

Security for the Smart Grid – Enhancing IEC 62351 to Improve Security in Energy Automation Control

Steffen Fries*, Hans Joachim Hof*,
Thierry Dufaure⁺

Siemens AG

*Corporate Technology; ⁺Energy Automation
Germany

{steffen.fries; hans-joachim.hof;
thierry.dufaure}@siemens.com

Maik G. Seewald

Cisco Systems

Hallbergmoos, Germany
maseewal@cisco.com

Abstract— Information security has gained tremendous importance for energy distribution and energy automation systems over the last years. Security for the smart grid is crucial to ensure reliability and continuous operation of the smart grid. However, the smart grid comes along with new use cases that impose new challenges on existing standards like IEC61850. IEC61850 offers standardized communication services and standardized data models for communication in energy automation, hence it is beneficial for the realization of the smart grid. IEC 61850 is flanked by the standard IEC 62351 that addresses security and specifies technical requirements, which have to be met by vendors. This paper provides an overview about the different aspects of security necessary to build and operate smart grid systems by describing current and new use cases. The focus lies on the current state of the standardization of IEC 62351 and its applicability to the described use cases. Moreover, this work discusses potential enhancements of the standard to address potential shortcomings through changed business and operation models leading to changed trust relations in new use cases like decentralized energy generation and load control. These shortcomings are addressed by describing potential enhancements for part 4 of IEC 62351 allowing multiple parallel distinguishable sessions based on the Manufacturing Message Specification and proper end-to-end authentication as well as authorization.

Keywords – Smart Grid; Information Security; Cyber Security; Authentication; Authorization; Energy Automation; Smart Home; IEC Standards; NERC-CIP.

I. INTRODUCTION

Power generation and distribution systems are characterized by the existence of two infrastructures in parallel, the electrical grid, carrying the energy, and the information infrastructure used to automate and control the electrical grid. Especially the latter is becoming more and more one of the critical parts of power system operations as it is responsible not only for retriev-

ing information from field equipment but most importantly for sending control commands. A dependable management of these two infrastructures is crucial and strongly relies on the information infrastructure as automation continues to replace manual operations. Hence, the reliability of the power system strongly depends on the reliability of the information infrastructure. Therefore the information infrastructure must be managed to the level of reliability needed to provide the required stability of the power system infrastructure to prevent any type of outage.

The current, rather centralized approach for power generation is evolving to a decentralized power generation involving existing power plants, power plants producing renewable energy (like wind parks) down to households having their own micro power plants (e.g., solar cells). Decentralized energy generation (e.g., solar cells) is believed to become more and more important and common in the future to fight global warming by reducing the CO₂ footprint. Introducing decentralized energy generators into the current energy distribution network poses great challenges for energy automation (EA) in the smart grid scenario, especially secure communication between a control station (e.g., substation) and equipment of users (e.g., decentralized energy generators) must be addressed. Moreover, electro mobility will become more important and needs to be integrated into the current power system landscape. This increases the complexity of power systems even more. In addition, there is also the trend to interconnect the formerly closed and proprietary architectures with office environments and enterprise systems to provide new functionalities and increase cost effectiveness on the move to smarter grid infrastructures. This is accompanied by complete restructuring of the conventional roles on energy market participants.

The classical system architecture of the electric power grid defines distinct roles for energy producers, suppliers and consumers. With the new paradigm of smart grids driving towards sustainability, some of these roles will be redefined. The energy supplier systems have to handle an increasing amount of energy gained from distributed renewable energy sources and independent power production systems in residences. These forms of energy are produced in a much more decentralized way and also have a much more volatile characteristic compared to traditional forms of energy provided by existing power plants, often called bulk generation. At the same time one of the key factors for efficient and economic power generation is a balanced load level on power plants. Smart grid is the approach to address the mismatch between energy generation and consumption. Both aspects directly influence the distribution process of transport and distribution system operators and require the adoption of advanced information and communication technologies (ICT) in these processes.

As the information infrastructure can be described as the backbone of the smart grid and therefore needs appropriate protection to ensure a stable operation of power systems in order to support the required system reliability. Information and cyber security provides the base for protection and resiliency against cyber attacks. This has also be addressed in the comprehensive document set NISTIR 7268 from the Smart Grid Interoperability Panel (cf. [6], [7], and [8]).

The remainder of this paper is organized as follows: Section II provides an overview about energy automation control frameworks focusing on IEC 61850 as one corner stone for the smart grid. Section III discusses security requirements in the context of smart grid. The following Section IV discusses the currently available security in terms of the standard IEC 62351. Based on this, Sections V to VIII discuss potential shortcomings of the standard that become visible through new smart grid use cases. Sections IX and X provide an outlook for potential future work and a conclusion.

II. ENERGY AUTOMATION CONTROL FRAMEWORKS

Typical automation systems are built in a hierarchical way. Figure 1 shows typical layers of an automation pyramid. On the lowest level there are sensors and actors like switchgear that are connected to field devices. Serialized field buses as used for a long time are increasingly be replaced by standard communication

technology as Ethernet and IP. These field devices are actuated by, e.g., substation controllers, which may be interconnected with other substation controllers using TCP/IP based protocols. On the top are interconnections to supervisory systems the so called control centers, again via TCP/IP.

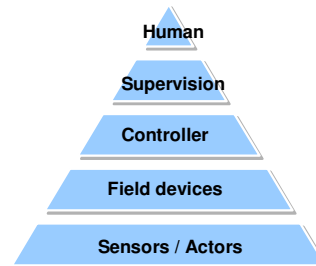


Figure 1. Automation Pyramid

IEC 61850 is a popular standard for communication in the domain of energy automation. It is assumed to be the successor of the currently used standards IEC 60870-4-104 and DNP3 also for the North American region. IEC 61850 enables interoperability between devices used in energy automation, i.e., two IEC 61850 enabled devices of different manufacturers can exchange a set of clearly defined data and the devices can interpret and use these data to achieve the functionality required by the application due to a standardized data model. In particular IEC 61850 enables continuous communication from a control station to decentralized energy generators by using a standardized data format.

IEC 61850 addresses the data exchange on three levels: process level, field level, and station level. It defines the following four important aspects on these levels: Standardized self-describing data, standardized services, standardized networks, and standardized configuration for a complete description of a device. An XML-based system description language – Substation Configuration Language (SCL) – is used to describe a device. Standardized services are used to send standardized data over standardized communication systems. However, IEC 61850 defines abstract communication services that are mapped on existing protocols like TCP/IP, and Ethernet, using the Manufacturing Message Specification (MMS). Moreover, there are also dedicated IEC standards mapping of the IEC 61850 to the target application domain, like IEC 61400-25 providing an adaptation for wind power plants. Here, a mapping to Web Services is targeted and currently under discussion. Security for IEC 61850 is addressed in the related standard IEC 62351 that is described in the following section.

Today, IEC 61850 is mainly used for reporting status and transmitting sampled value information from Intelligent Electronic Devices (IED) to Substation automation controller as well as for command transport from Substation automation controller to IEDs. It also addresses the communication directly between IEDs using the Generic Object Oriented Substation Event (GOOSE) instead of dedicated wires. Necessary tasks comprise also configuration of equipment as well as control of circuit breakers.

The following Figure 2 gives an example of the communication between multiple substations using IEC 61850.

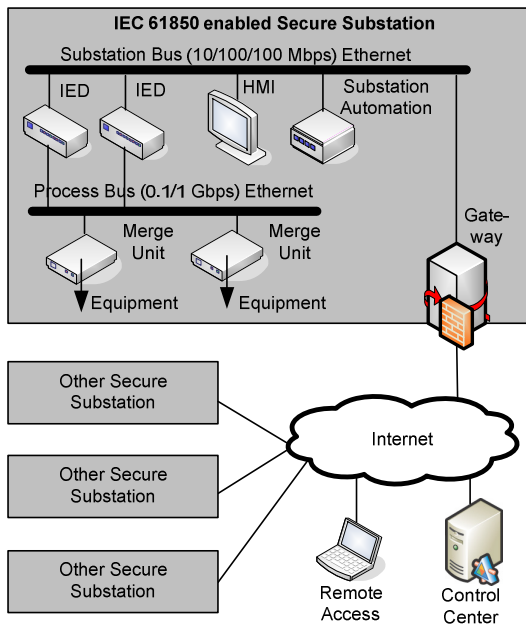


Figure 2. Typical IEC 61850 Scenario

III. SMART GRID SECURITY REQUIREMENTS

Security requirements stem from regulation, technical boundary conditions, and/or direct end-customers. Regulative requirements are given, e.g., by the following regulations.

A. Regulations and Regulative requirements

NERC-CIP: North American Electric Reliability Council (NERC) has established the Critical Infrastructure Protection (CIP) Cyber Security Standards CIP-002 through CIP-009, which are designed to provide a foundation of sound security practices across the bulk power system. These standards are not designed to protect the system from specific and imminent threats.

They apply to operators of Bulk Electric Systems (see also [2]). The standards originate in 2006. Last updates have been made in May 2009, but new parts of the standards (CIP 010 and CIP 011) are currently under development.

NERC-CIP provides a consistent framework for security control perimeters and access management with incident reporting and recovery for critical cyber assets and cover functional as well as non-functional requirements. TABLE I provides an overview about the different NERC-CIP parts.

TABLE I. NERC-CIP Overview

CIP	Title / covers
002	Critical Cyber Asset Identification Identification and documentation of Critical Cyber Assets using risk-based assessment methodologies
003	Security Management Controls Documentation and implementation of Cyber Security Policy reflecting commitment and ability to secure Critical Cyber Assets
004	Personnel and Training Maintenance and documentation of security awareness programs to ensure personnel knowledge on proven security practices
005	Electronic Security Protection Identification and protection of Electronic Security Perimeters and their access points surrounding Critical Cyber Assets
006	Physical Security Program Creation and maintenance of physical security controls, including processes, tools, and procedures to monitor perimeter access
007	Systems Security Management Definition and maintenance of methods, procedures, and processes to secure Cyber Assets within the Electronic Security Perimeter to do not adversely affect existing Cyber Security Controls.
008	Incident Reporting & Response Planning Development and maintenance of a Cyber Security Incident response plan that addresses classification, response actions and reporting
009	Recovery Plans for Critical Cyber Assets Creation and review of recovery plans for Critical Cyber Assets
Draft 010	Bulk Electrical System Cyber System Categorization Categorization of BES systems that execute or enable functions essential to reliable operation of the BES into three different classes.
Draft 011	Bulk Electrical System Cyber System Protection Mapping of security requirements to BES system categories defined in CIP-010

As already stated, NERC-CIP relates primarily to the operation of critical infrastructure. Nevertheless, this also places requirements on the product vendors to cope with certain security requirements.

BDEW: The “Bundesverband für Energie- und Wasserwirtschaft – BDEW was founded by the federation of four German energy related associations: Bundesverband der deutschen Gas- und Wasserwirtschaft (BGW), Verband der Verbundunternehmen und Regionalen Energieversorger in Deutschland (VRE), Verband der Netzbetreiber (VDN) and Verband der Elektrizitätswirtschaft (VDEW). The BDEW introduced a white paper defining basic security measures and requirements for IT-based control, automation and telecommunication systems, taking into account general technical and operational conditions. It can be seen as a further national approach targeting similar goals as NERC-CIP but less detailed. The white paper addresses requirements for vendors and manufacturers of power system management systems and can be used as an amendment to tender specification.

B. Supportive actions

Besides regulative actions, there are also supporting actions, that currently take place, e.g., by investigating in currently available standards and technologies, e.g., by the NIST (National Institute of Standards and Technologies) Smart Grid Interoperability Project (see also [4]). There are two documents, which are mentioned here as they are very compulsory covering a wide range of existing material as well as requirements for further investigation, that have been accomplished by NIST:

- *NIST Framework and Roadmap for Smart Grid Interoperability Standards*, identifying technical standards and specifications, which are also relate to smart grid security (cf. [5]).
- *NISTIR 7628* (cf. [6], [7], and [8]) originates from the Smart Grid Interoperability Panel (Cyber Security WG) and targets the development of a comprehensive set of cyber security requirements building on the NIST SP 1108 (cf. [5]), also stated above. The document consists of three subdocuments targeting strategy (cf. [6]), security architecture (cf. [7]), and requirements, and supportive analyses and references (cf. [8]).

In addition to the NIST activities, the IEC has issued the IEC SG3 report (SMB/4175/R), which encompasses requirements, status and recommendations of standards relevant for the Smart Grid. Security is cov-

ered in detail in a separate section of this document. An overall security architecture capturing the complexity of the Smart Grid is requested. Beside this, the following recommendations pertaining open items and necessary enhancements are listed:

- A specification of a dedicated set of security controls (e.g., perimeter security, access control...)
- A defined compartmentalization of Smart Grid applications (domains) based on clear network segmentation and functional zones
- A specification comprising identity establishment (based on trust levels) and identity management
- Security of the legacy components must be addressed by standardization efforts
- The harmonization with the IEC 62443 standard to achieve common industrial security standards
- Finally, it is recommended to review, adapt and enhance existing standards in order to support general and ubiquitous security across wired and wireless connections.

IV. SECURE ENERGY AUTOMATION BASED ON IEC62351

Security services to be supported in energy automation comprise the usual suspects:

- **Authentication:** The property that the claimed identity of an entity is correct.
- **Authorization:** The process of giving someone permission to do or have something.
- **Integrity:** The property that information has not been altered in an unauthorized manner.
- **Non-repudiation:** The property that involvement in an action cannot be denied.
- **Confidentiality:** The property that information is not made available or disclosed to unauthorized individuals, entities or processes.

In contrast to office networks, automation networks have different requirements to security services as shown in the following figure.



	Office 	EA-Network 
Confidentiality (Data)	High	Low – Medium
Integrity (Data)	Medium	High
Availability / Reliability	Medium	High
Non-Repudiation	Medium	High
Component Lifetime	Short - medium	Long

Figure 3. Comparison Office/Automation security

In the context of energy automation, IEC 62351 defines explicit security measures for TCP-based and serial protocols. It applies directly to substation automation deploying IEC 61850 and IEC 60870-x protocols as well as in adjacent communication protocols supporting energy automation, like ICCP (TASE.2) used for inter-control center communication. A clear goal of the standardization of IEC62351 is the assurance of end-to-end security. The standard comprises multiple parts that are in different state of completion.

While part 1 and 2 are more general and comprise the explanation of threat scenarios and the definition of terms, part 3 to 8 are directly related to dedicated protocols like IEC 61850 (IEC 62351 Part 6) and IEC 60870-5-x (IEC 62351 Part 5) and their mappings to lower layer protocols like TCP/IP (IEC 62351 Part 3) and MMS (IEC 62351 Part 4) as well as the mapping of security to the network management (part 7) and role-based access control (part 8). These parts utilize symmetric as well as asymmetric cryptographic functions to secure the payload and the communication link. The remaining part of this section provides an overview about the different parts of IEC 62351 and their current status in standardization.

IEC 62351 applies existing security protocols like Transport Layer Security (TLS, cf. [10]), which has been successfully used in other technical areas and industrial applications, in different parts of the standard. The application of TLS provides for security services like mutual authentication of communication peers and also integrity and confidentiality protection of the communicated data. Thanks to the mutual authentication required by IEC 62351 attacks like Man-in-the-Middle can be successfully countered.

Part 3 of IEC 62351 defines how security services can be provided for TCP/IP based communication. As TLS is based on TCP/IP part 3 specifies cipher suites (the allowed combination of authentication, integrity protection and encryption algorithms) and also states requirements to the certificates to be used in conjunction with TLS. These requirements comprise for instance dedicated certificate context, application of signatures, and the definition of certificate revocation procedures. For the latter, the focus lies mostly on Certificate Revocation Lists (CRL). The application of the Online Certificate Status Protocol (OCSP) is not considered due to limited communication links within the substations. In contrast to office applications, the connections in energy automation are relatively long

lasting. This requires the definition of strict key update and CRL update intervals, to restrict the application of cryptographic keys not only for a dedicated number of packets but also for a dedicated time. Another challenge are interoperability requirements between implementations of different vendor's products.

Part 4 of IEC 612351 specifies procedures, protocol enhancements, and algorithms targeting the increase of security messages transmitted over MMS. MMS is an international standard (ISO 9506) dealing with a messaging system for transferring real time process data and supervisory control information either between networked devices or in communication with computer applications. Part 4 defines procedures on transport layer, basing on TLS, as well as on application layer to protect the communicated information. One goal of this paper is to analyze if the defined security is appropriate especially in the context of smart grid applications. This will be discussed in detail in Section VI.

Besides TCP/IP, IEC 62351 Part 5 relates to the specialties of serial communication. Here, additional security measures are defined to especially protect the integrity of the serial connections applying keyed hashes. This part also specifies a separate key management necessary for the security measures.

Part 6 of IEC 62351 describes security for IEC 61850 Peer-to-Peer Profiles. It covers the profiles in IEC 61850 that are not based on TCP/IP for the communication of Generic Object Oriented Substation Events (GOOSE), and Sample Measured Values (SMV) using, e.g., plain Ethernet. Specific for this type of communication is the usage of multicast transfer, where each field device decides based on the message type and sender if it processes the message or not. Security employs digital signatures on message level to protect the integrity of the messages sent, to also cope with multicast connections.

IEC 62351 Part 7 describes security related data objects for end-to-end network and system management (NSM) and also security problem detection. These data objects support the secure control of dedicated parts of the energy automation network. Part 7 can help to implement or extend intrusion detections systems for power system specific objects and devices.

Part 8 of the standard is currently in definition and addresses the integration of role-based access control mechanisms into the whole domain of power systems. This is necessary as in protection systems and in con-

trol centers authorization as well as stringent traceability is required. One usage example is the verification of who has authorized and performed a dedicated switching command. Part 8 supports role-based access control in terms of three profiles. Each of the profiles uses an own type of credential as there are identity certificates with role enhancements, attribute certificates, and software tokens.

The following table provides a short overview about the different IEC 62351 parts and their status in standardization:

TABLE II. IEC 62351 Overview

IEC 62351	Definition of Security Services for	Standardization Status
Part 3	TCP / IP (Profile)	Technical Specification
Part 4	MMS (Profile)	Technical Specification
Part 5	60870-5 and Derivates	Technical Specification
Part 6	IEC 61850	Technical Specification
Part 7	Network Management	Technical Specification
Part 8	Role-based Access Control	Committee Draft
Part 9	Credential Management	New Work Item Proposal

A first glimpse at the current IEC 62351 parts shows that many of the technical security requirements to be applied to energy automation components and systems can be directly derived from the standard. For instance part 3 and 4 explicitly require the usage of TLS. They define cipher suites, which are to be supported as mandatory. These parts also define recommended cipher suites and also deprecate cipher suites, which shall not be applied from IEC 62351 point of view. Note, that the mandatory cipher suites do not collapse with the cipher suites the different TLS versions (1.0 – RFC 2246, 1.1 – RFC 4346, 1.2 – RFC 5246) state as mandatory. IEC 62351 always references TLS v1.0 probably to better address interoperability.

Analyzing the standard more deeply shows that several requirements are provided rather implicit. These requirements relate mostly to the overall key management, which guarantees a smooth operation of the security mechanisms. IEC 62351 uses heavily certificates and associated private keys, e.g., in the context of transport layer protection (using TLS) but also on ap-

plication layer as in part 6 to secure GOOSE. But to apply this type of credentials, the general handling and life-cycle management including generation, provisioning, revocation, and especially the initial distribution to all participating entities needs to be considered. This is currently underspecified, but has been acknowledged by standardization as important for the general operation but also for the interoperability of different vendor's products. As the standard is extensible a new part, describing credential handling in the context of IEC 62351 services is under development. Moreover, a security architecture, required for building, engineering, and operating power systems is a necessary base to ensure safety and reliability of these systems. Hence further work has been initiated to describe hands-on security architecture guidelines for system engineers and operators to implement, manage and operate power systems securely.

Besides standard enhancements, which have become necessary through findings during the implementation of IEC 62351, new scenarios may also require the further evolvement of already existing or new parts of the standard, to better cope with new use cases. This is the focus of the next section, investigating in new scenarios, which slightly deviate from standard substation automation and thus lead to new security requirements.

V. NEW USE CASES FOR IEC 61850 AND IEC 62351

Current challenges for the power grid include the integration of fluctuating renewable energy sources, distributed power generation, short interval feedback on users on their energy usage, user indicated demand peaks, and the foreseeable need for the integration of private electronic cars, leading to an even higher energy demand of customers at peak times. A "smarter" grid can meet many of these challenges. With the move to a Smart Grid the importance of IT communication technologies in energy automation rises. With the availability of pervasive IT communication services, a bunch of new use cases become possible that enhance the service to the customer and mitigate the impact of the challenges mentioned above. These new use cases include dynamic pricing, time of use pricing, selling local power into the grid, smart metering, and the like. As IEC 61850 is an introduced standard, the trend is to use this standard to realize these new use cases. While this keeps the effort low to implement new use cases, it may bring new security requirements up that are not addressed by IEC 62351 yet.

A. Consumer Perspective: Smart Home

Many use cases center around the Smart Home scenario. Smart Home in combination with the Smart Grid will allow people to understand how their household uses energy, manage energy use better, sell energy produced by local distributed energy generation, and reduce their carbon footprint. IEC 61850 is a natural candidate to use for communication between instances of the Smart Grid and the gateway of a Smart Home.

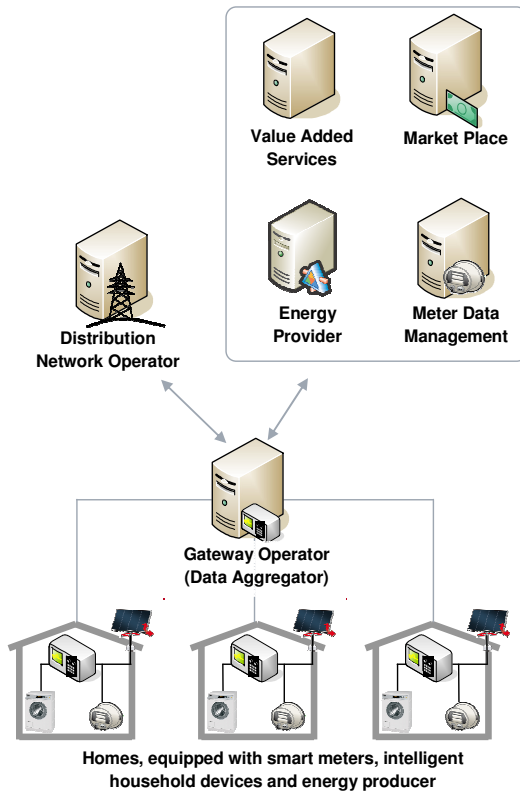


Figure 4. Connection of households to the smart grid

Figure 4 shows a typical system architecture of a smart grid:

- Homes are equipped with smart meters, intelligent household devices, and energy producers.
- Home gateways control the communication between the devices in a home and the Smart Grid and define a security perimeter. The home gateway hides the complexity of the in-house network from the Smart Grid. The home gateway may act as a proxy for the appliances of the home, e.g., on the market place.
- A gateway operator is responsible for administration of the home gateways and provides connectivity for the home gateways.

- The distribution network operator communicated with the home gateways by the means of another instance (in this case, the gateway operator is this instance) that hides the complexity of the home gateway management from the distribution network operator.
- The Meter Data Management manages the metering data received from the smart meters. The Meter Data Management processes the metering data for the various energy providers and provides them with a summary for accounting.
- At the energy market, consumers (resp. their home gateways) buy energy, and energy generators sell energy; hence the market offers a demand regulated price. An energy market alleviates the integration of distributed energy generators (e.g., solar cells).
- The smart grid communication infrastructure and the energy market are the enabler for other value added services.

Having a communication and IT infrastructure like this at hand, the following use cases are possible in a Smart Home scenario:

1) Energy-aware home appliances

Nowadays, the price of energy for private consumers is mostly constant. From the perspective of a utility it would be beneficial to have dynamic pricing to influence the energy usage of customers. On the customer side, new intelligent, energy-aware home appliances can optimize the costs for energy usage by starting and stopping energy extensive tasks (e.g., cloth or dish washing) at appropriate times (e.g., start when energy is cheap). This requires that the current price of energy is known and there is some way to determine the price of energy for the duration of an operation (e.g., washing a load of wash). One way to implement such a system is an energy market, where energy-aware home appliances buy a certain amount of energy before they start an operation. Especially charging a private electrical car during the night is an extremely flexible operation that requires much energy but has a large time window for execution, hence benefits from a good deal.

To implement this use case with the architecture presented above, the home gateway trades energy at the energy market. Accounting for any contract on the energy market includes the energy provider as well as the meter data management.

2) Distributed power generation

If energy is produced in a home, e.g., by solar cells,

the energy is traded on an energy market to achieve the best possible price. Especially if the energy market is on a large scale, selling the energy may be more attractive than a fixed pricing.

To implement this use case with the architecture presented above, the home gateway trades energy at the energy market. Accounting for contracts includes the distribution network provider as well as the smart meter management.

3) *Energy Management and User Awareness*

An application with integrated user interface in the home is used for communication with the utility, e.g., to get a diagram of current energy usage, to get current energy pricing, to get the personal energy usage history, to get energy saving tips and the like. The user interface may also be used to receive energy outage forecasts, for troubleshooting, or to dynamically select a desired energy mix.

Even energy-aware home appliances may offer a user interface that states the current price for one operation execution. E.g., a coffee machine may state the price per coffee pot.

To implement this use case with the architecture presented above, the home gateway informs appliances about current energy prices, which it either gets at the energy market or directly from the energy provider (price signals as special incentive for special behavior).

B. *Utility Perspective*

Other use cases are focused on keeping the distribution network stable and keeping costs for utilities low (e.g., because it is not necessary to buy additional energy at short notice). As IEC 61850 is already widespread in use in the distribution network, it is a natural candidate for the following use cases:

1) *Reactive shutoff of home appliances*

A utility has the ability to shut down certain home appliances in the household of users on short notice to react on certain situations in the network (e.g., if too many consumers are active). Such switch-off commands can be based on special contracts between user and utility operator.

To implement this use case with the architecture presented above, the utility must have a list of home appliances that can be shut off as well as the communication addresses of the associated home gateways. In the architecture above, home gateways may be addressed

by the gateway operator that also ensures the connectivity of the home gateways. The utility sends a shutoff message via the gateway operator to a set of home gateways. Sending this shutoff message to many households must be finished in a short time to allow fast reactions. The shutoff message must be protected to avoid being misused by attackers. The home gateway takes the appropriate actions to meet the request of the utility, especially, it communicates with proper appliances to be shut off.

2) *Shutoff of power generator*

The utility may not only turn off certain home appliances, it may also instruct distributed power generators not to feed energy to the distribution network to fight situations when there is a low demand for energy. The signaling process is the same as in the last use case.

3) *Demand Response*

Another use case from a utility prospect is demand response: A utility can send price signals (either a rather high price if energy demand is too high or a low price if the energy demand is too low) to influence energy usage of intelligent home appliances without using the energy market. Price signals are especially interesting for the loading of electric cars. Price signals can be sent for future time periods or as real time pricing information. The utility sends price signals via the gateway operator that knows to address the home gateways. The home gateways distribute the pricing information in the home to the appropriate home appliances.

4) *Asset Management*

Yet another use case from the utility perspective is asset management. Given a rising number of equipment for decentralized energy generation in the households of the users, managing the network gets more complex. An automated asset management helps to reduce costs and gives a good view on the state of the distribution network. IEC 61850 includes self-describing configurations of device and all kind of tracking data; hence it is a natural candidate for the following use cases:

- Utilities collect data about the state of the network and about the equipment in a user's home.
- Utility gathers circuit and/or transformer load profiles, makes decisions on asset replacement based on a range of inputs including comprehensive off line and on line condition data and analysis
- Utility performs localized load reduction to relieve circuit and/or transformer overloads

- Utility system operator determines level of severity for an impending asset failure and takes corrective action

C. New Requirements

One requirement arising from these new use cases is scalability. Security solutions for the Smart Grid must scale with millions of devices - Germany for example has more than 39 million households and each household may have more than one device. Multiple levels of hierarchy from a control station to a device in a household are a common solution to address scalability. This includes communication other than the point to point communication used today.

As shown in Figure 4, in smart grid scenario's new roles and/or components may be introduced in terms of a home energy gateway operator. This gateway operator is in charge of concentrating the communication from the home energy gateways up to the control center as well as providing an easy way to the control center to reach a high number of energy gateways at once. Moreover, a gateway operator may also offer additional services like remote management of the home energy gateways, e.g., to provide enhanced functionality or path and updates for installed software. This new component changes the trust assumptions for the substation communication as it may be seen new intermediate component, which belongs to a different security domain. This component most likely terminates the transport connection between a control center and the home energy gateway, which is used synonym here for a field device.

Today's security solutions assume trusted intermediate nodes if one application connection is realized over multiple transport connections. This assumption may not hold in the future and new security concepts may only assume intermediate nodes that forward traffic but may or may not be trusted.

The following section targets the analysis of applying IEC 62351 in the context of the smart grid scenario just described to discuss, if the standardized security provides sufficient counter measures.

VI. MISSING PIECES IN IEC62351

As stated in Section II above, part 4 of IEC 62351 specifies procedures, protocol enhancements, and algorithms targeting the increase of security of applications utilizing the MMS. MMS is an international standard (ISO 9506) dealing with a messaging system for trans-

ferring real time process data and supervisory control information either between networked devices or in communication with computer applications. Within IEC 61850 there exists a mapping to MMS to transport commands and data between the different energy automation components. Thus IEC 61850 can directly leverage the security enhancements defined in part 4 of IEC 62351.

The security, as defined in IEC 62351 part 4, is described by two profiles targeting transport security as T-Profile on one hand and application security as A-Profile. The T-Profile describes the protection of information, which is exchanged over TCP/IP using TLS. This is mainly being done by referring part 3 for TLS application and the definition of additional mandatory cipher suites. The A-Profile defines security services on application layer, targeting mainly authentication. Note that the authentication in the A-Profile is performed only during connection establishment on application layer using the MMS initiate command. Moreover this authentication is defined in a way that it does not provide application layer message integrity. Furthermore the authentication phase is not used to form a session. A session in this context cryptographically binds the authentication performed during the connection setup with subsequent messages exchanged between the communicating peers. Thus, in the current stage of the standard, messages on application layer are not protected regarding their integrity. To achieve integrity protection, the application of the T-Profile is being referred.

Combining A-Profile and T-Profile provides a connection allowing for authentication, integrity protection and confidentiality on transport level and authentication on application level. This approach works fine in scenarios, where the transport connection spans the same entities as the application connections as shown in Figure 5.

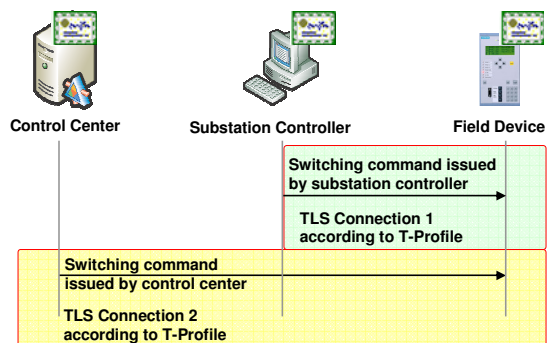


Figure 5. Direct switching action

While this approach may be sufficient for many energy automation scenarios, it may not cope with new use cases, for instance the ones described in Section V.

As soon as there is a difference in transport connection hops and application connection hops, security problems may arise. An example may be a scenario in which a proxy is used, e.g., to combine different connections or to multicast a single command to several other connections as described in Figure 4 by the gateway operator. From the standard energy automation architecture – Control Center, Substation Controller, Field Device – this gateway operator resembles the substation controller and operates as a communication proxy as shown in Figure 6. Therefore, the T-Profile is terminated by the substation controller, while the application connection may be established end-to-end, directly with the actual entity to be reached. Since IEC 62351 part 4 does not provide application level integrity, no end-to-end application level security is provided.

Such a scenario can be described as multi-hop connection from a transport level view and would require that the proxy is a trusted intermediate host, which cannot be guaranteed in many scenarios. For example in one of the new use cases addressed in the last section, a utility may use a number of proxy that multicasts a single “switch off” command issued by the control station to multiple households. This approach allows multiple hierarchy level for issuing the “switch off” commands to achieve scalability and fast reaction.

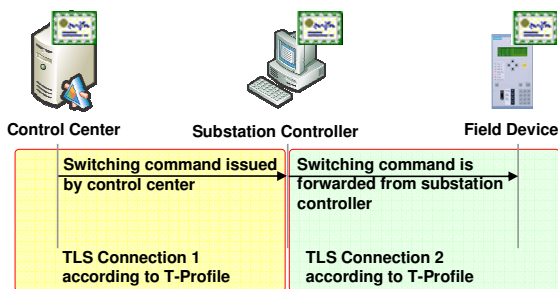


Figure 6. Proxied switching action

To provide also end-to-end integrity in multi-hop use cases with intermediate nodes additional measures have to be defined. Ideally, these will enhance the standard IEC 62351 to foster both, security and interoperability.

The approach to find appropriate security enhancements taken here involves the investigation into existing protocols, which already provide a secure session concept on application layer. The following section

analyzes different approaches to enhance part 4 based on existing security measures.

VII. CANDIDATES FOR ADAPTATION

This section discusses three potential candidates, which are already defined and widely used in communication technology and their suitability for IEC 62351 part 4 to better cope with multi-hop scenarios. As stated in the previous section, the additional security requirements to be met comprise peer authentication and message integrity on application layer between end-to-end communicating peers. The three candidates are:

- HTTP Digest Authentication as typically used in web based communication
- H.235 based security as used to protect multimedia communication
- XML security as applied in web service frameworks

The goal is the enhancement of MMS communication to allow cryptographically based sessions to provide end-to-end security on application layer. Moreover, being able to associate MMS commands with a dedicated session, also allows running multiple parallel distinguishable sessions over the same T-Profile protected link(s).

A. Candidate 1 HTTP Digest Authentication

RFC2617 (cf. [9]) describes authentication options in the context of HTTP (Hypertext Transport Protocol), which is used in many web-based applications. While basic authentication is deprecated because of its worst security, digest authentication is being widely used. In digest authentication a shared secret needs to be available on both ends of the communication, which is used to calculate an MD5 checksum over either a certain part of the message or the complete message as part of a challenge response mechanism to provide integrity protection. Typically each HTTP request can be challenged to authenticate the requestor. In the worst case this would mean that each communication action is doubled. The general approach is depicted in Figure 7.

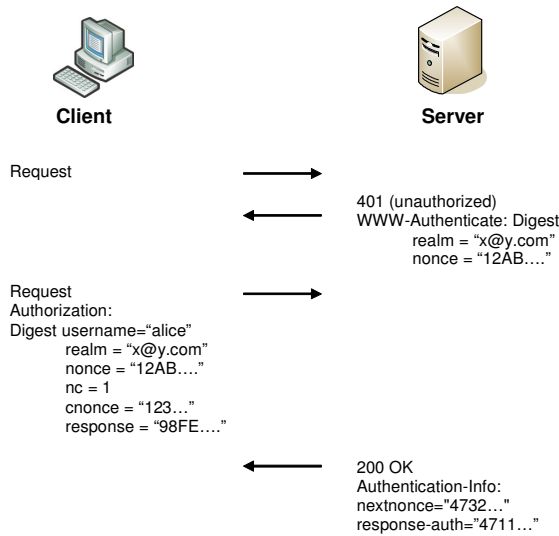


Figure 7. HTTP Digest Authentication

To avoid the doubling of all message exchanges the challenge for the next exchange can be transmitted as part of the response message to the initial request as optimization of this method. The next nonce mechanism in combination with the initial application of username and password can be used to form a (weak) cryptographic session.

B. Candidate 2 H.235 based security

H.323 is an umbrella recommendation defined by the ITU-T (International Telecommunication Union) to address call control, multimedia management, and bandwidth management in telecommunication environments. H.235 is also an ITU-T based standard describing security functions for the multimedia communication standard H.323. H.235 features in summary nine different profiles, were only some of them are interesting to be discussed in the context of leveraging them for the securing of MMS:

- **H.235.1** provides signaling integrity and authentication using mutually shared secrets and keyed hashes, based on HMAC-SHA1-96. This profile is widely implemented in available H.323 solutions.
- **H.235.2** provides signaling integrity and authentication using digital signatures on every message in gatekeeper-routed scenarios. Since signature generation and verification is costly in terms of performance, this profile may not gain momentum and is stated here rather for completeness.
- **H.235.3** is a hybrid approach using both, H.235.1 and H.235.2. During the first handshake a shared

secret establishment is performed, protected by digital signatures. Afterwards keyed hashes are used for message integrity protection, based on the established shared secret.

The syntax of the H.323 messages is depicted in Figure 8. As it can be seen, security is provided based on an included crypto token in the message, which transports all necessary data to integrity protect the message.

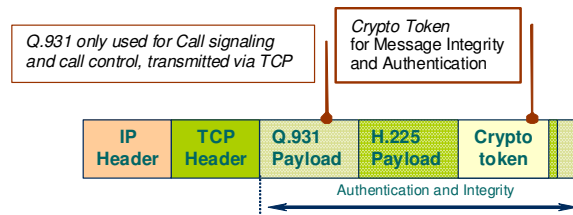


Figure 8. H.235 protected message

As H.235.3 allows for a hybrid security approach, utilizing asymmetric and symmetric cryptography, the crypto token is defined to serve for both approaches at once and carries all necessary information for both phases.

C. Candidate 3 XML Security

The Extensible Markup Language (XML) is a simple, very flexible text format, which is defined by the W3C (World Wide Web Consortium). It specifies a set of rules for encoding documents in machine-readable form and is meanwhile used in a variety of applications and builds the base for message structures in several protocols and language derivations.

The W3C also provides recommendations for security of XML data. XML security comes in two flavors, XML Encryption and XML Signature. Both can be used on XML encoded data in so-called XML elements and provide privacy and integrity protection. XML encryption allows the encryption of any type of data with symmetric and asymmetric methods. The key to be used can be selected by key names. XML signature on the other side applies asymmetric methods to achieve integrity protection and non-repudiation and can be included in the XML document directly or provided in a detached fashion (see also [18]).

VIII. PROPOSED ENHANCEMENTS OF IEC62351

Based on the discussion of candidates in the previous section and the fact that integrity protection is the first protection goal in energy automation networks, the approach of candidate 1 and 2 and their application to

MMS is discussed here further, as they allow the integrity protection of application layer messages based on an cryptographic authenticated and integrity protected session. The application of a hybrid approach as in candidate 2 in this context, using asymmetric key material for the authentication and protection of a session key establishment and symmetric key material for the remaining session provides for a high flexibility while keeping the load on the system low during the application of the symmetric key. This cannot be achieved with candidate 1.

Candidate 3 is not discussed further here as directly it maps to web services instead of MMS. IEC 61400-25 (for wind power plants) describes a mapping of IEC 61850 services to web services. Moreover, other approaches like OPC-UA (Object Linking and Embedding for Process Control – Unified Architecture) also apply web service technology and may also be used in this context. As for web services own security measures are defined (e.g., XML security), these security measures may be applied straight forward. Nevertheless, these possibilities should be kept in mind, to provide an adequate security level for MMS, operating at the same level as web-services. This is especially important for the protocol interworking when different transport mappings are used.

Again, the goal is the enhancement of MMS-based communication to allow multiple parallel distinguishable integrity protected sessions started with the MMS Initiate command and proper authentication (and authorization).

Providing this security session approach can generally be done in different ways:

1. Enhancement of commands transported via MMS with security tokens to allow authentication and authorization to be bound to the messages directly. This approach would be independent of MMS security and thus may be applied over other transports as well.
2. Enhancement of MMS itself to allow security services on the layer transporting IEC 61850 commands. This approach requires fewer changes in the current message structure and better interoperates with other approaches, like security options for web services.

The enhancement of the MMS messages itself requires changes in IEC62351 Part 4 for security of MMS communication as currently only the MMS initiate command has the appropriate ASN.1 structures to

transport the security information. It also requires changes in the IEC 61850 standard to provide the necessary integrity field carrying the security parameters as a base for the introduction of a cryptographic session concept.

Therefore, the current approach of MMS must also be enhanced to provide not only authentication, but also integrity protection. This means the current description of the signature calculation in IEC62351 Part 4 needs to be revised.

The following discussion relates to candidate 1 and 2 explained in the previous section:

The basic idea for both approaches, the enhancements of the syntax of the commands send via MMS (case 1 above) or of the MMS message syntax (case 2 above), is the enhancement of the datagram with a substructure to transport all necessary security information. This change may be done as Figure 9 suggests, based on the investigation into the realization of candidate 2 in the previous section.

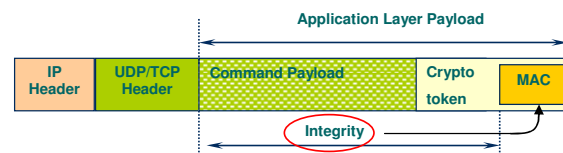


Figure 9. Message protection using a crypto token

The application of a *crypto token* provides a dedicated security container to transport message authentication codes and additional information, e.g., necessary to setup a session key.

An alternative addressing only message integrity on application layer without enabling the transport of key establishment values for the integrity protection is depicted in Figure 10. This approach would be suitable, when focusing on candidate 1.

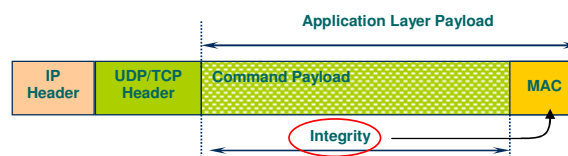


Figure 10. Message integrity protection

For the following discussion, the approach using a *crypto token*, as depicted in Figure 9 is favored as it offers most flexibility. The command payload may be seen either on MMS level (Layer 6) or on application level (Layer 7). In any case, the *crypto token* to be included in the payload carries at least (necessary pa-

parameter should be discussed, depending on the solution approach; the following list may not be complete):

- tokenOID Object identifier
- certificate certificate information
- timestamp Timestamp
- sequence Sequence number
- random nonce value
- dhkey Diffie Hellman set (to negotiate a session key)
- receiverID Receiver Identifier
- sendersID sender Identifier
- hashed message authentication code based on keyed hash (HMAC)
- signed message authentication code based on signatures

The inclusion of the *crypto token* in the messages enables the following functionality:

1. Authentication of connected to and connecting peer during first message exchange, here during the MMS Initiate. Based on the chosen credentials, this may be done using either symmetric or asymmetric long term keys (hashed or signed).

2. Negotiation of a session key during the first handshake to be used for all subsequent messages in this session. This may be done by using for instance the Diffie Hellman Key Agreement, were both, the client and the server provide to the session key. The session enables the distinction of messages sources in terms of applications or users.
3. Integrity protection of messages on application layer. In scenarios, were multiple hosts are traversed this approach does not require to trust an intermediate hosts to not alter messages contents. The intermediate hosts needs only to be trusted to deliver the message.
4. Replay protection through the use of timestamps and sequence numbers or nonce's alternatively.

A potential call flow between a control center and a field device via a substation controller using the described approach of candidate 2 using the MMS layer is shown in Figure 11. This figure also merges the existing energy automation systems with roles and systems of smart grid scenarios with residential integration as shown in Figure 4.

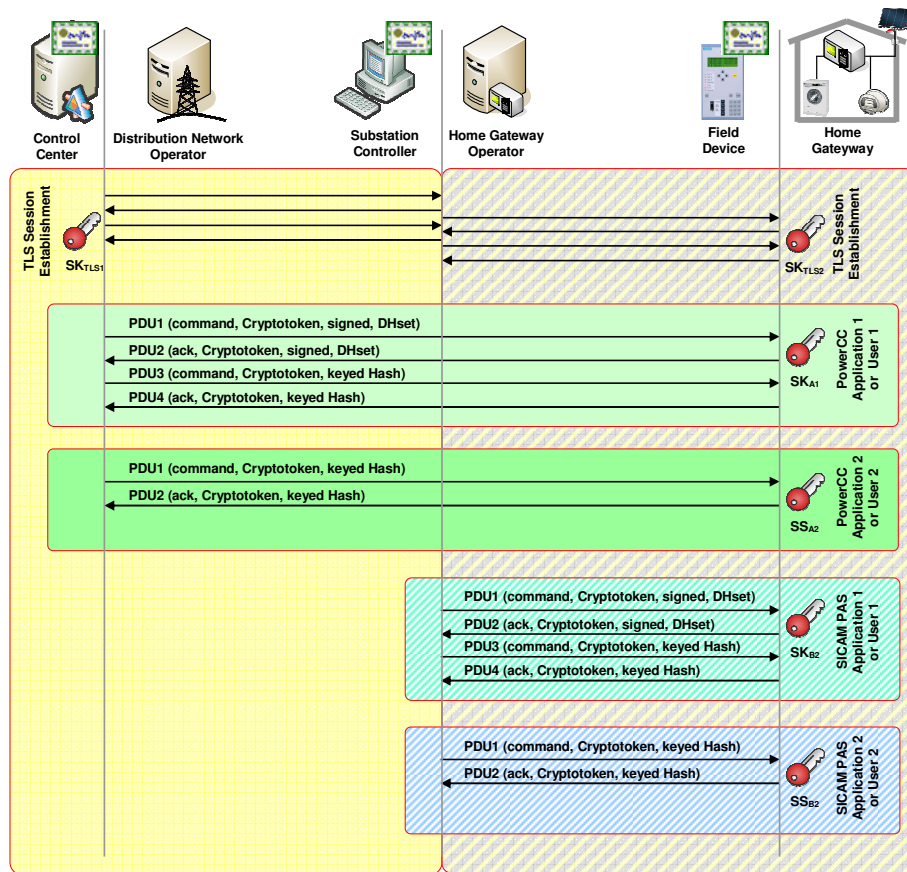


Figure 11. Security enhanced call flow

The following description explains this call flow:

- At first a TLS connection is established on both hops. Here, TLS negotiates session keys on transport level on both hops: SK_{TLS1} and SK_{TLS2} .
- Afterwards an application/user A1 on the control center issues a command to the field device. As this is the first command for this application/user, the command is authenticated using the long term credential (e.g., digitally signed). The acknowledgment in turn is secured using the long term credential of the field device. During the handshake a session key may be established SK_{A1} using a Diffie Hellman key agreement. This session key may then be used to secure all subsequent traffic between A1 and the field device. The command is send via the TLS protected hops via the substation controller to the field device.
- A second application/user A2 on the control center issues a further command to the field device. As both communication parties possess a shared secret SS_{A2} , it is used to secure the message exchange applying a keyed hash (e.g., HMAC-SHA1). The command is send via the same TLS protected hops via the substation controller to the field device.
- Then an application/user B1 on the substation controller issues a command to the field device. As this is the first command for this application/user, the command is authenticated using the long term credential (e.g., digitally signed). The acknowledgment in turn is secured using the long term credential of the field device. During the handshake a session key may be established SK_{B1} . This session key may then be used to secure all subsequent traffic between B1 and the field device. The command is send via the TLS protected hop to the field device.
- A second application/user B2 on the substation controller issues a further command to the field device. As both communication parties possess a shared secret SS_{B2} , it is used to secure the message exchange applying a keyed hash (e.g., HMAC-SHA1). The command is send via the same TLS protected hops via the substation controller to the field device.

The advantage of this approach is that single TLS connections can be used on the hops to secure the transport between all involved peers, while multiple applications or users may use these TLS connections to transport specific commands to the field devices. Moreover, due to the session concept, the long term credentials need only to be used during the first handshake, while all other communication can rely on the

negotiated session keys. If digital signatures are performed during the first handshake, performance can be saved on all further messages of this application connection, as the keyed hash operation is less consuming compared to a signature generation or verification. The approach as shown in Figure 11 is suitable for both, MMS or direct command integration.

IX. FUTURE WORK

As already stated in chapter VI, Web Services are gaining more momentum. They have already been addressed as part of the wind power craft related standard IEC 61400-25 and it is expected that there will be a mapping for IEC 61850 in the near future. Web services are also one building block in the OPC-UA framework initially mentioned were security functions already being considered on transport and application layer.

Web services enable the application of Web security mechanisms like XML Security to provide encryption and integrity protection. Moreover authorization can also be addressed utilizing the Security Assertion Markup Language (SAML). SAML allows the definition of secured tokens, to be issued by a trusted component. Currently, security is also not being addressed in the wind power standard. Nevertheless, as web service security is already defined (by the W3C), the standard only needs to be enhanced with a mapping to the available web security, without the necessity to defined own security mechanisms.

To ensure security interworking between installations utilizing different mappings of IEC 61850 like MMS or Web Service secure services transition functions need to be defined. Therefore, from the interworking perspective, the integration of security enhancements in MMS may provide a better base for secure interworking as it operates on the same level as web services and already provides an end-to-end application layer connection.

X. CONCLUSION

This paper provides an overview of smart grid environment focusing especially on the security of dedicated new scenarios, which become more likely through the integration of renewable energy sources not only on substation level, but also on end-user level. Additional security requirements will be the result of these new use cases. The energy automation security standard IEC 62351, which is used to secure communi-

cation according to the standards IEC 61850 and IEC 60870-x and to provide End-to-End Security plays a major role here. Because of the manifold Smart Grid activities and the standardization efforts driven by NIST, new parts of IEC 62351 can be expected soon. Motivated by the analysis of new use cases for Smart Grids, some shortcomings of IEC 62351 are presented. Especially, IEC 62351 can currently not offer application layer end-to-end security if multiple transport layer connections are used. Such multi-hop connections are important for new use cases. Currently, often a trusted intermediate is assumed for application layer end-to-end security. This assumption may be a weakness in the overall system design depending on the use case and may not hold in the future.

An extension of IEC 62351 is proposed to overcome the identified weaknesses by introducing security sessions for MMS connections in IEC 62351. The extension enables cryptographic sessions on application layer providing application layer end-to-end security for new use cases in Smart Grid scenarios.

REFERENCES

- [1] Fries, S.; Hof, H-J; Seewald, M.: The Fifth International Conference on Internet and Web Applications and Services – ICIW 2010: “Enhancing IEC 62351 to Improve Security for Energy Automation in Smart Grid Environments”, May 2010, ISBN 978-0-7695-4022-1
- [2] NERC, North American Reliability Corporation, last access February 2011: <http://www.nerc.com/page.php?cid=2120>
- [3] BDEW – Bundesverband der Energie- und Wasserwirtschaft, Datensicherheit, last access January 2011: http://www.bdew.de/bdew.nsf/id/DE_Datensicherheit
- [4] NIST, National Institute of Standards and Technologies, Smart Grid Interoperability Project, last access January 2011 <http://www.nist.gov/smartgrid/>
- [5] NIST Framework and Roadmap for Smart Grid Interoperability Standards, Version 1.0, last access January 2011, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf
- [6] NIST IR 7628 Guidelines for Smart Grid Cyber Security, Vol. 1 Smart Grid Cyber Security Strategy, August 2010, last access January 2011: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
- [7] NIST IR 7628 Guidelines for Smart Grid Cyber Security, Vol. 2 Security Architecture and Security Requirements, August 2010, last access January 2011: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf
- [8] NIST IR 7628 Guidelines for Smart Grid Cyber Security, Vol. 3 Supportive Analyses and References, August 2010, last access January 2011: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf
- [9] RFC2617: HTTP Authentication: Basic and Digest Access Authentication, J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart, June 1999
- [10] RFC 5246: The Transport Layer Security (TLS) Protocol, Version 1.2, T. Dierks, E Rescorla, August 2008
- [11] ISO-IEC 61850, Part 1: Introduction and Overview, May 2003
- [12] ISO-IEC 61850, Part 8-1: Specific Communication Service Mapping (SCSM) – Mappings to MMS (ISO 9506-1 and ISO 9506-2) and to ISO/IEC 8802-3, May 2004
- [13] ISO-IEC IEC 61400, Part 25-4: Communications for monitoring and control of wind power plants – Mapping to communication profile, August 2008
- [14] ISO-IEC 62351, Part 4: Communication Network and System Security – Profiles Including MMS, October 2006
- [15] ISO-IEC 62351, Part 5: Security for IEC 60870 and Derivatives, February 2007
- [16] ISO-IEC 62351, Part 6: Security for IEC 61850, October 2006
- [17] H.235.0: Security framework for H-series, ITU-T, 2005
- [18] XML Signature Syntax and Processing (second Edition), W3C Recommendation, 10.June 2008, last access January 2011: <http://www.w3.org/TR/xmlsig-core/>