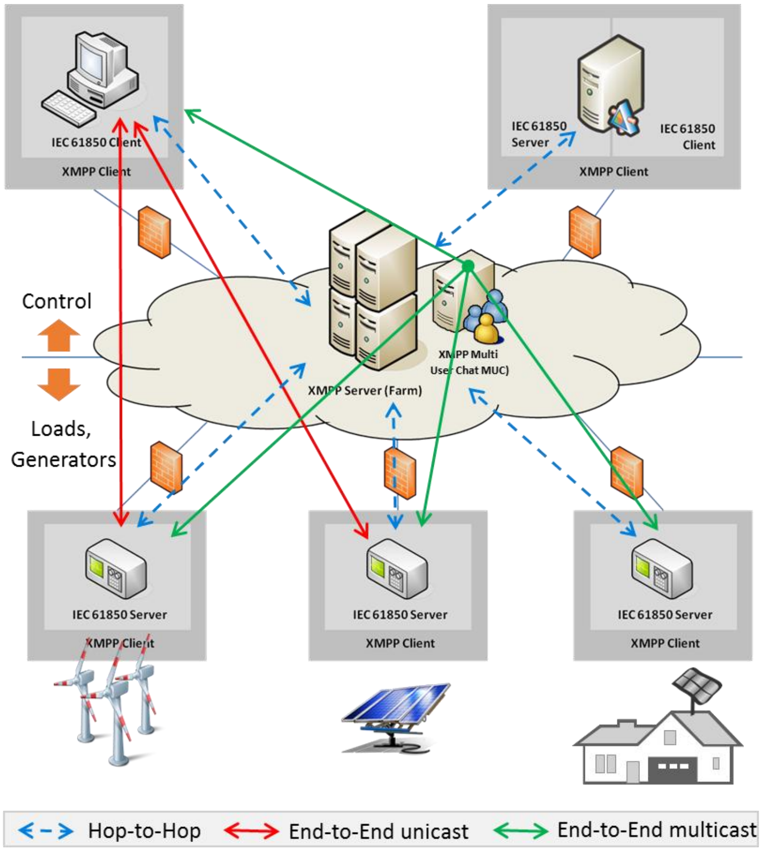

Figure 2. Security Relations for DER Integration

B. *Mapping of exisiting Security Measures*

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

1) *Security Options in XMPP*

XMPP as defined in RFC 6120 [6] and shown in Figure 3 already considers the following integrated security measures:

- Transport layer protection using the Transport Layer Security protocol (TLS, specified in RFC 5246 [10]), allows for
    - mutual authentication of involved peers,
    - integrity protection of data transfer, and
    - 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 [11], addresses R1) to authenticate users.

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 available or are currently discussed within standardization groups. Examples are:

- IETF RFC 3923 [12] describes end-to-end signing and object encryption utilizing S/MIME, like a secure email. This approach addresses the security requirements R2, R4a, and R6a by applying asymmetric cryptography on a per-message base. Two important points to note here are the following ones: Asymmetric cryptography in this context relates to the application of X.509 certificates and corresponding private keys in a similar way as in email applications. Note that the asymmetric encryption is typically much more costly in terms of required computational power compared to symmetric encryption, in particular for frequently exchanged messages. Hence, applying this approach may influence the performance in a negative way. Secondly, RFC 3923 is restricted to the application of RSA (Rivest, Shamir, Adleman) as asymmetric cryptographic algorithm for digital signature and encryption. More recent standards also support elliptic curve cryptography, which provides an adequate security level utilizing a much shorter key. Moreover, the operation is much more performant.
- The IETF draft draft-miller-xmpp-e2e [13] 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. Note that this draft Internet standard document has expired. It is mentioned here, as the general approach may provide a solution.
- The IETF draft draft-meyer-xmpp-e2e-encryption [14] describes XTLS as end-to-end TLS (like) channel. It would have been applicable to address R 2, R 4a, and R 6a, but the work has stopped and the draft has expired. The draft is stated here for completeness, as the mechanism intended to evolve the security provided in IEC 62351-4 uses a similar approach (see the next subsection).

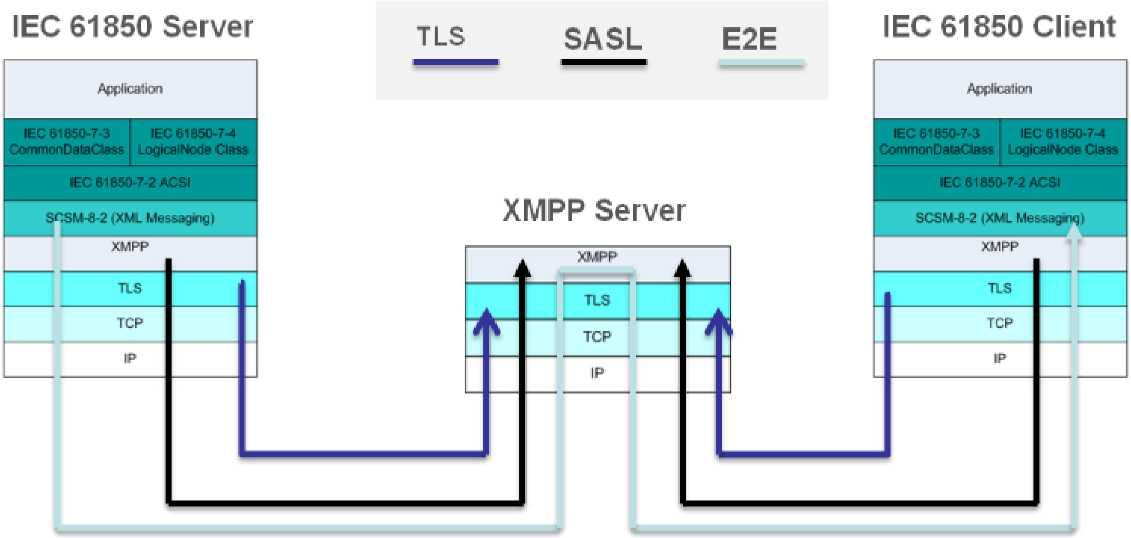

Figure 3. XMPP Security Options

2) *IEC 62351 – Security for IEC 61850 and beyond*

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 [15] has been defined, which is meanwhile split into 14 different parts with different level of completeness. Figure 5 shows the existing parts and their relation to the target energy automation standards.

Out of this set of specific security parts, mainly four parts are within the scope for the further discussion of security mechanisms that 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/IS 62351-3: Profiles including TCP/IP: This part basically profiles the use of TLS and is referenced from part 4, 5, 6, and 9. Profiling here relates to narrowing available options in TLS like the requirement to utilize mutual authentication reducing the number of allowed algorithms or the disallowance of utilizing certain cipher suites, not providing sufficient protection. Moreover, this part also provides guidelines for utilizing options, which depend on the embedding environment. An example is the relation of using session renegotiation and session resumption in conjunction with the update interval of the certificate revocation information.
- IEC/TS 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/TS 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 targeted as depicted in Figure 4 below.

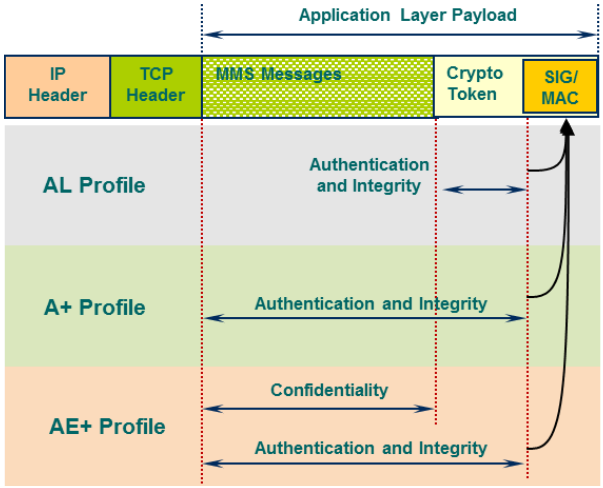
Application Layer Payload
IP Header
TCP Header
MMS Messages
Crypto Token
SIG/ MAC
AL Profile
Authentication and Integrity
A+ Profile
Authentication and Integrity
AE+ Profile
Confidentiality
Authentication and Integrity

Figure 4. IEC 62351-4 A-Profile enhancements

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

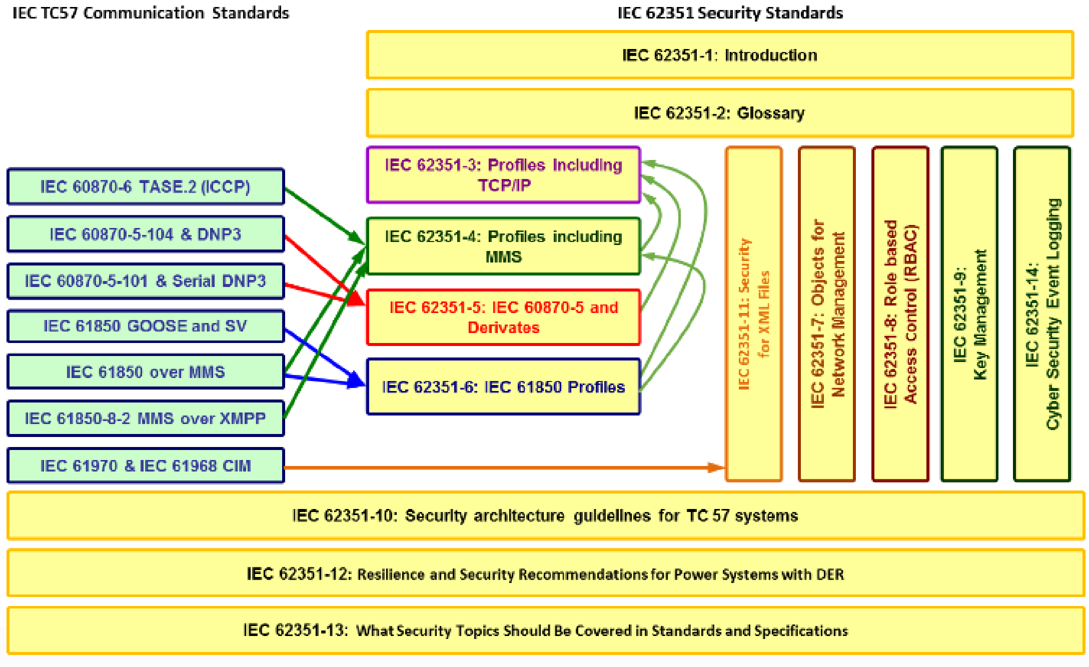
IEC TC57 Communication Standards
IEC 62351 Security Standards
IEC 62351-1: Introduction
IEC 62351-2: Glossary
IEC 60870-6 TASE.2 (ICCP)
IEC 60870-5-104 & DNP3
IEC 60870-5-101 & Serial DNP3
IEC 61850 GOOSE and SV
IEC 61850 over MMS
IEC 61850-8-2 MMS over XMPP
IEC 61970 & IEC 61968 CIM
IEC 62351-3: Profiles including TCP/IP
IEC 62351-4: Profiles including MMS
IEC 62351-5: IEC 60870-5 and Derivates
IEC 62351-6: IEC 61850 Profiles
IEC 62351-11: Security for XML Files
IEC 62351-7: Objects for Network Management
IEC 62351-8: Role based Access Control (RBAC)
IEC 62351-9: Key Management
IEC 62351-14: Cyber Security Event Logging
IEC 62351-10: Security architecture guidelines for TC 57 systems
IEC 62351-12: Resilience and Security Recommendations for Power Systems with DER
IEC 62351-13: What Security Topics Should Be Covered in Standards and Specifications

Figure 5. IEC62351 addressing energy automation communication

- IEC/TS 62351-6: Security for IEC 61850: This part targets the integrity protection of Ethernet multicast communication exchanges in substations utilizing GOOSE (Generic Object Oriented Substation Event), but can also be applied to the exchange of synchrophaser communication over wide area networks, also utilizing the GOOSE protocol. The originally standardized security measure employs on digital signatures on a per message base is currently being reworked to address performance shortcomings. It will be enhanced to allow for a group security approach utilizing symmetric cryptography to better cope with the performance requirements of GOOSE communication. This approach can also be leveraged to support the secure integration of DER addressing R4b and R6b in multicast environments.
- 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, including the enrollment and revocation of certificates, but also symmetric keys applicable for group communication. For the latter, the IETF defined Group Domain of Interpretation (GDOI), RFC 6407 [16], is used to provide the key material for IEC/TS 62351-6. To achieve the transport of the IEC 61850 related key material and the connected security policy, GDOI had to be enhanced with the appropriate key data payloads. This enhancement is described in [18].

As there are some fundamental differences between automated pairwise (unicast) and group based (multicast) key management and the application of the key, the following two subsections provide some background on both issues.

a) Pairwise or unicast security

A typical protocol example for pairwise key establishment and application is TLS, which is already used by IEC 62351 to secure TCP based traffic. Here, both peers possess a X.509 certificate and a corresponding private key that are used to authenticate and to protect the negotiation of a session secret and an associated security policy between these peers. As TLS is required to be used with mutual authentication, the session key negotiation is best done by applying the Diffie-Hellman key agreement scheme that is already part of several TLS cipher suites. As a result, both peers possess a pairwise shared secret as session key that is the base for the further symmetric protection of the message exchanges. The combination of the key with dedicated security services (integrity, encryption or both) is negotiated during the handshake based on proposed cipher suites. Just the same approach is being used to setup the session keys in the realization of the A-profiles shown in Figure 4. Here, there are much less security options provided compared to TLS. Figure 6 provides an overview on this handshake.

The base for the session key establishment is the signed handshake in the initiation phase. This handshake carries the Diffie Hellman parameter of both peers in a signed message. After the exchange both sides can derive the Diffie Hellman secret and utilize it to secure the concurrent session. The cleartokens shown in Figure 6 carry the necessary information for the Diffie Hellman key agreement.

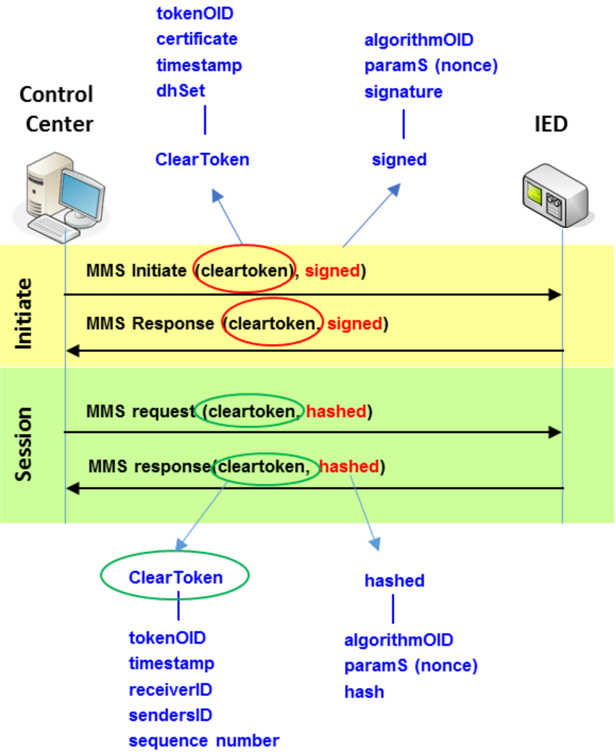

Figure 6. IEC 62351-4 Session Key establishment for A-Profiles

The trust in the certificates on both peers is provided through a trusted third party that has issued these certificates. This is a typical task of a certification authority (CA), which is part of a Public Key Infrastructure (PKI). It is assumed that both peers trust the same CA. This CA can issue the certificates offline. The certificates are verified during the TLS handshake that does not involve the trusted third party directly. Note that the revocation state may also be provided offline through the use of certificate revocation lists (CRLs), which are typically refreshed once a day.

b) Group based or multicast security

The general approach of group based security clearly differs from the more common unilateral security approach. As stated before, the chosen approach for IEC 62351 is GDOI [16]. An overview of multicast security options for power systems can be found in [17].

In case of GDOI a trusted third party, the key distribution center (KDC), needs to be online as part of the session key establishment. Here, the session key is a key shared between a group of participants.

Figure 7 shows the setup of a group of three IEDs, which form a group. The authentication towards the KDC is performed based on X.509 certificates and corresponding private keys. According to the security policy, the KDC distributes the key information (Key-ID) for the associated message flow (Stream-ID) to the authenticated IEDs. Each IED can then apply the group key to secure the message exchange between the three IEDs.

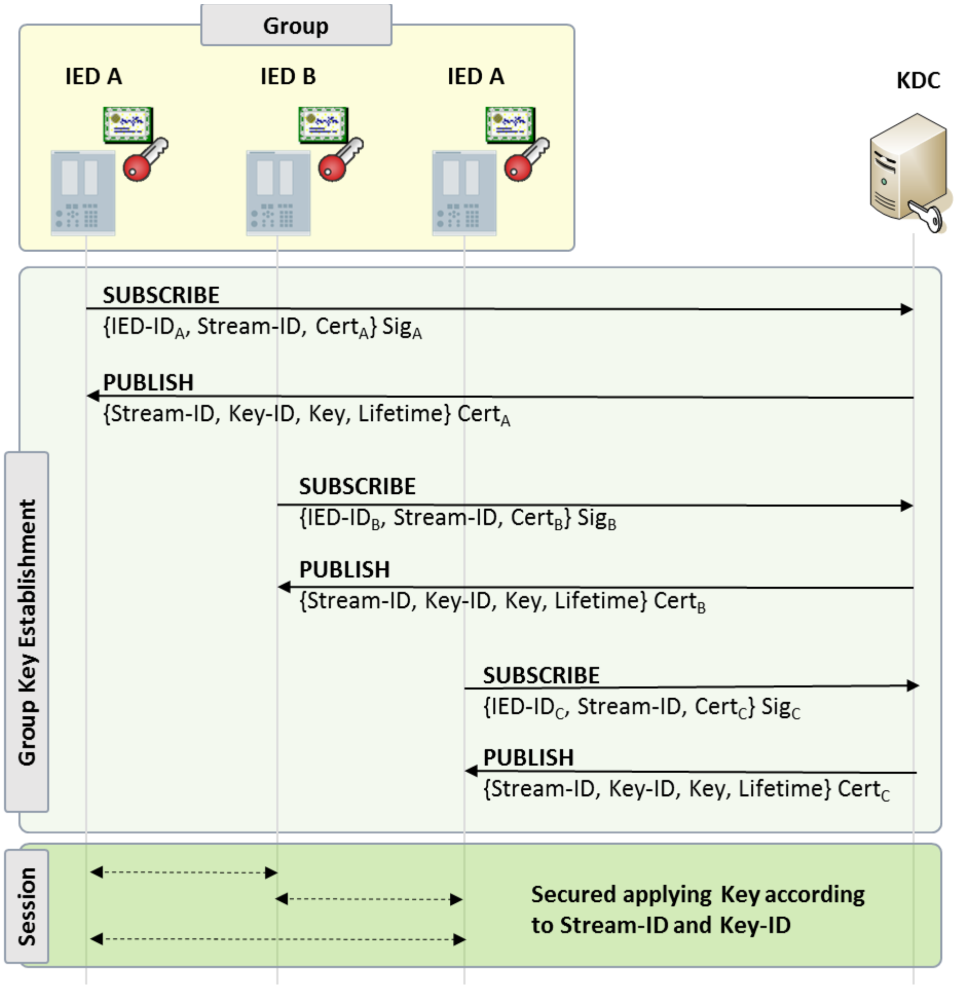
Group
IED A
IED B
IED A
KDC
Group Key Establishment
SUBSCRIBE
{IED-ID_A, Stream-ID, Cert_A} Sig_A
PUBLISH
{Stream-ID, Key-ID, Key, Lifetime} Cert_A
SUBSCRIBE
{IED-ID_B, Stream-ID, Cert_B} Sig_B
PUBLISH
{Stream-ID, Key-ID, Key, Lifetime} Cert_B
SUBSCRIBE
{IED-ID_C, Stream-ID, Cert_C} Sig_C
PUBLISH
{Stream-ID, Key-ID, Key, Lifetime} Cert_C
Session
Secured applying Key according to Stream-ID and Key-ID

Figure 7. GDOI based Key Distribution

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 TLS profile for protecting TCP based IEC 61850 traffic. The credentials used for authentication are X.509 certificates and corresponding private keys 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, i.e., between two XMPP client instances, 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 a provisioning of access lists of allowed XMPP clients (DER resources) for the XMPP server upfront provided by the DNO (as blacklist or white list) to the XMPP server operator. This is especially necessary, if the DNO uses an own PKI infrastructure. Also, it may be in the interest of the XMPP server operator to utilize an own PKI for issuing certificates used to access the provided service to better divide potential liability issues. This is especially interesting if the DNO and the XMPP service provider are two distinct legal entities.

B. *Multicast security means*

For multicast communication, the multicast distribution point is the MUC, residing at the XMPP server side. Using XMPP out of the box, the multicast communication is protected only hop-to-hop between MUC and XMPP clients. Access to the MUC is controlled by user authentication. Here two basic approaches are possible:

- If TLS is used with mutual authentication, the client certificate needs to carry the JID to provide the information about the authorization to use a dedicated JID to the MUC and/or presence service.
- Alternatively, if TLS is used with either unilateral authentication or in case of mutual authentication, with a certificate not carrying the JID and thus bound to the device and not the user, user authentication is performed using SASL to control access to the MUC and/or the presence service.

To achieve cryptographic end-to-end integrity and confidentiality protection, additional means are necessary. As the aforementioned group based key management protocol GDOI is already considered in the overall security architecture, it is also recommended for utilization to reuse existing features and components as far as possible. This establishes a group key shared between the authenticated members of the group. The security 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 functionality 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 or VPP side, while the group key distribution would be performed using the MUC of the XMPP architecture. This 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. The final mapping of the group based security scheme heavily depends on the underlying trust model. This trust model and the connected scenarios are currently under discussion in the IEC working group. The proposed solution builds one option to realize the group based communication technically. Note that there is currently work ongoing to also invest on one hand into the feasibility of using other group based key management schemes and also regarding the placement of the KDC in the overall architecture.

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 [19] could be involved here. This would allow also the utilization of already established solutions.
- Option 3: While the user authentication is performed locally by the XMPP server, e.g., using SASL, or a user certificate with included JID, the access control check is performed remotely. This approach would lead to a token based approach, which may utilize functionalities like SAML (Security Assertion Markup Language) tokens [20] or JSON web tokens [21].

These topics require further research, and the results will have to be part of future standardization work to ensure interoperable solutions.

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 research are the management of multicast membership: Which entity serves as the room creator that is aware of the group communication need for the current use case and determines, 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. The final solution will heavily depend on the underlying trust model, especially, if the XMPP server, including the MUC is operated by the DNO itself or a third party. This underlying trust model also builds the main point designing a solution to protect the information collected on the XMPP server itself. The information of published resources collected (and provided) at the XMPP server can be considered as essential asset, as it allows the potential control and information exchange with the connected energy resources, and can therefore be used to influence the connected energy grid in a sensitive way.

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 focus in this paper was placed on securing the information exchange between a DER system and a DNO controlling the energy grid. This approach considered the utilization of a potentially untrusted or less trusted environment for the communication exchange. The process for the definition of a standardized security solution is currently ongoing within the IEC taking the proposed solution as base.

Open issues relating to authentication options of peers to the different service points (DNO, XMPP server operator) and also for leveraging multicast communication 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. A proof of concept implementation of the proposed technical security approach to protect unicast communication is currently ongoing.

As outlined, but not address in this paper, the protection of collected information at the XMPP server is a necessary prerequisite to ensure a reliable management of DER. This is especially important as the number of connected DER is increasing and thus, the amount of energy, which can be controlled over publish subscribe mechanisms will increase.

REFERENCES

[1] S. Fries, R. Falk, H. Dawidczak, and T. Dufaure, "Secure Integration of DER into Smart Energy Grid and Smart Market," Proceedings IARIA SMART 2015, June 2015, ISBN: 978-1-61208-414-5, page 56-61, https://www.thinkmind.org/download.php?articleid=smart_2015_4_20_40020, [retrieved: January 2016]

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

[3] "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].

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

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

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

[7] 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].

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

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

[10] 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].

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

[12] 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].

[13] M. Miller and C. Wallace, "End-to-End Object Encryption and Signatures for XMPP," expired IETF draft, https://datatracker.ietf.org/doc/draft-miller-xmpp-e2e/ [retrieved: Jan. 2016].

[14] D. Meyer and P. Saint-Andre, "XTLS: End-to-End Encryption for the Extensible Messaging and Presence Protocol (XMPP) Using Transport Layer Security (TLS)," expired IETF draft, https://www.ietf.org/archive/id/draft-meyer-xmpp-e2e-encryption-02.txt, [retrieved: Jan. 2016]

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

[16] 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].

[17] R.Falk and S. Fries, "Security Considerations for Multicast Communication in Power Systems," International Journal on advances in Security, 2013 vol 6 nr. 3&4, ISSN: 1942-2636, [retrieved: Jan. 2016]

[18] B. Weiss, M. Seewald, and H. Falk, "GDOI Protocol Support for IEC 62351 Security Services," IETF draft, June 2015, https://tools.ietf.org/id/draft-weis-gdoi-iec62351-9-06.txt, [retrieved Dec. 2015]

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

[20] Web Services Security SAML Token Profile Version 1.1.1, OASIS Standard, March 2012, http://docs.oasis-open.org/wss-m/wss/v1.1.1/os/wss-SAMLTokenProfile-v1.1.1-os.html, [retrieved Jan. 2016].

[21] M. Jones, J. Bradley, and N. Sakimura, " JSON Web Token (JWT)." IETF RFC 7519, May 2015, https://tools.ietf.org/html/rfc7519, [retrieved Jan. 2016].