End-to-End Secure Application Interactions over Intermediaries on the Example of Power System Communication

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

***Abstract*—End-to-end security is often a requirement for interacting systems, including energy automation systems. As the term can be interpreted on different layers of the Open System Interconnection (OSI) reference model, it is necessary to clearly define the end points that need to provide or rely on the exchanged data. Connecting client and server applications directly via a transport connection allows the usage of existing security protocols directly, as known from classical Web applications. Typically, Transport Layer Security (TLS) is applied to protect the communication link end-to-end. This approach is utilized in substation automation of energy grids to protect the Transmission Control Protocol (TCP/IP)-based communication between a substation controller and a protection relay applying mutual authentication of the end points. Here, the communicating end points on the application layer terminate in the same entity as the transport layer end points, which essentially provides end-to-end security on a component level. If a direct communication link is not available, communication is realized over an intermediary system. Providing end-to-end security over multiple communication hops, including mutual endpoint authentication (client and a destination application service) as well as integrity and confidentiality of communicated data, deserves specific attention, even if the communication hops with the intermediary are protected hop-by-hop by security protocols like TLS. In power system automation, this kind of communication involving an intermediary is used with publish subscribe protocols, e.g., when integrating Decentralized Energy Resources (DER) or when integrating smart meters in the German Smart Meter Gateway architecture. This paper investigates existing solutions and specifically analyses the end-to-end security approach defined for power system automation within the International Electrotechnical Commission (IEC). A broader application of end-to-end security using session-based communication over intermediaries is desired.**

Keywords—security; device authentication; end-to-end security; multi-hop security; IEC 62351; Publish/Subscribe.

I. INTRODUCTION

Critical Infrastructures (CI) are technical installations that are essential for the daily life of a society and the economy of a country. Examples of CI are provided by technical systems in different application domains like healthcare, telecommunication, transportation, water supply, and power systems. The latter are taken as focus in the context of this paper. In all application domains, there is a clear trend towards increased connectivity and a tighter integration of systems from Information Technology (IT) in common enterprise environments with the Operation Technology (OT) part of the automation systems in the energy and other industrial domains.

This integration enables an enhanced and automated data exchange between industrial systems and IT systems to provide enhanced services. It becomes clear that this integration also requires security measures to avoid negative effects of the formerly isolated OT through control options and to ensure the quality of data provided to the IT for further processing regarding authenticity and integrity but also regarding protection of privacy and potentially know how. Furthermore, this integration also leads to potential physical effects through processing of the provided data. Typically, IT and OT environments have different characteristics in management and operation, which led to distinct domain specific security requirements. This must be considered when designing interconnected cyber-physical systems.

Security in power system communication is getting more momentum [1]. Communication technologies applied in power systems are manifold and comprise, e.g., serial communication in the context of telecontrol. In addition, communication based on the Transport Control Protocol (TCP) is used for monitoring, control, and maintenance of power systems. Multicast Ethernet based communication as further technology is applied in the context of protection relays in substation automation, were real-time capable communication is required. In many scenarios, the security associations established on the transport layer also protect the application layer connection as both terminate at the same entity. But there are scenarios which require multiple consecutive transport connections to exchange application layer data between a sender and a receiver. This paper focuses on the application layer interaction of two entities and the protection of the application data in an ideally transport connection independent manner. The focus is placed on the discussion of secure application layer end-to-end interactions by addressing authenticity, integrity, and confidentiality to ensure reliable control and monitoring of the system.

Nevertheless, for the overall system, there are also privacy related considerations that have to be addressed to

avoid misuse of the exchanged and collected person-related information. This is obviously necessary for information that can be associated with a single household or a single user, which could be the case for smart meter information, but may also be relevant if provider-based services are used to provide customer-specific information in an online fashion. Although the security discussed here can be leveraged to also address certain privacy properties, privacy specific measures are not in the main focus of this paper.

The remaining part of the paper is structured as follows. Section II provides examples for security requirements for communicating systems, which have been formulated in guidelines and standards or are required by legislation. Section III describes the communication overview of the target scenario and derives high level security requirements to be addressed by specific technical means. These requirements are taken into consideration later in the description of the security approach taken for the integration of Decentralized Energy Resources (DER) into the power system based on IEC 61850. Section IV investigates a selection of existing approaches to provide end-to-end security (message-based and session-based methods). Section V provides more insight into the actual design and application of the protocol defined in IEC 62351-4 to motivate broader application. Section VI provides an evaluation of the investigated application layer security options regarding a derived set of requirements. Section VII concludes the paper with an outlook.

II. Examples of Security Requirements Formulated in Regulation/Guidelines/Standards

Security in communication infrastructures is not a new topic. In office environments or information technology (IT), it is handled as state of the art, and depending on the operational environment certification requirements of specific security processes is mandatory, or at least provides a competitive advantage.

Critical infrastructures or operational technology (OT) on the other hand also rely on communication and utilize increasingly standard communication protocols or standard components whenever possible. This provides some commonalities regarding the utilized technology for communication, but there are distinct differences in the management and operation of these infrastructures as seen in Figure 1.

	Critical Infrastructures, e.g., Power Systems	Office IT
Protection target for security	OT, e.g., generation, transmission	IT- Infrastructure
Component Lifetime	Up to 20 years	3-5 years
Availability requirement	Very high	Medium, delays accepted
Real time requirement	Can be critical	Delays accepted
Physical Security	Very much varying	High (for IT Service Centers)
Application of patches	Slow (in maintenance windows)	Regular / scheduled
Anti-virus	Hard to deploy, white listing	Common / widely used
Security testing / audit	Increasing, partially	Scheduled and mandated

Figure 1. Comparison IT/OT management and operation

These differences in management and operation of the IT systems consequently lead to different high level security requirements as outlined in Figure 2.

	Critical Infrastructures	Office IT
Security Awareness	Increasing	High
Security Standards	Under development, regulation	Existing
Confidentiality (Data)	Low – medium	High
Integrity (Data)	High	Medium
Availability / Reliability	24 x 365 x ...	Medium, delays accepted
Non-Repudiation	Medium to High	Medium

Figure 2. Comparison IT/OT high level security requirements

For critical infrastructures, the European Network and Information System (NIS) Directive [2] requires security measures to be supported by the system operator. This directive has been ratified by the European member states. Germany, for instance, has passed the Information technology (IT) Security Act already in 2015 [3], which requires the definition of domain-specific security standards that have to be implemented by operators of critical infrastructures. For the power system infrastructure, the domain specific security standard is provided by ISO 27019 [4] in conjunction with the IT security catalog of the German BNetzA [5]. Both documents target communication security in terms of authentication of communicating entities in addition to integrity and confidentiality protection of the data exchange, but without specifying specific technical means in terms of security protocols or security mechanisms to be used. A further document to be stated here is the BDEW White Paper [6]. This guideline has been developed by the German Association of Energy and Water Industries ("Bundesverband der Energie- und Wasserwirtschaft" (BDEW), addressing communication security requirements in operations of energy and water utilities. This white paper was one main source for developing ISO 27019.

Security requirements for critical infrastructures are also defined outside Europe, for instance in requirements specified by NIST Cybersecurity framework [7] and specifically for the power system infrastructure by the North American Energy Reliability Council in the NERC Critical Infrastructure Protection (CIP) standards [8]. These documents pose similar requirements, which relate most often to the security processes of an operator and only partly to supporting technology. Common to all requirement documents is that additional standards/specifications are necessary to address the technical implementation of such requirements in components and systems, while ensuring interoperability between different vendor's products. The combination of both, procedural and technical security measures provide the necessary support for reliable operation of critical infrastructure systems.

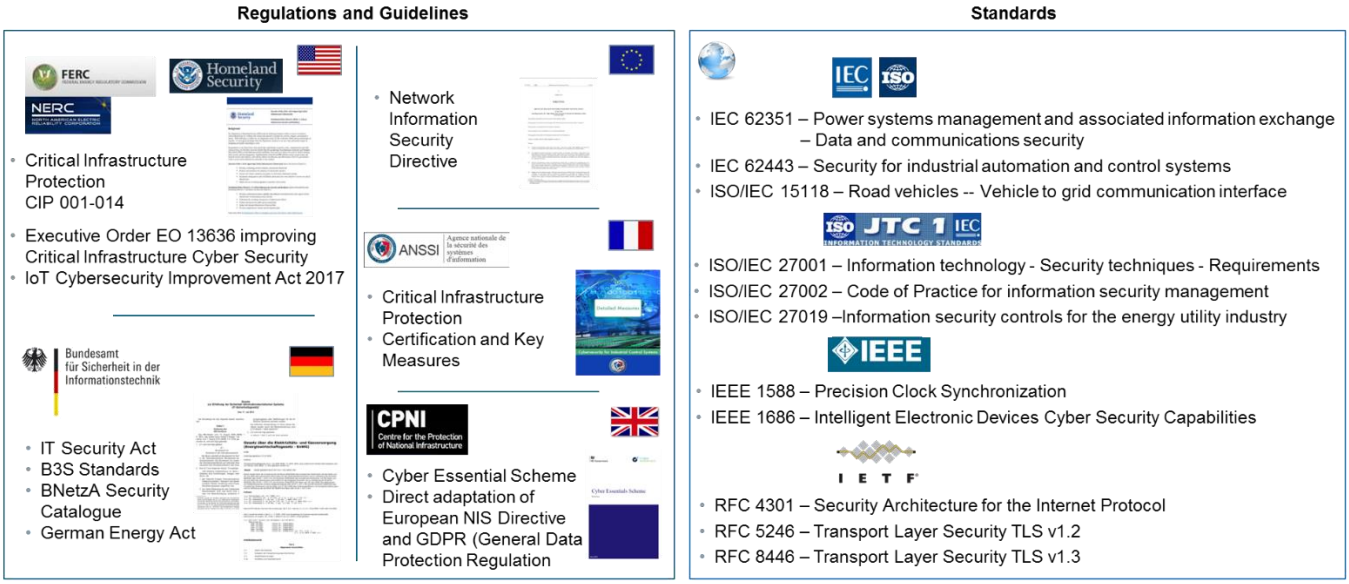

Figure 3. Examples for security requirements in regulation and standardization for critical infrastructures as power systems

A standard defining specific technical requirements is provided by the framework IEC 62443 [9]. Beyond other, it describes in two distinct parts technical requirements on system and component level, targeting four different security levels, which relate to the strength of a considered attacker. The framework also addresses also communication security.

Besides these technical requirements, different standards and draft standards exist that address concrete measures for entity authentication, integrity protection, and confidentiality protection on a level ensuring interoperability between different vendors' systems. One example for such a standard protecting specifically TCP/IP based communication is provided by the Transport Layer Security Protocol (TLS 1.2 [10], TLS 1.3 [11]). TLS is a widely used security protocol and most commonly known from the protection of web-based communication, e.g., when accessing a specific web resource. Meanwhile, TLS is applied in further standards to protect domain specific communication protocols.

An example here is the standard ISO 15118 [12], which utilizes TLS to protect the charging related control communication for electric vehicles. A further example is IEC 62351 [16], a framework providing security for data in transit and data at rest in power system automation.

As analyzed in [1] and [13], the necessity to support communication over multiple hops between two entities in power system automation has been emphasized by the support of Decentralized Energy Resources (DER). Integrating DER into the current energy distribution network requires to monitor and control these DER to a similar level as centralized energy generation in power plants to keep the stability of the power network. To cope with the fact that DER are typically operated within a private operator network protected by a firewall, the standard IEC 61850-8-2 [14] defines a communication approach based on the eXtensible Messaging and Presence Protocol – XMPP [15]. Here, both sides, the DER controller, as well as the control center, connect to an intermediate server node, which facilitates the communication between both entities. In this specific case, the standard IEC 62351-4 [16] ensures that the communication between the control center and the DER is secured in an end-to-end fashion. Meanwhile, this standard has been released and will be compared to other existing or currently developed solutions.

The following section elaborates technical means to address these requirements focusing securing communication in an end-to-end fashion.

III. Communication Architecture and Derivation of Technical Security Requirements

The discussion of requirements and matching security features and solutions is best done on a concrete use case. Examples for multi-hop communication in power system automation are provided by the integration of DER into distribution networks, the integration of smart meters into a meter data management solution or the connectivity to cloud services providing enhanced data services. Common to all of them is that an intermediary is necessary to support interconnection by providing a rendezvous functionality.

A. Communication architecture

For the discussion of end-to-end communication, the integration of DER resources into a power system control network is taken as example, see Figure 4. The lower part of the figure shows the distributed power generators, which may be photovoltaic systems or wind power systems. These are managed by the control function shown in the upper part as control center. The control function may be located at a Distribution Network Operator, a virtual power plant operator, or at a smart energy market operator. All entities are connected via a communication network in which the intermediary XMPP server in the middle provides the connectivity between the control center and the DER

controller. All entities essentially work as XMPP clients connecting to the XMPP server, working as dispatcher by facilitating the data exchange between the different XMPP clients. In addition, each XMPP client has a specific functionality from an application perspective. The DER resembles a server, providing power infeed into the distribution network, and provides information by regularly publishing generated power values. The control center in turn works as application client, consuming the generation values to generate a system wide view. Besides the monitoring of generation, the control center may also provide information to the DER devices to control the infeed into the distribution network. For this, the same communication channel is used.

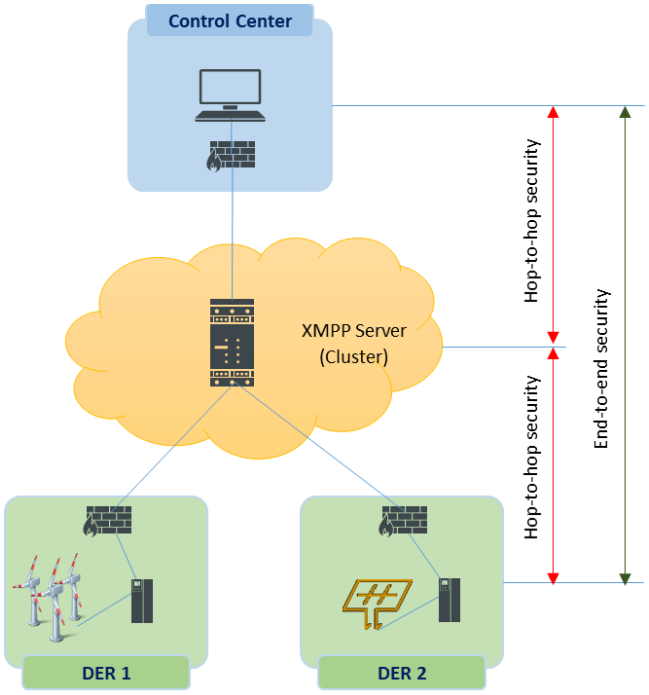

Figure 4. DER Integration based on IEC 61850 over XMPP

The data exchanged between the DER controller and the control center comprises different types of data:

– Customer data, which may be identification information, location data, consumption data or other information belonging to the DER owner.
– Control data, which may be either commands issued by the control center, or event and monitoring information from the DER controller.
– Market data, which may be tariff information provided from a marketplace via the control center or directly (not shown in Figure 1) to the DER controller.

In the context of utilizing IEC 61850 to connect DER to a control center, the communication between the DER controller and the XMPP server is secured using TLS as transport layer security protocol. The same holds for the connection between the control center and the XMPP server. Note that the XMPP server may belong to a different administrative domain and may therefore not be trusted to access the data exchanged between the DER controller and the control center. Hence, the communication relation between the DER controller and the control center is secured at application layer using IEC 62351-4, which will be analyzed in more detail in Section V.

B. Derivation of Technical Security Requirements

As stated in the introduction, there are different types of security requirements stemming, on one hand, from the obligation to comply with international and national regulations. On the other hand, security requirements are derived from the system architecture based on a risk-based approach. The international industrial security standard IEC 62443 [9] is a security requirements framework jointly developed by the International Electrotechnical Commission (IEC) and the International Society of Automation (ISA99) to address the need to design cybersecurity robustness and resilience into Industrial Automation and Control Systems (IACS). The standard covers both organizational and technical aspects of security over the life cycle of systems. It can be used in conjunction with ISO/IEC 27019 (the Information Security Management System (ISMS) profile for the energy domain based on ISO 27002) and with IEC 62351, providing specific security solutions. Here, the parts IEC 62443-3-3 (focus on system security requirements) and IEC 62443-4-2 (focus on component security requirements) can be used in the context of a risk-based approach, as they specify technical security requirements for four security levels, corresponding to different strengths of an attacker. For both views, system and component, foundational requirements groups have been defined. For each of the foundational requirements, several concrete technical Security Requirements (SR) and Requirement Enhancements (RE) to address a specific security level exist.

The overall approach applies to the systems and the communication connections are shown in Figure 4. In the context of this paper, the focus is placed on the communication relations, to address the specific target of providing communication security over potentially untrusted nodes. The protection of the communication is addressed by different security requirements focusing on end-to-end security and hop-to-hop security. Note that the hop-to-hop security requirements contribute to the overall system security approach and may be used in conjunction with the end-to-end security. Note that the end-to-end security is intended to be independent of the hop-to-hop security as the endpoints may not have control about the hop-to-hop security setup.

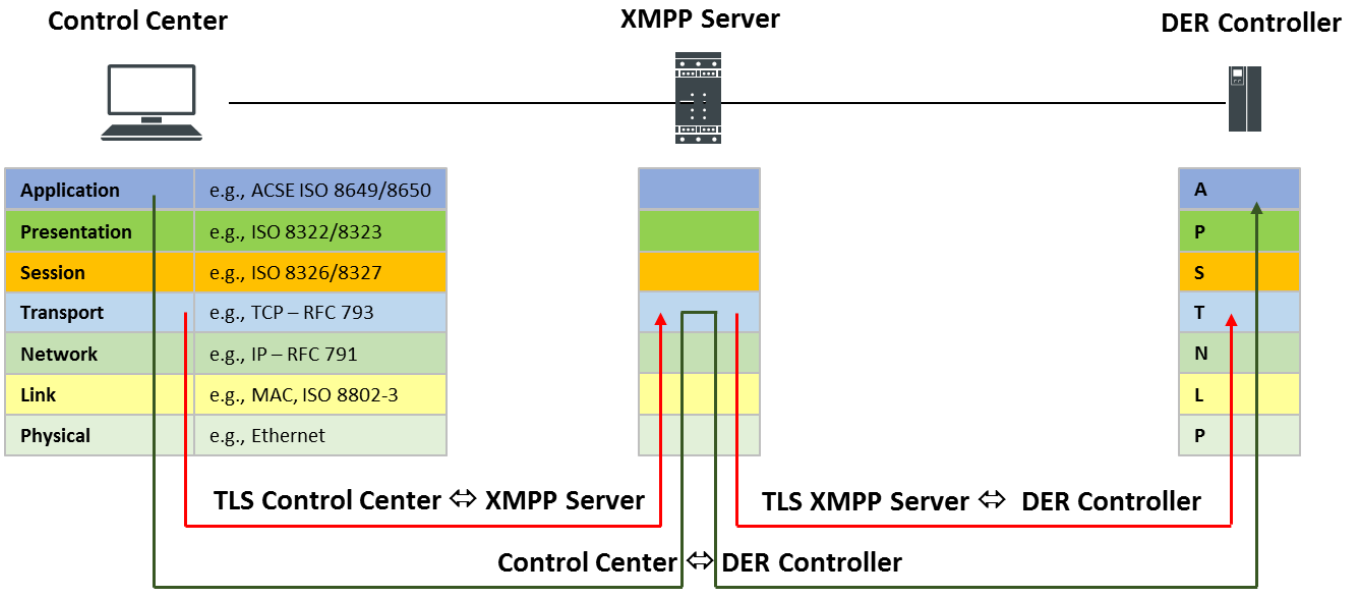

Figure 5. End-to-end-Security and hop-by-hop security according to IEC 62351-4

Figure 5 shows the data exchange between the control center and the DER controller via the XMPP server. The security requirements comprise specifically:

[R 1] End-to-end authentication between the DER controller and the control center to ensure identification and authentication of the communicating endpoints.

[R 2] End-to-end integrity protection to ensure that data in transit has not been tampered with (unauthorized modification) between the DER controller and the control center.

[R 3] End-to-end confidentiality protection to ensure that data in transit has not been accessed (read) in an unauthorized way by the XMPP server. Note that this requirement may not be generally applicable. Use cases exist in which intermediaries need to access the transmitted information. For these use cases the requirements [R 1] and [R 2] may be sufficient.

Hop-to-hop authentication between the XMPP client (DER controller, control center) and the XMPP server is used to identify and authenticate an intermediary system proxying the end-to-end communication between the DER controller and the control center.

IV. Security Measures on Application Layer

This section investigates a selection of existing end-to-end security approaches, which can be used to provide authentication, integrity, and confidentiality. Note that XMPP enhancements to achieve end-to-end security between the clients connected via the XMPP server have already been discussed as part of [13]. The IETF originated drafts discussed in this paper are already outdated and have not been updated in the last years. Therefore, they are not considered further here.

In the following examples of existing standards or standards in development supporting end-to-end security on application layer, are summarized. They are distinguished into message-based approaches and session-based approaches. Message-based approaches are independent of the actual communication session and can be applied to single messages. They typically rely on security credentials, which are setup out of band. These security credentials are applied to the messages directly. Session-based approaches rely on a communication connection, which comprises at least an initialization phase setting up security credentials to be used in the established session only and a data exchange phase. The establishment of the session related security credentials may be bound to long term security credentials of the respective entities. Both approaches have their merits, but also certain drawbacks.

A. *Message-based security*

The following examples target the protection of single messages and do not rely on an established communication connection. They utilize existing security credentials to protect the messages. In general, this type of security is best for occasionally exchanged messages but not necessarily for a consistent data exchange or bulk data exchange. All of the provided examples support the requirements [R 1], [R 2], and [R 3]. Note that confidentiality protection [R 3] is optional.

– IETF RFC 3923 [17] describes end-to-end signing and object encryption utilizing S/MIME to protect the messages exchanged over XMPP connections. This approach is similar to using secure email. It provides end-to-end authentication based on a digital signature

and confidentiality protection based on symmetric encryption. As this approach targets message-based communication, without a communication session it will result in a higher per message overhead, as the messages are protected using symmetric encryption, while the key for the symmetric encryption is encrypted with the recipient's public key. This approach has two drawbacks. It is performance intensive due to the use of asymmetric operations and it is bound to RSA as asymmetric algorithm. Newer algorithms like ECDSA based on elliptic curves may not be used.

- W3C defined XML security may also be used to address a secure data exchange on application layer. There are two different standards available, which are already utilized to provide security: XML Signatures [18] and XML Encryption [19]. Both can be used in conjunction, ideally on XML encoded data in so-called XML elements and support the given security requirements. XML encryption allows the encryption of any type of data with symmetric and asymmetric methods. XML signature on the other side applies asymmetric methods to achieve integrity protection and non-repudiation. Note that there exist adequate standards for the binary data representation to safe bandwidth during transfer.
- The IETF working group for JavaScript Object Signing and Encryption (JOSE) defined two further standards, which can be used to protect messages encoded in JavaScript Object Notation (JSON). IETF RFC 7515 [20] specifies JSON Web Signatures, while IETF RFC 7516 [21] defines JSON Web Encryption. The combination of both documents is similar to XML documents developed by W3C for specific JSON encoding.
- A further IETF standard is provided with RFC 8152 [22] defining authentication, integrity protection, and confidentiality protection for Concise Binary Object Representation (CBOR), which enhanced the data model of JSON with a binary representation. This approach allows for enveloping and encryption of arbitrary message blocks.

B. Session-based security

The following examples target the protection of communication sessions for application data exchanges. For this, it is assumed that a communication session is established between two entities during which both participants can authenticate and negotiate a set of session keys for protecting further communication. This approach has the advantage for consecutive communication to result in less overhead for the bulk data handling as part of the communication session. This is due to the fact that the combination of symmetric encryption and an additional integrity protection or the direct application of authenticated encryption has a much better performance instead of invoking asymmetric cryptography on a per packet base.

- An IETF standard focusing on object security is RFC 8613. It defines a method for application-layer protection of the Constrained Application Protocol (CoAP), using CBOR Object Signing and Encryption (COSE) called Object Security for Constrained RESTful Environments (OSCOR). This standard defines that client and server establish a shared security context used to process COSE objects. It utilizes pre-shared keys (PSK) for the security context, which are expected to be established out of band or by a different key management protocol. Therefore [R 1] is met with restrictions. For the object protection OSCOR builds on Authenticated Encryption with Associated Data (AEAD). This has to be kept in mind, as it therefore always addresses [R 2] and [R 3].
- IETF draft on Application Layer TLS [24] leverages the existence of a TLS implementation on the communicating entities. The approach utilizes the option of TLS stacks to create and process TLS records based on access to the byte buffer. Based on this, the TLS packets may be transmitted over arbitrary transport connections. The draft targets two different application scenarios, as there is the transport over non-IP networks like Zigbee and the transport over IP based networks. This approach has the advantage that the application layer security immediately benefits from new cipher suites and cryptographic algorithm support by the underlying TLS stack. In addition, several TLS stacks allow key material export using the approach defined in IETF RFC 5705 [25] to leverage the TLS key agreement and to utilize the negotiated key in the context of other protocols. Essentially, ATLS copes with all of the requirements [R 1], [R 2], and [R 3]. Note that when used with TLS 1.3, ATLS will always provide end-to-end confidentiality protected transport.
- Off-the-Record (OTR) [26] is a protocol developed for messenger applications to ensure integrity and confidentiality and most notably plausible deniability. Starting from version 2 of the protocol, peer authentication is also supported. Here, shared keys are utilized to achieve the authentication. The development stopped in 2016. OTR directly addresses the requirements [R 2] and [R 3].
- Signal [27] is another protocol used in messaging systems. It is based on OTR and allows to establish a secure session based on an authenticated triple Diffie Hellman key agreement in which EdDSA signatures are employed for integrity protection during the key establishment phase. The negotiated key material is applied to protect the integrity and confidentiality of the established session based on the Double Ratchet algorithm. It ensures ongoing renewal and maintenance of short-lived session keys. Note that peer authentication is not directly supported by signal. Note also that Signal supports plausible deniability, which

may not be desired in industrial environments to be able to ensure an audit trail. Signal therefore focuses on the requirements [R 2] and [R 3].

– Application Layer Transport Security (ATLS) [28] has been developed by Google in 2017 and is utilized to secure Remote Procedure Calls (RPC). The protocol is defined in a similar way as TLS, consisting of a handshake protocol and a record protocol. It allows for mutual authentication and session integrity and confidentiality. Authentication is bound to an entity rather than an instance (e.g., hostname) as the approach targets mainly cloud environments. Note that there are tradeoffs to TLS described in the specification [28], which relate to privacy concerns for the handshake messages and perfect forward secrecy. Note that these properties are supported out of the box in TLS 1.3, but not in TLS 1.2 and below. ALTS directly addresses the requirements [R 1], [R 2], and [R 3].

V. END-TO-END SECURITY DESIGN IN IEC 62351-4

The security requirements derived in Section III.B for providing application layer end-to-end security supporting DER integration are reviewed and enhanced to better address the target scenario to:

[R' 1] Peer authentication between the DER controller and the control center (mutual authentication) based on X.509 certificates.

[R' 2] Integrity protection of exchanged data to ensure that data in transit has not been tampered with.

[R' 3] Optionally, confidentiality protection to ensure that an intermediary cannot access the content of the data exchange. The reason for handling this requirement as optional is based on the necessity in some deployment scenarios that at the security perimeter an inspection of the data may be required. By allowing a mutual authenticated and integrity protected communication connection, the communication may be monitored, e.g., if the control commands cope match a certain system state or to support an audit trail.

[R' 4] Session key management supporting initial key agreement providing perfect forward secrecy (PFS) as well as key update.

Note that it should be possible to use either distinct algorithms for integrity and confidentiality or a combined approach (authenticated encryption). This in general is supported supporting cryptographic agility in the protocol to allow the application of different cryptographic algorithms. Note also that the endpoints typically have no guarantees about what level of transport layer security is enforced along the communication path with multiple hops.

A. Design rational

The design of the final solution specified in IEC 62351-4 already started in 2014. Not all of the security approaches depicted in Section IV were available at this time, but the concept of message-based security and session-based security was defined and applied. The available message-based and session-based approaches were seen to not match the refined requirements in an optimal way. Message based approaches were ruled out as they come with increased processing overhead for a consistent communication connection due to employment of asymmetric key material on a per message base. From the session-based approaches, the messenger-based solutions cannot be applied in industrial communication as they do not provide the necessary means for peer authentication. From the remaining approaches, ATLS would be the closest one from a functionality point of view as it provides an application protocol and transport protocol independent solution. The development of ATLS begun in 2017 and is still an individual draft in the IETF. Moreover, ATLS requires the existence of a TLS implementation on the communication peers.

Based on the review of the existing solutions and the requirements posed for power systems an own solution was seen necessary and the solution was designed based on approaches taken in the design of TLS. This development lead to an update of the standard IEC 62351-4 targeting also multi-hop communication in 2018. The standard meanwhile specifies a transport security profile and an application security profile. The application security targets the provisioning of end-to-end security, as outlined by the requirements above. The following subsections describe the technical preconditions, the session handling, and the packet construction of the protocol.

B. Precondition

The involved endpoints are expected to possess a X.509 certificate and corresponding private key as well as a root certificate trusted by both sides (e.g., bound to the operator) and a common set of Diffie Hellman public parameter. These can be part of the system configuration. Based on the peer certificates and the common root certificate the endpoint authentication can be performed. The Diffie Hellman parameter are then used in a key agreement phase to establish a master key for the application layer context.

As the security targets the application layer a protocol is assumed that supports session handling on application layer in terms of at least initiating a session. In the specific example, this is provided by the Manufacturing Message Specification (MMS [29]) using the *MMS Initiate* and *MMS Initiate Response* messages. MMS in turn is used to carry the IEC 61850 payload to monitor and control the DER resources. As the MMS session is initiated by only one roundtrip, followed by IEC 61850 specific exchanges, the security is expected to proceed in one round trip as well, without adding additional message exchanges.

C. Session Handling

The session handling can be distinguished into the initial key agreement during the session initialization, the key usage phase, and the key update phase. The sequences for the key agreement phase and the key update phase are shown in Figure 6. The key usage phase is neglected, as the

application of the negotiated key set is straight forward complying with the agreed cryptographic algorithms for integrity protection and optionally confidentiality protection.

At the beginning of the session, both sides generate a Diffie Hellman key pair to be used in the key agreement resulting in an ephemeral Diffie-Hellman secret. All data necessary for the establishment of the security association between both peers are kept in a data structure called clear token (as the data is transmitted in clear, but integrity protected).

```
ClearToken1::= SEQUENCE {
  sigAlg       AlgorithmIdentifier,
  version      Version DEFAULT {v1},
  assoID       AssoID,
  dHKey        DiffieHellmanSet,
  hmac         ALGORITHM.&id,
  time         TimeStamp,
  encr-mode    CHOICE {
    aea           SET SIZE (1..MAX) OF
      oid         ALGORITHM.&id,
    non-aea       SEQUENCE {
      encr           [0] SET SIZE (1..MAX) OF oid,
      icvAlgID       [1] SET SIZE (1..MAX) Of oid,
    ... },
  confParams   ConfidentialityParms,
  pkCert       PKCert,
  certPath     CertPath OPTIONAL,
  attCert      ACert OPTIONAL,
  ... }
```

Figure 6. Clear token (*ClearToken1*) for key establishment (simplified)

Figure 6 shows the clear token used during connection establishment. Besides the parameter for the session key establishment like the Diffie Hellman values and used certificates also session related information like algorithm identifiers for integrity protection as well as optional confidentiality protection and synchronization information is contained. In addition, the structure allows to also transport an attribute certificate, which may be used to additionally support attribute-based or role-based access control in conjunction with the authentication. To ensure the integrity of the initial exchange, the messages are cryptographically signed.

From each of the handshake messages a fingerprint is taken using a hash function. For this the following procedure is used. The hash h_A is calculated over the concatenation of the current message and the hash of the previous message (the initial message uses "0" as value of the previous message). This fingerprint is used to ensure the right order of messages and to provide additional randomness to the messages. This randomness bases on the generated Diffie Hellman parameter. Note that the calculated hash is never transmitted over the communication connection and only serves as local additional parameter in the final key derivation. Upon reception of the initiation message, the receiver verifies the signature, calculates the hash over the received message and stores the fingerprint h_A. It then generates the response message, from which again the fingerprint is taken by concatenating the response message with the stored fingerprint h_A to calculate the resulting hash h_B. This "running" hash spanning subsequent messages was inspired by the TLS handshake [10].

After providing the signed response to the initiator, both sides can calculate the Diffie-Hellman secret DH_S and utilize it together with the resulting hash h_B as input for the hash based key derivation function HKDF.

This will generate different keys per direction for integrity protection, and for confidentiality protection, resulting in four keys IK_A and IK_B, and EK_A and EK_B. The keys are applied according to the security association. It is necessary that both peers store the hash value h_B to be used in a later key update.

The key update uses a different clear token *(ClearToken2)*, a more simplified structure, as only a restricted set of parameter needs to be transmitted during the data transfer phase. The key update itself can be performed using a single message.

```
ClearToken2::= SEQUENCE {
  version          Version DEFAULT {v1},
  assoID           AssoID,
  time             TimeStamp,
  seq              SequenceNumber,
  iv          [0]  InitializationVector OPTIONAL,
  rekey       [1]  DhPublicKey OPTIONAL,
  reqRekey    [2]  BOOLEAN DEFAULT FALSE,
  changedKey  [3]  BOOLEAN DEFAULT FALSE,
  ... }
```

Figure 7. Clear token (*ClearToken2*) for key update (simplified)

Figure 8 shows the key update triggered by the control center. As in the initial step, the control center generates a fresh Diffie Hellman key pair and utilizes the already received and stored Diffie-Hellman key from the DER controller to immediately to calculate a new Diffie-Hellman secret DH_{S1} and the resulting set of updated session keys for integrity protection. Once this message is received by the DER controller, it can calculate the updated set of keys.

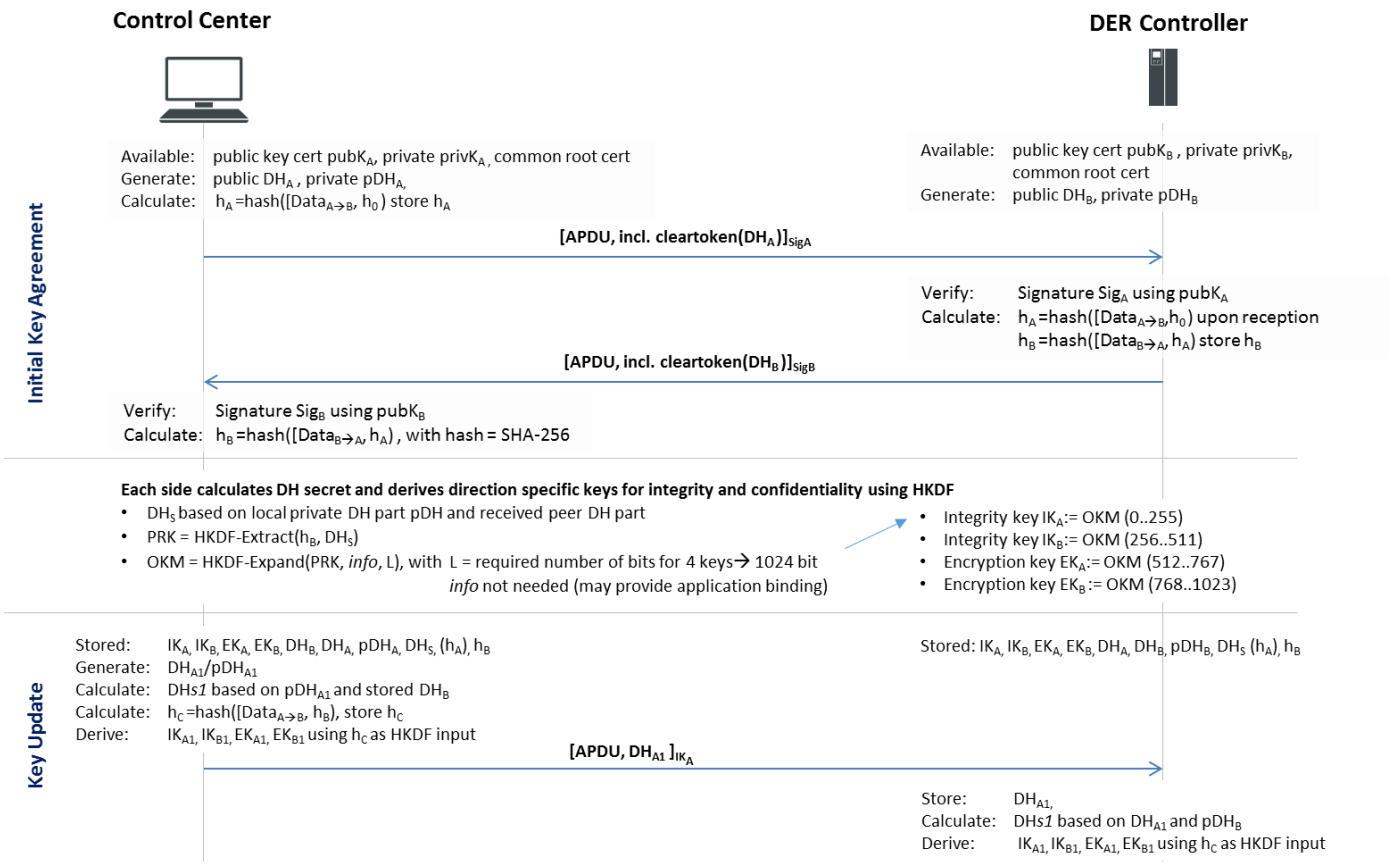

Figure 8. End-to-end-Security and hop-by-hop security according to IEC 62351-4

D. Packet construction

Figure 9 shows the packet construction and how the different parts of the messages are protected. Note that the clear token is only integrity protected while the payload of the packet (ADPU in Figure 9). As stated before, the clear token carries all cryptographic parameter necessary to establish the security association.

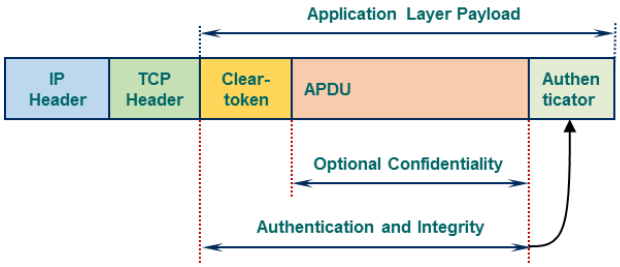

Figure 9. Packet structure of IEC 62351-4 end-to-end security

Although Figure 9 shows the transport over TCP/IP, other transports may be taken. The defined approach has no dependency on the underlying transport protocol. It has to be obeyed that for the session setup one roundtrip is necessary. In the target scenario for embedding DER into the power grid, the *MMS Initiate* and *MMS Initiate Response* message sequence is used to piggyback the secure session establishment. During the session setup, the initial handshake is performed. In the initial setup, the authenticator is provided by invoking the peer certificate and the corresponding private key to calculate a digital signature over the message as indicated in Figure 8 by the *SigA and SigB* indices on the initial handshake messages. For all subsequent messages the authenticator is build using the established session key for integrity protection. Note that the established keys are direction dependent resulting in two keys IK_A and IK_B for the ICV calculation. If confidentiality protection has been negotiated during the initial handshake two additional keys EK_A and EK_B are derived and can be used to encrypt the payload.

VI. EVALUATION

In the following, the different approaches for providing application layer security described in Section IV and Section V are compared regarding their match to the derived requirements [R' 1] to [R' 4].

In addition to the comparison of requirements match, further properties are being investigated. This comprises the effort for the initial handshake and the key update using the notion of Round Trips (RT). Additionally, as the target scenario addresses the integration of DER into the power grid and thus uses longer lasting connections, the potential performance impact based on a qualitative judgement is considered.

TABLE I. EVALUATION OF INVESTIGATED METHODS

Criteria	Message-based approaches				Session-based approaches					
	IETF RFC 3923 (Sig/Enc)	***XML security (Sig/Enc)***	***IETF JOSE (Sig/Enc)***	***IETF RFC 8152 (Sig/Enc)***	***IETF RFC 8613***	***IETF Draft ATLS***	***OTR***	***Signal***	***Google ALTS***	***IEC 62351-4***
[R' 1]: Peer authentication	X	X	X	X	(based on PSK)	X			X	X
[R' 2]. Integrity protection	X	X	X	X	X	X	X	X	X	X
[R' 3] Optional confidentiality protection	X	X	X	X		(X)	X	X	(X)	X
[R' 4] Mngmt. of session keys					X	X	X	X	X	X
Inital handshakes (using X.509 certificates)	Not applicable	Not applicable	Not applicable	Not applicable	1 RT	TLS 1.2: 2,5 RT TLS 1.3: 2 RT	2 RT	2 RT	2 RT	1 RT
Key Update handshakes	Not applicable	Not applicable	Not applicable	Not applicable	1 RT	TLS 1.2: 2 RT TLS 1.3: 0-1 RT	2 RT	2 RT	1 RT (via sesion resume)	0-0,5 RT
Performance impact	High	High	High	High	Low	Low	Low	Low	Low	Low
Notes	Utilizes RSA only for signatures.	Similar approach availabnle for binary transfer.		Binary transfer	Due to mandatory use of AEAD, no integrity only mode available.	Requires local TLS stack. TLS updates can be applied, but TLS 1.3 is restricted to AEAD.			Supports session resumption. Mandatroy encryption of payload.	No sessison resumption. Session key update with a single message.

For this, it is assumed that asymmetric operations are always applied in message-based approaches, while session-based approaches utilize asymmetric cryptography for a key establishment of a session key, which is used with symmetric crypto algorithms. Note that in the comparison for the key updates, it is stated for ATLS and also for IEC 62351-4, that the update may be performed without additional messages, basically in parallel to the existing data exchange, by stating "0-RT". This leverages the fast that in TLS 1.3 it is possible to send protected communication already in the *ClientHello* message, which can be used in the key update. In IEC 62351-4, the key Update would be signaled in the *ClearToken2* structure, as shown in Figure 7.

Based on the available solutions at the time of starting the specification of IEC 62351-4 in 2015, it was seen that none of existing solutions provides a perfect fit. The message-based approaches were directly ruled out as they have a big influence on the message processing due to the number of necessary asymmetric operations. From the session-based approach, not all of the discussed approaches were available at this time. The ongoing standardization approach of ATLS in the IETF looks promising for applications already utilizing TLS to protect the transport layer communication. Moreover, ATLS directly benefits from updates to the base TLS protocol. Contrary looking at TLS 1.3 integrity only operation will not be supported but may be necessary in power system automation to enable monitoring. IEC-62351-4 on the other hand was tailored to cope with the boundary conditions of the deployment environment resulting in no influence of the target application protocol in terms of additional handshakes. Due to this, the protocol has also less options to be configured or negotiated. This may be beneficial also for other applications as less complexity is often favored. This is visible also in a recently started activity in the IETF by proposing a compact version of TLS 1.3 [30].

VII. CONCLUSIONS

This paper investigates the handling of end-to-end security over intermediate nodes from a system point of view, by investigating existing security requirements and existing solutions. Moreover, the specific use case of incorporating DER into the power grid was taken as main use case for comparing the different approaches. The analysis was divided into message-based approaches and session-based approaches, in which the session-based approaches came out as winner due to the lower performance overhead in long lasting connections. Besides the

investigation into existing approaches, the motivation and description of the end-to-end security approach defined in IEC 62351-4 was described.

It establishes an end-to-end security session between two communicating peers with mutual entity authentication resulting in session keys being applied for end-to-end message integrity and confidentiality.

Two points should be obeyed when applying the discussed approach. First, the initial key agreement results in an ephemeral set of session keys, as both sides are expected to generate fresh Diffie Hellman parameters. The key update performed in a single message initiated by either peer results in a semi-static Diffie Hellman key agreement. Depending on the security requirements, the receiver may initiate another key update to ensure the freshness of his Diffie Hellman parameters. The second point relates to potential privacy requirements. The initial key agreement utilizes a clear-text token, which is only integrity protected. Thus, all information contained in the token is potentially readable by an intermediary. As the clear token also contains certificate information, it may allow to identify the communication end points. Applications with similar boundary conditions may leverage this approach in other scenarios or protocol frameworks in industrial communication.

As an outlook to the application of the described approach in IEC 62351-4, it is intended to investigate also the application of other publish-subscribe protocols utilized in automation scenarios like MQTT or AMQP.

In addition to the provided security measures, the application of specific privacy preserving techniques needs to be investigated to specifically address the data exchange with end-user related systems and services to keep their personal relation and data protected.

REFERENCES

[1] S.Fries and R.Falk, "End-to-End Application Security over Intermediaries on the Example of Power System Communication", Proceedings IARIA Securware 2019, ISBN: 978-1-61208-746-7, pp. 22-27, [Online]. Available from: https://www.thinkmind.org/download.php?articleid=securware_2019_2_10_30063 2020.01.10

[2] European Commission, "The Directive on security of network and information systems (NIS Directive 2016/1148)", [Online]. Available from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj 2020.01.10

[3] German IT Security Act, official web site (German), [Online]. Available from: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/KRITIS/IT-SiG/it_sig_node.html 2020.01.10

[4] ISO 27019: Information technology - Security techniques - Information security controls for the energy utility industry, [Online]. Available from: https://www.iso.org/standard/68091.html 2020.01.10

[5] IT Security Catalog, [Online]. Available from: https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Energie/Unternehmen_Institutionen/Versorgungssicherheit/IT_Sicherheit/IT_Sicherheitskatalog_2018.pdf 2020.01.10

[6] BDEW White paper "Requirements for Secure Control and Telecommunication Systems," BDEW, May 2018, [Online]. Available from: https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf 2020.01.10

[7] NIST Framework for Improving Critical Infrastructure Cybersecurity, [Online]. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf 2020.01.10.

[8] NERC CIP Set of Standards, [Online]. Available from: https://www.nerc.com/pa/Stand/pages/cipstandards.aspx 2020.01.10

[9] IEC 62443, "Industrial Automation and Control System Security" (formerly ISA99), [Online]. Available from: https://www.isa.org/isa99/ 2020.01.10

[10] T. Dierks and E. Rescorla, "Transport Layer Security Protocol version 1.2", RFC 5246, August 2008, [Online]. Available from: https://tools.ietf.org/html/rfc5246 2020.01.10

[11] E. Rescorla, "Transport Layer Security Protocol version 1.3", RFC 8446, August 2018, [Online]. Available from: https://tools.ietf.org/html/rfc8446 2020.01.10

[12] ISO/IEC 15118-2:" Road vehicles -Vehicle-to-Grid Communication Interface - Part 2: Network and application protocol requirements", March 2014, [Online]. Available from: https://www.iec.ch/search/?q=15118, 2020.01.10.

[13] S. Fries, R. Falk, H. Dawidczak, and T. Dufaure, "Decentralized Energy in the Smart Energy Grid and Smart Market – How to master reliable and secure control Secure Integration of DER into Smart Energy Grid and Smart Market," International Journal of Advances in intelligent Systems, vol. 9 no 1&2, 2016, ISSN: 1942-2679, page 65-75, [Online]. Available from: https://www.thinkmind.org/download.php?articleid=intsys_v9_n12_2016_6 2020.01.10

[14] ISO 61850-x: "Communication networks and systems for power utility automation", [Online]. Available from: https://www.iec.ch/search/?q=61850 2020.01.10

[15] P. Saint-Andre, "Extensible Messaging and Presence Protocol (XMPP): Core," RFC 6120, [Online]. Available from: https://tools.ietf.org/html/rfc6120 2020.01.10

[16] IEC 62351-x Power systems management and associated information exchange – Data and communication security, [Online]. Available from: https://www.iec.ch/search/?q=62351 2020.01.10

[17] P. Saint-Andre, "End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)," RFC 3923, [Online]. Available from: https://tools.ietf.org/html/rfc3923 2020.01.10

[18] W3C: XML Signature Syntax and Processing Version 2.0, June 2015, [Online]. Available from: https://www.w3.org/TR/xmldsig-core2/ 2020.01.10

[19] W3C: XML Encryption Syntax and Processing Version 1.1, April 2013, [Online]. Available from: https://www.w3.org/TR/xmlenc-core1/ 2020.01.10

[20] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Signature (JWS)," RFC 7515, [Online]. Available from: https://tools.ietf.org/html/rfc7515 2020.01.10

[21] M. Jones and J. Hildebrand, "JSON Web Encryption (JWE)," RFC 7516, [Online]. Available from: https://tools.ietf.org/html/rfc7516 2020.01.10

[22] J. Schaad, "CBOR Object Signing and Encryption (COSE)," RFC 8152, [Online]. Available from: https://tools.ietf.org/html/rfc8152 2020.01.10

[23] G. Selander, J. Mattsson, F. Palombini, and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, [Online]. Available from: https://tools.ietf.org/html/rfc8613 2020.01.10

[24] O. Friel, R. Barnes, M. Pritikin, H. Tschofenig, and M. Baugher, "Application layer TLS," IETF Draft, [Online].

Available from: https://tools.ietf.org/html/draft-friel-tls-atls-04 2020.01.10

[25] E. Rescorla, Key Material Exportes fro Transport Layer Security, " RFC 5705, [Online]. Available from: https://tools.ietf.org/html/rfc5705 2020.01.10

[26] Off-the-record Protocol Description version 3, [Online]. Available from: https://otr.cypherpunks.ca/Protocol-v3-4.1.1.html 2020.01.10

[27] Signal protocol, [Online]. Available from: https://signal.org/docs/ 2020.01.10

[28] Application Layer Transport Security, [Online]. Available from: https://cloud.google.com/security/encryption-in-transit/application-layer-transport-security/ 2020.01.10

[29] Manufacturing Message Specification, ISO 9506, [Online]. Available from: https://www.iso.org/standard/37080.html 2020.01.10

[30] E. Rescorla, R. Barns, and H. Tschofenig, "Compact TLS 1.3", IETF Draft, [Online]. Available from: https://datatracker.ietf.org/doc/draft-rescorla-tls-ctls/ 2020.01.10