SANDIA REPORT
SAND20XX-XXXX
Printed March 2020

Sandia National Laboratories

Recommendations for Data-in-Transit Requirements for Securing DER Communications

Ifeoma Onunkwo

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico
87185 and Livermore,
California 94550

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology & Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@osti.gov
Online ordering: http://www.osti.gov/scitech

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5301 Shawnee Rd
Alexandria, VA 22312

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.gov
Online order: https://classic.ntis.gov/help/order-methods/

ABSTRACT

With the adoption of Distributed Energy Resource (DER) interoperability standards, common communication protocols are now being deployed between power system operators and DER devices. In 2018, a revision to the US interconnection and interoperability standard, Institute of Electrical and Electronics Engineers (IEEE) Std. 1547, required DER equipment to have an IEEE 2030.5, IEEE 1815, or SunSpec Modbus communication exchange interface. This change supports the future transition to secure connection and exchange of information between the DER equipment and implementing parties, such as grid operators.

Adoption of standardized communication protocols and associated information models is a critical step toward interoperability between power system operators and DER, such as photovoltaic (PV) and energy storage systems. However, security requirements for these standardized communication protocols are not comprehensive, resulting in non-standard and vendor-specific implementation that may leave DER equipment susceptible to cyberattacks.

This paper examines the data-in-flight security requirements for standardized DER communication protocols, per IEEE 1547-2018 revision, as it relates to device authentication, key management, and encryption. The state of the art for these security features is also explored, addressing their impact on communication and performance of low-cost single board computers, which are typical of DER devices. In conclusion, a recommendation is provided to adopt a common set of communication requirements, which are intended to achieve interoperability and implement data security over DER network pathways, while ensuring reliable, secure, and real-time information delivery.

ACKNOWLEDGEMENTS

The author thanks the SunSpec/Sandia DER Cybersecurity Workgroup for valuable discussions on this topic and contributions to these recommendations. Special thanks go to, Jay Johnson [Sandia National Laboratories (SNL)], Tom Tansy [SunSpec], Gordon Lum [Kitu], Patricia Cordeiro [SNL], Frances Cleveland [Xanthus Consulting International], Jorg Brakensiek [Wivity], Alfred Tom [Wivity], Matthew Schlau [SNL], Randall King [Operant Networks], Keith Rose [Operant Networks], Prasanth Gopalakrishnan [Kalkitech], Kudrat Kaur [SunSpec], Andrew Levy [Obvius Holdings], Ryan Davidson [MPR Associates], Paul Duncan [MPR Associates], Roger K. Alexander [Eaton], Craig Pruess [Black & Veatch], Kari Kostiainen [ETH Zurich], Kirk W. Rosener [CPS Energy], Nate Diamond [Doosan GridTech], Nguyen Dzung, Anthony Johnson [SCE], Dylan Tansy [SunSpec], Nicholas Manka [GridSME], Adam Todorski [AutoGrid], Aegir Jonsson [Solectria], Christine Lai [U.S. Government], Alexander Miranda [Michigan Tech], Ralph Mackiewicz [SISCO], and Brian Gaines [SNL]for their substantial contributions shaping this paper.

This work was partially funded by the "DER Cyber Security Standards Development" project, which is funded by the Department of Energy's (DOE) Solar Energy Technologies Office (SETO).

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

ACRONYMS AND DEFINITIONS

Abbreviation	Definition
ACL	Access Control List
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
BITW	Bump in the Wire
CA	Certificate Authority
CBC-MAC	Cipher Block Chaining Message Authentication Code
CCM	Counter with CBC-MAC
CN	Common Name
CPUC	California Public Utilities Commission
CRL	Certificate Revocation List
CSIP	Common Smart Inverter Profile
DER	Distributed Energy Resource
DERMS	DER Management System
DES	Data Encryption Standard
DMS/OMS	Distributed and Outage Management Systems
DNP3	Distributed Network Protocol 3
DOE	Department of Energy
DR	Demand Response
ECDHE	Elliptic-curve Diffie-Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
EdDSA	Edwards-Curve Digital Signature Algorithm
EV	Electric Vehicle
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
GOOSE	Generic Object-Oriented Substation
ICCP	Inter-Control Center Communication Protocol
IDevID	Initial Device Identifier
IEC	International Electrotechnical Commission
IED	Intelligent Electronic Device
IEEE	International Institute of Electrical and Electronics Engineers
IEEE 802.1AR	IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity
IETF	Internet Engineering Task Force

Abbreviation	Definition
ISO/RTO	Independent System Operator/Regional Transmission Organization
ISP	Internet Service Provider
LDevID	Locally Significant Device Identifiers
LFDI	Long Form Device Identifier
MIB	Management Information Base
MMS	Manufacturing Message Specification
MRID	Master Record Identifier
NIST	National Institute of Standards
OCSP	Online Certificate Status Protocol
OpenADR	Open Automated Demand Response
OpenFMB	Open Field Message Bus
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PMU	Phasor Measurement Unit
PV	Photovoltaic
QoS	Quality of Service
RC4	Rivest Cipher 4
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SETO	Solar Energy Technologies Office
SFDI	Short Form Device Identifier
SHA	Secure Hash Algorithm
SMV	Sampled Measured Values
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
WAN	Wide Area Network
XMPP	Extensible Messaging and Presence Protocol

1 INTRODUCTION

Distributed Energy Resources (DERs) are a class of technologies featuring electrical generating and storage units attached to the power grid through the distribution system. An increase in the quantity of DERs on the US power system[1] has resulted in necessary new control schemes and interoperability requirements to maintain grid reliability, stability, and performance. Interoperability is possible when using standard protocols across supported communication channels. These DERs have been fielded with a variety of data communication platforms and grid-support capabilities. With the new IEEE 1547-2018 interconnection and interoperability standard[2], users can remotely change the behaviors of thousands of DER devices. The communication interface(s) may be added-on by the original equipment manufacturer (OEM) or by a third-party gateway device. Each platform relies on its own embedded design, plus the complexities of any interfaces to the DER for communication. These communications can take place over wired or radio/wireless networks, as shown in Figure 1.

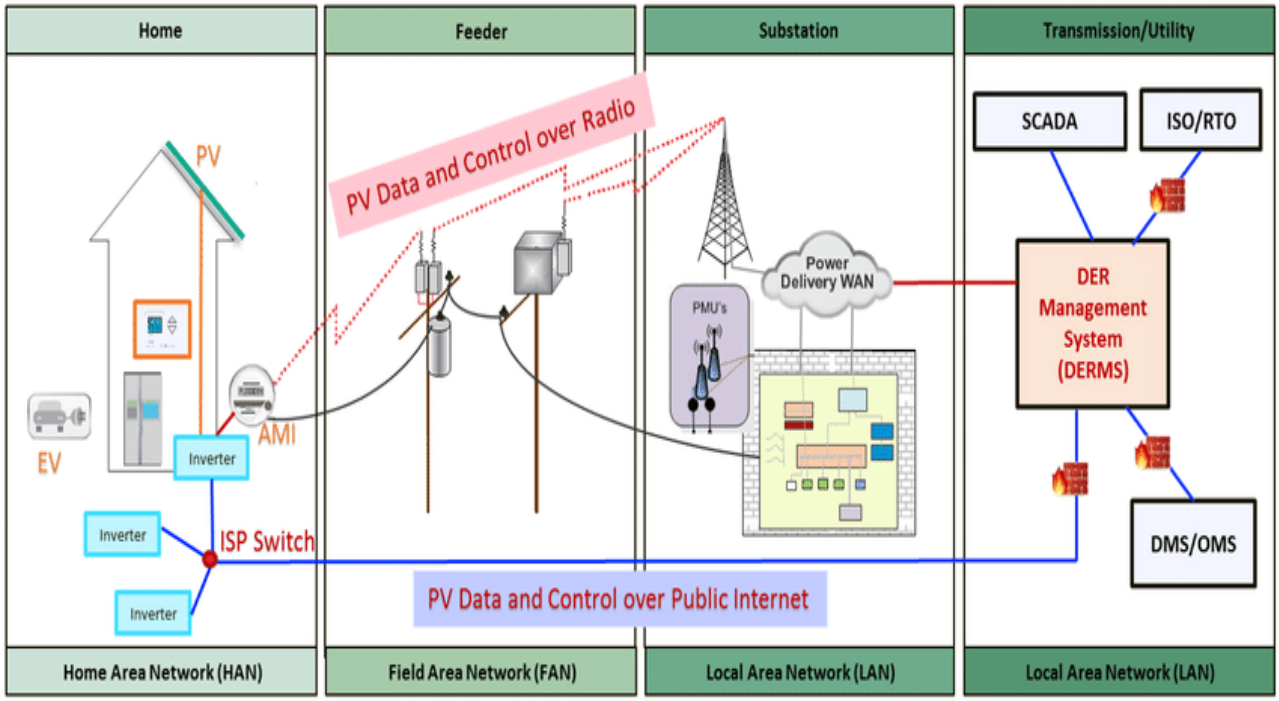

Figure 1: Different DER Control Network Architectures

Communication over a wired network typically routes through the insecure public internet[3], which threatens grid stability if the concentration of DER is significant and can be manipulated, thereby

[1] B. Kroposki and B. Mather, "Rise of Distributed Power: Integrating Solar Energy into the Grid [Guest Editorial]," in *IEEE Power and Energy Magazine*, vol. 13, no. 2, pp. 14-18, March-April 2015.
doi: 10.1109/MPE.2014.2381411
keywords: {Special issues and sections; Distributed power generation; Photovoltaic systems; Renewable energy sources},
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7048033&isnumber=7047989

[2] IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," in *IEEE Std 1547-2018 (Revision of IEEE Std 1547-2003)* , vol., no., pp.1-138, 6 April 2018
doi: 10.1109/IEEESTD.2018.8332112 URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8332112&isnumber=8332111

[3] "The attack on the internet service provider Dyn":https://www.networkworld.com/article/3134057/how-the-dyn-ddos-attack-unfolded.html

increasing its attack surface[4]. Wireless data communication makes it possible to connect devices without cabling them together. However, improper implementation techniques to deploying these wireless networks creates exposure to wireless threats[5] thus expanding its cyber threat attack surface as well. For information interoperability, IEEE 1547-2018 specifies the use of a "unified information exchange model for exchanging information between associated DER entities" (See Section 10 of the IEEE Std 1547™-2018), along the communication paths in Figure 2. The focus of this report is on the secure exchange of data between entities of the DER control architecture as specified in IEEE 1547. Therefore, ensuring the security of data in transit between DER Managing Entity at a utility and an Aggregator, across public/private network domains to the DER as shown in Figure 2, requires an analysis of the security strengths and weakness of the communication technologies.

Energy providers will soon adopt IEEE 2030.5, IEEE 1815 or SunSpec Modbus for DER communications. To guarantee the security of information that flows over public or private networks, DER communications and their corresponding security elements must be standardized, to prevent malicious control or misuse of DERs. For instance, some currently used protocols cannot support authentication. Without authentication and authorization, anyone with access to the communication network and knowledge of the targeted DER's address will be able to control the DER equipment[6]. Implementing cryptographic methods and techniques to enable authentication and confidentiality for those protocols not inherently built with security features may necessitate a bump-in-the-wire (BITW) feature – (recognizing that this does not provide application layer security and may result in unacceptable increase in latency), instead of natively securing the communication protocol. However, there are protocols that can provide authentication, integrity, and confidentiality capabilities, thus highlighting the disparity in the security features of DER communication protocols. The implication, therefore, is that for data in transit, security requirements are needed for DER equipment to 1) assure the authenticity of data going over the network, 2) verify the identity of devices, 3) confirm that the encryption keys used to protect data are securely managed, and 4) provide access control. Providing these requirements for DER communication protocols will enhance the secure connection and exchange of information between utilities, third-party aggregation of DER by aggregators, manufactures of DER devices, and other DER stakeholders.

The following sections of this report will explore a few topics.

1. The security principles which form the basis of a system's security framework.
2. The DER communication protocols specified in IEEE 1547 and their associated information models.
3. The security requirements of the DER communication protocols for identifying poorly defined security features for device authentication, encryption, and, the key management required for generation, exchange, and use of keys. Additionally, a few other protocols called out in IEEE 1547 and International Electrotechnical Commission (IEC) 61850/62351 will be explored.
4. The current state-of-the-art security features for securing data in transit information exchanges across IEEE 1547-identified DER communication paths in Figure 2: Utility-to-

[4] "Cyber attacks on Solar and Wind assets": https://www.utilitydive.com/news/first-cyber-attack-on-solar-wind-assets-revealed-widespread-grid-weaknesse/566505/

[5] Parks, Raymond C.. "Advanced Metering Infrastructure Security Considerations." (2007).

[6] Carter, Cedric & Onunkwo, Ifeoma & Cordeiro, Patricia & Johnson, Jay. (2017). Cyber Security Assessment of Distributed Energy Resources.

DER communication, Utility-to-Aggregator communication, and Aggregator-to-DER communication. Also included is the local gateway to DER protocol stack present at an industrial, commercial, or residential premise location.

5. Recommendations for adding new security features, while accounting for adverse quality of service (QoS) impacts to real-time operations. Throughput and latency are weighed, based on existing and future DER communication hardware.

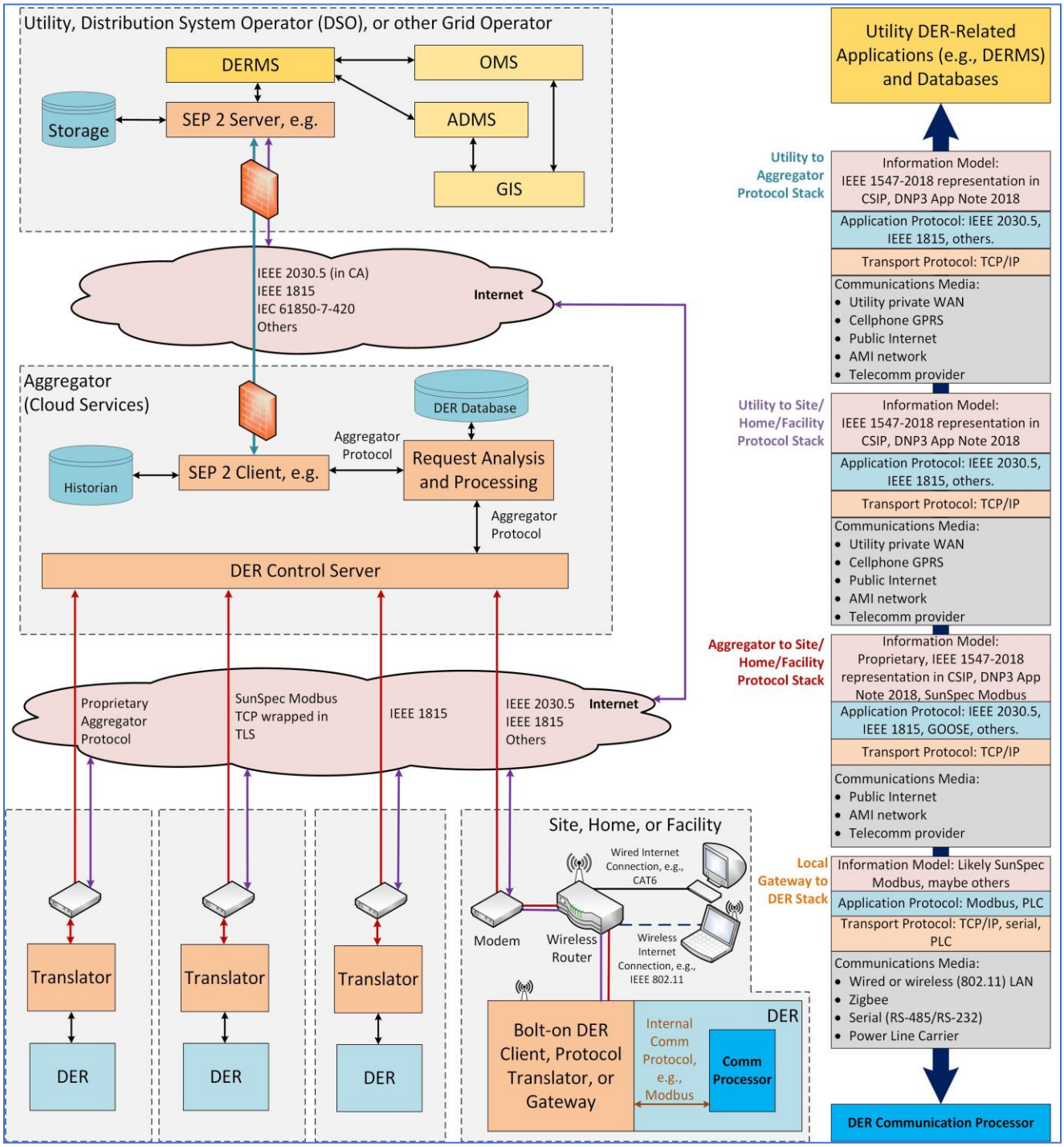

Figure 2: DER communication paths between the utility, aggregator, and DER equipment

2 GUIDING INFORMATION SECURITY REQUIREMENTS

2.1 Overview of Security Requirements for Cyber-Physical Systems

Cryptography is a powerful tool that can be leveraged to secure end-to-end communication in an energy distribution network system, providing the services necessary for securing DER system information and operations. Cryptography is also essential to supporting automated key management that is necessary for the establishment and updating of the keying material used with cryptographic algorithms to provide security services.
For typical information technology systems, *confidentiality*, *integrity*, and *availability* are core security requirements. Cyber-physical systems (CPS) are physical and engineered system whose operations are monitored, coordinated, controlled and integrated by a computing and network communication core[7]. As cyber-physical systems become more connected, they expand the cyber security attack surface and pose a significant risk to the resilience of the electric grid if controlled in aggregate. For CPS the security requirements must reflect that there can be physical impacts due to deliberate or even inadvertent cyber "attacks." Therefore, the important security requirements are *authentication, authorization, integrity, non-repudiation, confidentiality* and *availability*. These requirements outline the framework for building trust in identity and data authentication for DER communication standards. The definition and benefits of each of these security requirements are described below, where the first five rely mostly (but not exclusively) on cryptographic techniques, while the last, availability, relies more on engineering techniques:

- *Device authentication* provides assurance that the protected data came from an authenticated entity. This verification, using a digital certificate or other security token, can be provided with the use of digital signatures and cryptographic keys, which are formally bound to an entity, to identify an entity as either the sender or receiver of information. These services also provide non-repudiation, a means to prevent denial of authorship.

- *Authorization* establishes the access requirements, namely which users, systems or applications may read, write, create, delete, etc. specific types of information. Role-based access control (RBAC) is the primary technique for ensuring that access to stored data or data in transit is authorized.

- *Integrity* provides mechanisms to detect unauthorized (intentional or unintentional) data modifications, dropped or repeated messages. Message integrity extended to cover time or sequence message elements, can allow for protections against message delays or replays in session-less communications scenarios. Cryptographic authentication algorithms typically calculate a message authentication code or digital signature to verify the authenticity and integrity of the message.

- *Non-repudiation* provides the assurance of the origins of data in authenticated transactions. This surety can be provided with the use of a digital signature and other data about the sender or receiver that will be difficult to repudiate when aggregated.

[7] Ragunathan (Raj) Rajkumar, Insup Lee, Lui Sha, and John Stankovic. "Cyber-physical systems: the next computing revolution". In Proceedings of the 47th Design Automation Conference (DAC '10). ACM, New York, NY, USA, 731-736. 2010

- *Confidentiality* protects information from unauthorized or unintended disclosure. To protect data (e.g. power controls functions, communication functions, personally identifiable information [PII]) from disclosure during transmission, cryptographic mechanisms are used. Encryption algorithms are used to transform plaintext data, using an encryption key, into indecipherable data called ciphertext. Decryption algorithms are used to transform ciphertext data, using an encryption key, back to plaintext. In addition, perfect forward secrecy in the form of new session key per communications session, can be used to ensure that a breech affecting data protected with one session key does not expose any other data protected with different session keys, thereby preventing the leaking of all data when a single session key is compromised.
- *Availability* ensures that access to data is provided when needed. To avoid denying access to requested information, the system should be constructed with a framework that maintains a proper functioning operating system environment. It is also important that this structure understands expected network traffic operations, to be able to proactively respond to anomalous network traffic or information exchange patterns. An important aspect of availability is monitoring the health of systems and networks.

2.2 Rationales for Security Requirements for Cyber-Physical Systems

2.2.1 Rationale for Cryptographic Key Management

Cryptographic key management is required for establishing and updating most security techniques, including encryption of data for confidentiality, digital signing and hashing for authentication, storing of sensitive data such as Master Record Identifiers (MRIDs) and the keys themselves, and chaining of certificates from one owner to another, etc.

The generation, exchange, storage, use, replacement, and destruction of cryptographic keys provides the basis for trust in securing information. It is also critical to the security of a cryptosystem, since access to keys may equate to access to information.

2.2.2 Rationale for Mutual Authentication Between Systems, Devices, and Users

Mutual authentication of systems, devices, and users ensures that entities in a communication link trust each other before a secure connection is instantiated.

2.2.3 Rationale for Authorization

Physical security is a first layer of authorization – access cards tied to unique biometrics, room and/or station access, full logging/authentication, etc. Logical security happens once the physical has been verified and authorization to proceed has been granted. Authorization ensures that only authorized users, devices, and systems, based on their roles, may access (monitor, control, update, etc.) specific information. This prevents unauthorized entities from modifying or even accessing information that they should not be able to access.

2.2.4 Rationale for Integrity

Integrity of data is critical for cyber-physical systems since they rely on accurate information to perform their activities. Encryption does not necessarily provide integrity, since "garbage in, garbage out". Thus, altered data can lead to negative system or operational impacts even when the data is modified without access to or understanding of the unencrypted information. Therefore, additional security techniques, such as digital signatures or hashing techniques need to be used to ensure that data in transit has not been modified.

2.2.5 Rationale for Non-repudiation

Non-repudiation provides proof on the origins of the data so that a sender cannot deny that it is the originator of the message nor a recipient deny that it is the recipient of the message.

2.2.6 Rationale for Availability

Cyber-physical systems require high availability as they operate in very dynamic and rapidly changing situations. Monitoring the availability of networks, systems, and applications through Simple Network Management Protocol (SNMP) or other networking techniques is critical to reliable operation of these cyber-physical systems. Also, SNMPv3 provides secure access to the network monitoring information via a user-based security module with built in authentication and encryption features.

2.2.7 Rationale for Confidentiality

Confidentiality, through encrypting the data, ensures that the data is unreadable by untrusted parties unless a key to decode the data is provided. This confidentiality is mostly required for sensitive or personal information, and typically is not as critical for power data. Nevertheless, a possible attacker may gain valuable information on the setup of the network and its communication patterns, which may help the attacker pivot to other systems of interest and enable attacks such as sending system operators good signals while the equipment is being destroyed[8].

It is important to note that defense in depth of cyber-physical systems lies not just with cryptography, though essential as elucidated above. Techniques such as filtering network traffic by port and IP addresses, patch management, operating system hardening, log monitoring, certification procedures for data and communications security for DER[9], secure network architecture[10], etc. are other necessary cyber security requirements for achieving a multilayered defense strategy.

[8] https://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/
[9] Saleem, Danish & Carter, Cedric. (2019). Certification Procedures for Data and Communications Security of Distributed Energy Resources. 10.13140/RG.2.2.15474.04803.
[10] https://sunspec.org/wp-content/uploads/2020/01/EPRI-Security-Architecture-for-the-Distributed-Energy-Resources-Integration-Network.pdf

3 IEEE 1547-2018 DER COMMUNICATION PROTOCOLS

The table below describes the information models defining the security requirements for IEEE 1815, SunSpec Modbus, IEEE 2030.5, and IEC 61850 communication protocols. Although IEC 61850 is predominantly used outside of North America, its review is included because IEEE 1815 (DNP3) uses IEC 61850 information model data objects for interoperability in IEEE 1547. The associations of the information model and security requirement are described below in Table 1, followed by a brief overview of each of the protocols.

Table 1: DER interoperability and associated security standards

Communication Protocol	Data or Information Model	Associated Security Standards
IEEE 1815	DNP3 Application Note AN2013-001 based on IEC 61850	In IEEE 1815 (DNP3) Secure Authentication SAv2 and Sav6 (being updated)[11]
SunSpec Modbus	SunSpec Modbus Models	None, since Modbus cannot directly support security. The use of Virtual Private Networks (VPNs) is a current security technique. SunSpec Modbus over TCP/IP[12] recommends the use of TLS if encryption is desired.
IEEE 2030.5	IEEE 2030.5 information model with specific semantic requirements from the Common Smart Inverter Profile (CSIP)	In IEEE 2030.5, identified in CSIP
IEC 61850	IEC 61850-7-420 operational functions for IEEE 1547 functions, including basic IEC 61850-7-4 data objects	In IEC 62351 series (standard consists of 11 parts; which parts depend on which protocol is used) IEC 62351-3, -4 for authentication, data integrity, and confidentiality of client-server protocols IEC 62351-7 for availability of systems and networks IEC 62351-8 for authorization via Role-Based Access Control (RBAC) IEC 62351-9 for key management IEC 62351-100-xx for conformance testing of these security standards (still in progress)

[11] https://www.dnp.org/LinkClick.aspx?fileticket=hyvYMYugaQI%3d&tabid=66&portalid=0&mid=447&forcedownload=true accessed February 19, 2020

[12] https://sunspec.org/wp-content/uploads/2015/06/SunSpec-Best-Practice-Guide-Security-Recommendations-A42025-1.1.pdf

3.1 IEEE 1815

IEEE 1815 is a well-known supervisory control and data acquisition (SCADA) communication protocol. Devices that typically support this communication include computers, remote terminal units (RTU), non-remote terminal units' equipment, and master stations. IEEE 1815 features a monitoring master (central master) and outstation (remote device) relationship that is very fast and highly scalable. It can chain multiple master/outstations in series for aggregation or ownership. It has integrity features to detect transport errors and provide accurate timestamps. IEEE 1815 began with no data security features, but its security has since been supported by some vendors using bump-in-the-wire encryption hardware or SSH (Secure Shell). IEEE 1815 over the public internet is optionally secured by transport layer security (TLS) following the requirements taken from IEC 62351-3. Also, implementation choice such as VPN make this possible. DNP3 Secure Authentication (DNP3-SA) version 5[13] is an encryption option inherently using X.509v3 certificates and a public key infrastructure (PKI) to facilitate device and data authentication trust. Data confidentiality (encryption) will be added to a future release of DNP3.

3.2 SunSpec Modbus

Modbus transmission protocol is an automation communication protocol commonly used for connecting intelligent electronic devices (IEDs). Modbus, though widely used amongst industrial system users, was not built with security. Modbus operates a client/server architecture, where the client (also known as the master) initiates the request and the server (also known as the slave) supplies the requested information. This is also known as the send request and read response message. There are no security or encryption features in this communication standard, thus making some vendors rely on bump-in-the-wire technologies such as VPNs for add-on security. The development and updates to the Modbus protocols have been managed by the Modbus organization. Several versions of the Modbus protocol exist for the serial and ethernet ports. Some of the photovoltaic community has adopted the SunSpec Alliance Modbus[14] profile for interoperability.

3.3 IEEE 2030.5

IEEE 2030.5 is an application protocol for IoT device communications within the smart energy space. This space covers a wide variety of devices, from low-cost devices, such as energy sensors and smart light bulbs, to high-cost performance devices, such as solar inverters, electric vehicles, and energy management systems. The California Public Utilities Commission (CPUC) has been phasing new interoperability requirements into the California interconnection standard, Electric Rule 21[15], Generating Facility Interconnections. As part of this process, the California investor owned utilities (IOUs) established IEEE 2030.5 as the communications standard for smart inverters. The Common Smart Inverter Profile (CSIP)[16], which defines a specific set of requirements within the various mandatory and optional provisions of the IEEE 1547 standard, was developed to foster interoperability between IOUs and inverters or the aggregation services managing those inverters. In

[13] https://www.cs.ox.ac.uk/files/9139/esorics-tech-report.pdf
[14] https://sunspec.org/sunspec-modbus/
[15] https://www.cpuc.ca.gov/Rule21/
[16] https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-02-2018-1.pdf, accessed Feb 2, 2020

this environment, the client device is an aggregator or a DER device like a solar inverter. IEEE 2030.5/CSIP requires TLS for communication security.

3.4 IEC 61850

The IEC 61850 standard contains an information model (IEC 61850-7-420) and two protocols (IEC 61850-8-1 and 8-2) that are specifically relevant to DER communications. The information model covers IEDs, including those in substation automation, distribution automation, Distributed Energy Resources (DER), and now microgrids. Specifically, IEC 61850-7-420 defines all the interoperability requirements for the functions defined in IEEE 1547, and is used as the information model for the Application Note of DNP3. It also covers additional functions and models of resources, such as PV systems, fuel cells, microgrids (under development), and wind plants (IEC 61400-25).

The IEC 61850 protocols include three communication protocols based on Manufacturing Message Specification (MMS): Client-Server, Generic Object-Oriented Substation (GOOSE), and Sampled Measured Values (SMV). IEC 61850-8-2 specifies the MMS payloads to run over Extensible Messaging and Presence Protocol (XMPP). This standard does not include security, but relies on the security standards of IEC 62351-3, -4, and -6 (for GOOSE). IEC 62351 security standards are also responsible for providing security for IEC 60870-5, 60870-6, 61970, and 61968.

3.5 Other Communication Protocols

Communications and protocols are diverse, globally. A review is provided in "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators"[17]. Additionally, these protocols may be found in the DER communication paths under agreement between the utility, aggregator, and DER equipment. Further work needs to be done to identify the links (in Figure 2) where these protocols are used for communication as well as their security requirements in the DER ecosystem. Three protocols that could be used with DER include OpenADR for Demand Response, OpenFMB as a message bus, and OPC/UA for industrial automation.

3.5.1 Open Automated Demand Response (OpenADR)

OpenADR is a standards effort developed by companies and industry stakeholders for demand response (DR) communication from power system operators or independent system operator to electric customers[18]. It is an open and interoperable information exchange data model, and an emerging smart grid standard to communicate price and availability signals in response to load demand. The intention of the data model is to interact with building and industrial control systems that are pre-programmed to act based on a DR signal, enabling a demand response event to be automated. The current OpenADR version 2.0 can be secured using TLS [19]and PKI[20].

[17] C. Lai, N. Jacobs, S. Hossain-McKenzie, C. Carter, P. Cordeiro, I. Onunkwo, J. Johnson, "Cyber Security Primer for DER Vendors, Aggregators, and Grid Operators," Sandia Technical Report, SAND2017-13113, Dec 2017.
[18] https://drrc.lbl.gov/publications/open-automated-demand-response-2
[19] https://www.openadr.org/assets/openadr_drprogramguide_v1.0.pdf, accessed Feb 3, 2020
[20] https://www.openadr.org/cyber-security

3.5.2 Open Field Message Bus (OpenFMB)

OpenFMB[21] is a reference architecture and standard that has been ratified to provide an interoperability framework to enable distributed federation of data between the grid-edge devices. Information no longer needs to go to the central system to enable decision making. This architecture enables interoperability of devices that use different communication infrastructure and protocol standards - that may even be proprietary, to exchange federated local data and information.

3.5.3 Open Platform Communication Unified Architecture (OPC UA)

OPC UA[22] is an open standard that specifies information exchange for industrial communication. This machine to machine or computer to machine communication, features a client/server or publisher/subscriber technology for facilitating the exchange of real-world data between multiple vendor devices and control applications. In addition to fostering industrial interoperability, this platform-independent and service-oriented standard offers mechanisms for authentication, integrity, and encryption.

4 IEEE 1547-2018 DER COMMUNICATION PROTOCOLS SECURITY FEATURES REVIEW

4.1 Common Security Areas

As part of the interoperability and information exchange between DER entities, the IEEE 1547 standard identifies three communications protocols, IEEE Std 2030.5 (SEP2), IEEE Std 1815 (DNP3), and SunSpec Modbus. Of these, only two, IEEE Std 2030.5 and IEEE Std 1815 (DNP3) support security provisions.

4.1.1 Transport Level Security

The protocols identified in IEEE 1547 which use TCP/IP may use TLS to provide confidentiality and data integrity at the transport level. TLS is a cryptographic protocol used to provide system-to-system communication security over a computer network. TLS uses PKI certificates for authentication, as well as a key exchange algorithm to establish a secure traffic encryption key and cipher suite, for encrypting communication session.

IEEE 1815, IEEE 2030.5, and IEC 62351-3 permit TLS v1.2 or higher for encryption, and X.509 digital certificates for device authentication. However, the TLS protocols in use support cipher suites with varying degrees of security strength, ranging from weak to strong. The security strength of a TLS session is dependent on the cipher suites negotiated between the two end points, therefore, selecting an appropriate cipher suite ensures the strength of the security. It is for this reason that IEEE 2030.5 specifies the use of a single cipher suite (TLS_ECDHE_ECDSA_WITH _AES_128_CCM_8), selected for the strengths of its encryption and signing algorithms while conserving resources by minimizing hash lengths, for the targeted constrained device application.

[21] https://openfmb.ucaiug.org/
[22] https://opcfoundation.org/about/opc-technologies/opc-ua/

IEC 62351-3 lists deprecated cipher suites but does not explicitly list supported ciphers. For IEC 62351-3, support for TLS versions 1.0 and 1.1 is allowed for backwards compatibility but these older versions have security concerns that has necessitated its retirement. It also supports the use of RSA (with optional and mandatory key lengths), Diffie-Hellman, and ephemeral Diffie-Hellman for key exchange. In addition, it supports public key mechanisms based on elliptic curves. IEC 62351-4 defines cipher suites that must be supported. However, the mandatory cipher suite does not support perfect forward secrecy and makes use of SHA-1, a hash function with known weakness[23]. Amongst its optional cipher suites include RC4 which has been deprecated [24].

4.1.2 PKI, X509 Certificates, and Whitelist/Blacklist

The PKI models used between the different DER communication protocols differ significantly. For example, the PKI system for IEEE 1815 and the IEC 62351 parts associated with protecting IEC 61850 protocol for provisioning a PKI system, allow for certificate revocation management by using an offline certificate revocation lists (CRLs) or an online certificate status protocol (OCSP), which checks the validity or authenticity of a device while IEEE 2030.5 does not allow such provision. These PKI systems have most recently been explored in recent works, such as the "Recommendations for Trust and Encryption in DER Interoperability Standards"[25].

The support of X.509v3 digital certificate is universal for these protocols, but there are scenarios where support of self-signed certificate is permitted, which may be used beyond its recommended specific use cases by an implementor, making it less secure. In addition, the capability to use whitelists and blacklists in X.509 attributes is permitted in the IEC 62351 standards, specifically IEC 62351-3. IEEE 2030.5 refers to the use of blacklisting and whitelisting for the purpose of authentication. But as pointed out in Recommendations for Trust and Encryption in DER interoperability Standards, "the use of disconnected black/white lists operated by independent operators can lead to arbitrary processes resulting in fragmentation and uneven enforcement of the ecosystem."

4.2 IEEE 2030.5 Observations and Recommendations

Table 2: Trust and Cryptography Features in IEEE 2030.5/CSIP Communication Protocol

Protocol	Encryption (Data Confidentiality and Integrity)	Device Authentication	Key Exchange Algorithms
IEEE 2030.5, CSIP	IEEE 2030.5 requires TLS v1.2 AES_128_CCM_8. This is an Advanced Encryption Standard (AES) in the Counter with Cipher Block Chaining – Message Authentication Code Mode (CBC-MAC).	Uses X.509v3 Digital Certificates. Mutual client/server authentication is required.	IEEE 2030.5 requires Ephemeral Elliptic Curve Diffie-Hellman key exchange with Elliptic Curve Digital Signature Algorithm signatures (ECDHE_ECDSA).

[23] https://www.globalsign.com/en/blog/sha-1-collision-highlights-further-weakness
[24] https://tools.ietf.org/html/rfc7465
[25] J. Obert, P. Cordeiro, J. Johnson, G. Lum, T. Tansy, M. Pala, R. Ih, "Recommendations for Trust and Encryption in DER Interoperability Standards," Sandia Technical Report, SAND2019-1490, Feb 2019.

	This is an authenticated encryption algorithm, so the bulk traffic is being encrypted and every message authenticated.	In the CSIP California Implementation guide, the security framework for communication with a utility is dictated by the utility. Authentication may currently use a certificate authority of the CSIP, a third party or self-signed device certificates if there is no existing Certificate Authority. The Data-in-Flight working group notes that self-signed certificates allow for impersonation of a device or the utility to some extent.	

Table 2 summarizes the security requirements in IEEE 2030.5 while also outlining poorly defined features. The following recommendations are provided to improve the security of IEEE 2030.5.

Encryption: The Data-in-Flight working group recommends increasing the length of the authentication tag from 8 octets (64 bits) to something greater. This is because a short authentication tag could be more easily compromised by increasing the chance of tag guessing. RFC 2104 (written in 1997 when computing resources were not as powerful as what is obtained today) recommends "the output length be not less than 80 bits." 16 octets are typical for AES block ciphers. Also, AES 128 is still believed to be secure, per NIST[26]. AES 256 takes more resources and is not recommended.

Device authentication: In the California implementation guide, authentication may be done using self-signed device certificates when there is no existing Certificate Authority (CA). The Data-in-Flight working group notes that this allows for impersonation of a device or the utility to some extent. The working group also recommends that a security policy to disallow self-signed certificates be implemented.

Authorization: IEEE 2030.5 servers maintains an authorized lists of the client's truncated version of the x509v3 certificate fingerprint to allow client communication with the server. Access control lists which typically lists permissions are not required, and access policies which uses roles and privileges for permissions are instead used by the server grant access to authorized clients. Access policies are recommended by NIST[27]. Efforts by the DER Access Control work group to implement DER

[26] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar2.pdf
[27] https://nvd.nist.gov/download/800-53/800-53-controls.xml

polices to grant access to resources is recommended for consideration - while also leveraging the IEEE 2030.5 access policies.

Cipher suites: IEEE 2030.5 mandates the use of a single cipher suite; TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 that provides a security level of 128 bits defined in NIST SP 800-57[28], to prevent weak cipher downgrade attacks and to promote interoperability. This cipher supports mutual authentication of the server and client with no requirements to support session resumption or session tickets. Currently, there are no known weaknesses to AES-128 or Elliptic Curve Cryptography (ECC) with the P-256 curve and this cipher suite complies with all the security features used in TLS 1.3. Additional features and recommendations of the cipher suite as well as the implementation with embedded system components are provided in "Recommendations for Trust and Encryption in DER Interoperability Standards."

DER stakeholders[29] indicates that the IEEE 2030.5 cipher suite does meet the TLS 1.3 requirements (including its requirement for perfect forward secrecy) and is not listed in the TLS 1.2 cipher suite blacklist that was created around the same time in the Internet Engineering Task Force (IETF)[30]. Further thoughts should be given into understanding if the TLSv1.3 cipher suites are not compatible with TLSv1.2 because their specification is structured differently and does not map properly to the newer specification. Else, the TLSv1.2 cipher suite ECDHE_ECDSA_with_AES_128_CCM_8 is not disallowed for use in TLSv1.3 and its usage is either acceptable per RFC or per common usage exploitation. Also, a broader discussion needs to occur between stakeholders to determine if 1) this cipher suite should be retained for IEEE 2030.5 communication, and 2) to understand the use of TLS 1.3 for 2030.5 communication, including backward compatibility with "older" TLS 1.2 client/servers.

4.3 Modbus with TCP Security Observations and Recommendations

Table 3: Trust and Cryptography Features in Modbus with TCP Security Communication Protocol

Protocol	Encryption (Data Confidentiality and Integrity)	Device Authentication	Key Exchange Algorithms
Modbus/ TCP Security	Modbus TCP Security V21 requires Transport Layer Security 1.2 (TLS v1.2) or better. The specification recommends AES counter mode cipher suite (e.g. Galois/Counter Mode) for authenticated encryption. The support for NULL cipher suites is specified with emphasis on its placement as least priority.	Uses X.509v3 Digital Certificates. Mutual client/server authentication is required.	Modbus TCP Security V21 specifies that key exchange must support Rivest-Shamir-Adleman (RSA) public key cryptosystem. The Data-in-Flight working group notes that TLS_RSA does not

[28] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf, accessed Feb 6, 2020
[29] DER stakeholders: the nation's utilities, state public utility commissions (PUCs), distributed-generation control hardware and software vendors, and communication providers
[30] https://tools.ietf.org/html/rfc7540#appendix-A

			support forward secrecy and is broken by the Bleichenbacher attack.

Table 3 summarizes the security requirements in Modbus with TCP Security, in addition to outlining poorly defined features. The following recommendations are provided to improve the security of Modbus with TCP Security:

Encryption: The Modbus/TCP security allows for unencrypted communication paths using cipher suites with NULL for bulk encryption. The Data-in-Flight working group notes that this allows for a down-grade attack scenario. A stronger cipher suite recommended in this specification is the TLS_ECDHE_ECDSA_WITH_ AES_128_GCM_SHA256, meaning that the specified encryption is AES128 in GCM.

Device authentication: Authentication may be done using self-signed device certificates. The Data-in-Flight working group notes that this allows for impersonation of a device or the utility to some extent and recommends that a security policy to disallow self-signed certificates be implemented.

Authorization: For authorization, the protocol specifies the use of roles defined in the x509v3 certificate. However, strictly associating certificates with roles can cause the certificate to become invalid - in the event of role changes - thus necessitating the issuance of new certificates which may be non-trivial and costly to implement. On-going efforts by the DER Access Control work group to implement polices to grant access to resources as needed is recommended for consideration.

Cipher suites: The specification requires a minimum RSA key exchange with a cipher suite of either TLS_RSA_WITH_AES_128_CBC_SHA256 or TLS_RSA_WITH_NULL_SHA256. The specification also supports but does not mandate Elliptic Curve key exchange in the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256. This gives an ephemeral key generation of Elliptic-Curve Diffie-Hellman with Elliptic Curve signature. The Data-in-Flight working group recommends that Elliptic Curve be specified as the minimum instead.

4.4 SunSpec Modbus Observations and Recommendations

Table 4: Trust and Cryptography Features in Modbus Communication Protocol

Protocol	Encryption (Data Confidentiality and Integrity)	Device Authentication	Key Exchange Algorithms
SunSpec Modbus	None.	None.	None.

Table 4 summarizes that there are no security requirements in SunSpec Modbus. The following recommendations are provided to improve the security of Modbus or SunSpec Modbus:

Encryption: The Data-in-Flight working group recommends that SunSpec Modbus follows the example of and improve on Modbus TCP Security V21 or IEEE 2030.5/CSIP.

Device Authentication: The Data-in-Flight working group recommends that SunSpec Modbus follows the example of and improve on Modbus TCP Security V21 or IEEE 2030.5/CSIP.

Authorization: The Data-in-Flight working group recommends that SunSpec Modbus follows the example of and improve on Modbus TCP Security V21 or IEEE 2030.5/CSIP.

Cipher suite: The Data-in-Flight working group recommends that SunSpec Modbus follows the example of and improve on Modbus TCP Security V21 or IEEE 2030.5/CSIP.

4.5 IEEE 1815/DNP3 SA Observations and Recommendations

Table 5: Trust and Cryptography Features in DNP3 Communication Protocol

Protocol	Encryption (Data Confidentiality and Integrity)	Device Authentication	Key Exchange Algorithms
IEEE 1815, DNP3-SA	The specification recommends IPsec VPNs for securing access while TLS v1.2 is optional. Using TLS, the mandatory cipher suite (which complies with IEC 62351-4) is AES_128 with other optional recommendations including RC4_128, 3DES_EDE_CBC and AES_256. The Data-in-Flight working group notes that RC4[31] is considered insecure and 3DES[32] is considered weak.	Uses X.509v3 Digital Certificates. Mutual client/server authentication is required.	IEEE 1815-2010 SA v2 was limited to shared keys on limited ciphers (AES128, SHA1 and SHA256). IEEE 1815-2012 SA v2 includes PKI with certificates and optional broader cipher support (AES256 and RSAES-OAEP, AES-Galois Message Authentication Code-(GMAC)). Unfortunately, the specification recommends TLS_RSA_WITH_AES_128_SHA as mandatory, but TLS_RSA for key exchange is broken (Bleichenbacher attack). Both regular and ephemeral Diffie Hellman key exchanges are supported. The Data-in-Flight working group notes that regular Diffie-Hellman does not support perfect forward secrecy. IEEE 1815-2012 also allows for pre-shared keys and provides optional methods to remotely

[31] https://tools.ietf.org/html/rfc7465

[32] https://www.openssl.org/blog/blog/2016/08/24/sweet32/

			change pre-shared keys using either symmetric or asymmetric (public key) cryptography.

Table 5 summarizes the security requirements in IEEE 1815/DNP3 SA while also outlining poorly defined features. The following recommendations are provided to improve the security of IEEE 1815/DNP3 SA:

Encryption: The Data-in-Flight working group recommends using TLS with a stronger cipher suite e.g. TLS_ECDHE_ ECDSA_WITH_AES_128_GCM_SHA256 or TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384. For bulk encryption, the working group notes that AES with mode ECB in the specification is insecure and SHA is broken.

Device Authentication: DNP3 implementations using Transport Layer Security (TLS) shall comply with the requirements for certificate management taken from IEC/TS 62351-3. IEC 62351-3 supports X.509 certificates. The Data-in-Flight working group recommends that a security policy to disallow self-signed certificates in the specification be implemented.

Authorization: For multiple users, the specification permits access based on identity or roles using roles-based access control with limitations. The roles are defined in IEC 62351-8, which uses RBAC defined in either the x509v3 certificate or software tokens to grant access to information. Reviews from "A security evaluation of IEC 62351" indicate that certificates tied to specific roles become invalid when the roles change, thus requiring the issuance of new certificates – a non-trivial and costly process. Further recommendations from the paper are that "certificates are better suited for providing authentication to entities with a relatively long life-time while software tokens allow for flexibility in assigning and changing roles and should be used for authorization."
Again, efforts by the DER Access Control work group to implement polices to grant access to resources as needed is recommended for consideration.

Cipher suites: The Data-in-Flight working group recommends that DNP3-SA enables ephemeral key exchange and update the recommended cipher suites for strength. For example, bulk encryption with the stream cipher RC4 is deprecated and SHA for message authentication used during key exchange is broken.

4.6 IEC 61850/62351 Observations and Recommendations

Table 6: Trust and Cryptography Features of IEC 61850/62351 Security Capabilities

Protocol	Encryption (Data Confidentiality and Integrity)	Device Authentication	Key Exchange Algorithms
IEC 61850,	IEC 62351-3 requires TLS v1.2 or higher. For backward compatibility,	Uses X.509v3 Digital	IEC 62351 mandates the use of RC4, regular

IEC 62351-3, -4, & -6	support of TLS version 1.0 and 1.1 is specified. The Data-in-Flight working group notes that backwards compatibility though important, makes allowances for security loopholes which for example, in practice makes dangerous misconfigurations of TLS commonplace[33]. The cipher suites listed by IEC 62351-4 makes use of RC4 that is deprecated and 3DES for which NIST is developing a deprecation timeline[34].	Certificates per IEC 62351-9. Mutual client/server authentication is required at a minimum.	and ephemeral Diffie-Hellman key exchanges. IEC 62351-9 allows the use of pre-shared keys, CRLs, and OCSP. It includes the use of PKI with certificates, including attributes for black and white lists. It also includes asymmetric key generation requirements. The option of using non-PKI self-signed certificates in small deployments in addition to authorization and validation list are specified. The Data-in-Flight working group notes that regular Diffie-Hellman does not support perfect forward secrecy while RC4 has noted vulnerabilities[35,36]. The working group also recommends that a security policy to disallow self-signed certificates be implemented.
IEC 62351-7	Reliable system and network management using SNMP management information base (MIBs).		
IEC 62351-8	Role-Based Access Control. RBAC follows the security principle of least privilege which enables several security		

[33] Advances in Cryptology -- CRYPTO 2014: 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part II. (2014). Germany: Springer Berlin Heidelberg.
[34] https://csrc.nist.gov/News/2017/Update-to-Current-Use-and-Deprecation-of-TDEA
[35] https://www.cvedetails.com/cve/CVE-2015-2808/
[36] https://nvd.nist.gov/vuln/detail/CVE-2017-8076

	policies, networking, firewall, back-ups, and system operations.		

IEC 62351 has many cross-references due to the number of protocols it is composed of. Figure 3 identifies all the interrelationships between various protocols and IEC 62351 parts. Figure 4 identifies the specific IEC 62351 parts needed for securing IEC 61850-8-1 and IEC 61850-8-2 client-server protocols as well as the conformance test requirements (IEC 62351-100-3 and IEC 62351-100-4).

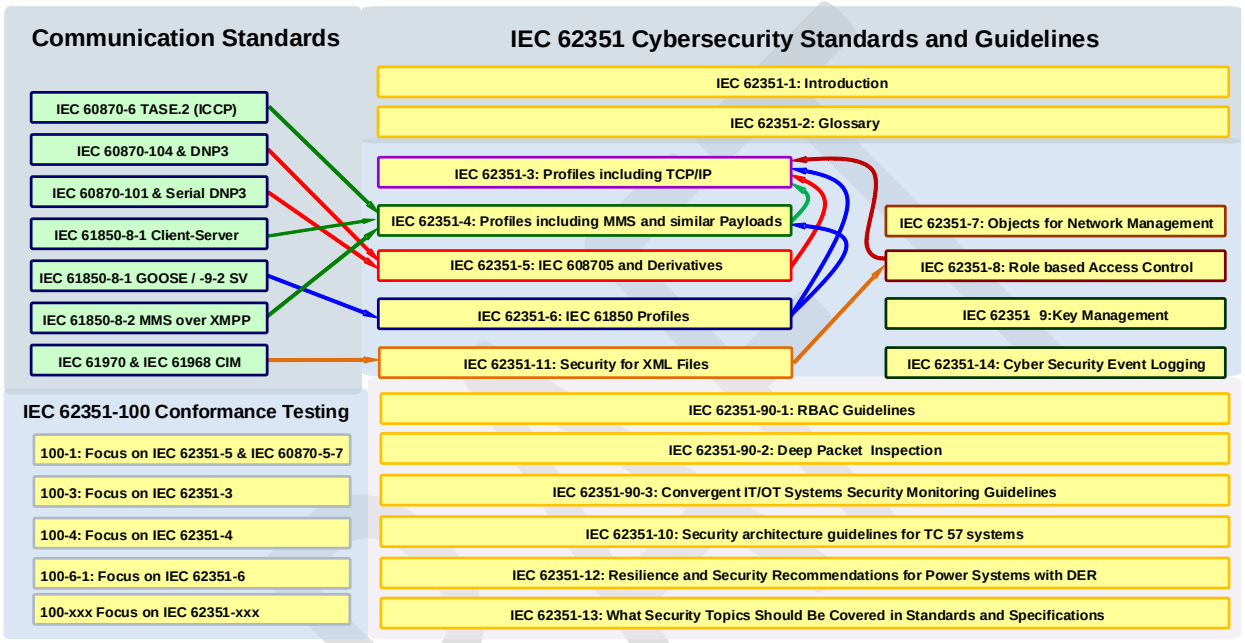

Figure 3: Overall Mapping of IEC 62351 cybersecurity standards to protocols

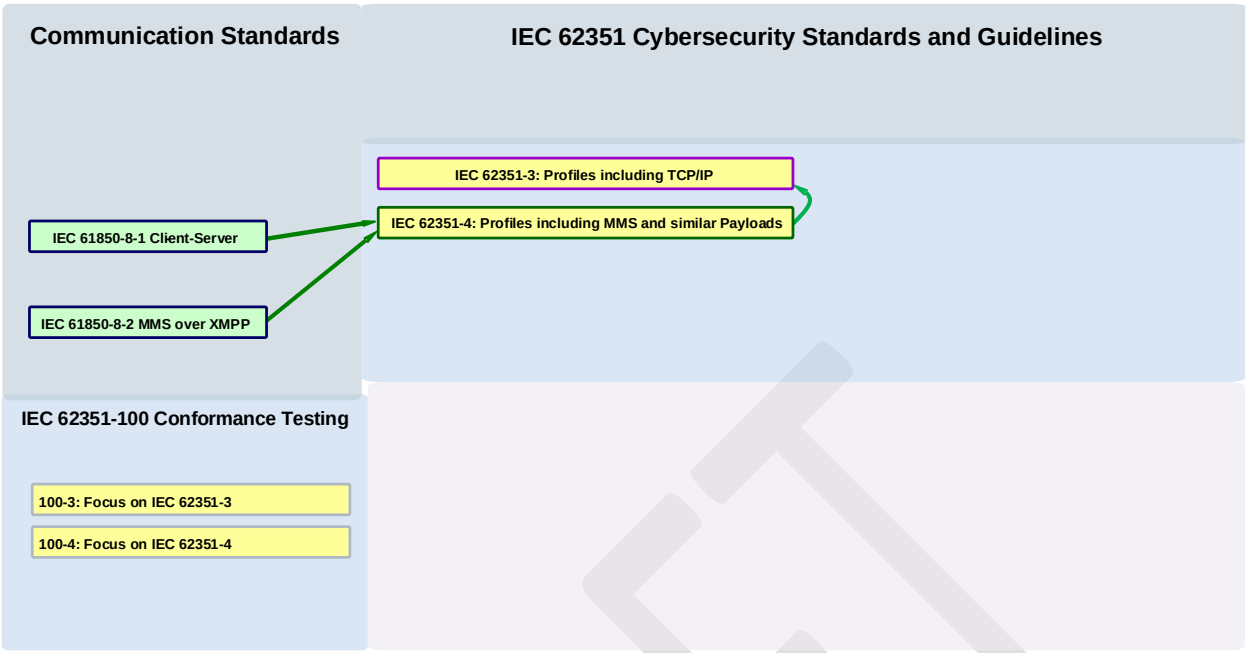

Figure 4: IEC 62351 cybersecurity standards for IEC 61850-8-1 and 8-2 client-server protocols

5 STATE OF THE ART SECURITY FEATURES FOR THE COMMUNICATION PATHS

The three generalized paths under discussion as depicted in Figure 2 are utility to aggregator, utility to DER, and aggregator to DER. The protocol stack for these communication paths are the information model, the application protocol, the transport layer, the network layer, and the physical communication media which could be combinations of serial, ethernet, cellular, or other physical media.

With California Rule 21, California leads with state-of-the-art smart grid policy, requiring that the paths to utilities implement secure communications using IEEE 2030.5 as the default protocol. The aggregator-to-DER path in California and all paths outside of California are not, however, bound to a secured protocol. An array of legacy, proprietary, and standard protocols remains in use. Additional example aggregator communications would be Inter Control Center Communication Protocol (ICCP) over leased lines to utilities, or wireless and internet-based protocols to DERs[37] (secured by IEC 62351-3 and IEC 62351-4).

The security features of the protocols required for DER interoperability, i.e. IEEE 2030.5, IEEE 1815, and SunSpec Modbus, and IEC 61850/IEC 62351 have been discussed in the sections above, and these protocols may be found in all three of the depicted paths. As shown previously, security is not a mandate within the scope of the interoperability standard, IEEE 1547.

[37] https://www.energy.gov/sites/prod/files/2015/06/f24/load_participation_ancillary_services.pdf, accessed Feb 3, 2020

Despite its attendant issues, one of the current best practices for communication and control security on internet-based protocols is, like IEEE 2030.5 and IEC 61850-8-2, to require transport layer security (TLS) to provide authentication, encryption, and data integrity for the data in transit. In addition, TLS can be used by any protocol that uses TCP/IP. As noted by stakeholders, tunneling IEEE 1815 (DNP3) and other protocols through mutual TLS tunnels[38] has worked quite well in a variety of distribution and transmission scale real-time control integration scenarios. Also, DNP3 SAv5 is seldom supported and, even when supported, it is cumbersome to work with. Rather than replacing built-in communication modules that lack security and are deemed irreplaceable, devices providing TLS can be inserted into the communication path to improve the security of legacy devices. However, TLSv1.2 defines many cipher suites, some of which are known to be compromised. Improvements to security and performance of TLSv1.2 informed the move to TLSv1.3. Therefore, the right selection of allowed cipher suites, preventing the peer device to switch to less-secure cipher suite or TLS/SSL version are crucial elements to secure a device. It is non-trivial to upgrade serial communication to IP-based communication, but there are devices that take in serial, encrypt and transfer data over TCP/IP. In keeping pace with technological advancements, it is critical that new DER hardware natively secure the communication protocol.

At the local gateway in the DER stack, the DER device has multiple communication options or interfaces designed to provide solutions to improve the installation process, monitoring, troubleshooting, and overall system reliability. To enable third-party access to data or the provision of remote maintenance, secure gateways compliant with DER communication protocols are recommended. Secure gateways enable amongst others:

- Secure remote management of devices including certificate management
- Securing device with low physical network security
- Ensure that only approved or signed firmware runs on the gateway
- User access management with granular permission levels
- Whitelisting and firewall capabilities
- Traffic inspection and logging

Although the output from this work is to define communication (data-in-transit) requirements to reach a consensus distributed energy resource (DER) cybersecurity standards, comprehensive security requirements and strategies for DER integration in the power grid can be found in NIST's 2014 Guidelines for Smart Grid Cybersecurity[39]. As evidenced by the three volumes comprising nearly 700 pages, the subject is nontrivial, encompassing security training, auditing, incident response, and more. NIST's guide thoroughly discusses security objectives, as well as solutions and their attendant implementation issues.

[38] https://www.pjm.com/markets-and-operations/etools/jetstream.aspx
[39] https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7628r1.pdf, accessed Feb 2, 2020

6 RECOMMENDATIONS FOR HARMONIZING DER COMMUNICATIONS PROTOCOLS SECURITY FEATURES

Cryptography, as previously noted, is an indispensable tool for protecting information in computer systems both at rest and in transit. In the DER network, it is important to ensure the authentication and integrity of the data, that the identity of the devices communicating are verified, and that the cryptographic keys used for protecting the data are appropriately managed. The current state of art segments of this tool is explored below leading to recommendations for unified security requirements.

6.1 Authenticated Encryption

For data encryption, the symmetric encryption (using a shared key that is determined via asymmetric encryption) algorithm AES with GCM or CCM cipher modes or Chacha20 are recommended per TLSv1.3. To implement authenticated encryption, authenticated encryption with associated data (AEAD) algorithms are recommended [40]. This assures integrity and authenticity of both encrypted and unencrypted information in the data while also ensuring confidentiality of the encrypted information. The visible header in a message needs integrity while the payload needs integrity and confidentiality. Both the header and payload need authenticity. AES_GCM is recommended because of the improved performance over CCM on most hardware and prevents ciphertext malleability. Aside, though, CCM was historically favored for many constrained device applications since encryption and decryption are performed by the same process, thus saving resources.

6.2 Device Authentication

The X.509 digital certificates help devices establish a secure connection in a PKI infrastructure by formally binding cryptographic keys to a device's identity. Per TLSv1.3, the algorithm for signing or verification should either be RSA, ECDSA, or EdDSA for digital signatures used as proof of identity. TLS controls the cipher suites that are offered, and the device certificates contains the public key for use with the device authentication. The certificates also specify expiration dates and other information in its data structure. For key lifecycle management best practices, it is recommended that the certificates be used for identification and authentication and not authorization. Authorization can be granted to a device in the form of an access control policy.

6.3 Cryptographic keys

PKI works by using a combination of asymmetric and symmetric processes. The symmetric process makes use of a secret cryptographic key while the asymmetric process uses two different cryptographic keys: a public key and a private key. The asymmetric process enables the generation of the symmetric key used for data encryption. The public key is available for encrypting information to the device associated with the private key. The private key may be used by that device to decrypt the encrypted information and create digital signatures. The private key is kept secret and represents "ownership." It is recommended to securely store the private key to prevent rogue device impersonation and to require pseudorandom unique keys. Research methods to secure device keys include the use of hardware security mechanisms like Mobile Trusted Module. Per IEC 62351-9,

[40] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

"during transport, the private key shall be protected against eavesdropping and tampering by being encrypted by a transport key such as defined in PEM, PKCS#8 ad PKCS#12." Research alternatives to securing the DER device private keys and querying security critical information by the SunSpec Blockchain work group efforts are in place. The proposed measures use permissioned blockchain, a technology that is intended to complement existing DER technology.

6.4 Ephemeral Symmetric Key Establishment

After the PKI-based mutual authentication is established, an ephemeral key can be established for efficient communications using a symmetric data encryption algorithm. The elliptic curve algorithm which is stronger and more efficient than RSA is recommended for key exchange. RSA based key exchange do not allow for forward security. In an RSA communication, one endpoint will generate the symmetric session key, encrypt it with the peer's public key. Once the RSA private key is broken, all communication is leaked, as the session keys can be re-created. Diffie-Hellman ephemeral prevents this. The key establishment algorithm should be ECC using the Diffie-Hellman ephemeral key agreement.

6.5 Transport Layer Security

In 2013, TLS version 1.2 was the latest standard for providing communication security over a network. In 2018, TLS version 1.3 was approved as an RFC[41] (Request for Comment). TLS 1.3 has made many changes to improve security[42]. For example, it has removed all insecure algorithms of TLS 1.2 and eliminated RSA for public key exchange algorithm. Another key element in TLS 1.3 is the deprecation of TLS version negotiation, which allowed downgrade of the TLS version.

To provide an umbrella security requirement of the communication protocols, it is recommended that new specifications (and new versions of a specification) use TLS 1.3 rather than TLS 1.2 to improve performance and security for TLS transactions.

Table 7 represents the proposal for a unified set of security recommendations for IEEE 2020.5, IEEE 1815, SunSpec Modbus, IEC 61850, IEC 62351 application protocols.

Table 7: Proposed Common Trust and Cryptography Features in DER communication Protocols

Protocol	Data Encryption (Bulk traffic) & Data Authentication	Device Authentication	Key Management
IEEE 2030.5, CSIP **SunSpec Modbus** **IEEE 1815, DNP3-SA** **IEC 62351-3** **Others**	Use TLS v1.3 with the following recommendations: **Encryption**: AES with GCM or CCM modes only (i.e. no electronic codebook mode because ECB is not a FIPS approved mode). **Authentication**: Authenticated encryption with additional data (AEAD) such as AES Galois Counter Mode	X.509v3 Digital Certificates with the following recommendations: Mutual client/server authentication is required at a minimum. Recommend the Digital Certificate only be used for identification and authentication. Another	Per TLSv1.3: **Bulk Traffic Encryption Key:** Ephemeral symmetric key derived by client and server using Diffie-Hellman Ephemeral or Elliptic Curve Diffie-Hellman Ephemeral **Signing Key:** Node Authentication by signatures generated with RSA, ECDSA, or EdDSA. **Caveat:**

[41] https://tools.ietf.org/html/rfc8446

[42] https://owasp.org/www-chapter-london/assets/slides/OWASPLondon20180125_TLSv1.3_Andy_Brodie.pdf, accessed Feb 20, 2020

	(AES_GCM_SHA256) reduces overhead by combining encryption and authentication operations. The use of longer authentication tags is recommended.	mechanism e.g. Access Control List (ACL) on the server is proposed to be used for authorization.	Recommend Elliptic Curve, not RSA with caution, for digital signature due to known weakness in TLS (Bleichenbacher cache attack against RSA node authentication key). This is in addition to the advantages of smaller keys and fast binary curves in hardware, as examples.

6.6 Review of PKI Technology and Application in DER

PKI is emerging as the de-facto standard for authentication, identification, and digital signatures. With PKI, certificates can be issued, distributed, stored, used, verified, and revoked using public key cryptography. For these DER communication protocols, some of the implementation challenges includes;

- Truly random private key generation
- Private key generation in a secure environment (e.g. secure element (SE) or Trusted Platform Module (TPM)?). If generated outside of the environment, how is it securely provisioned?
- Private key storage
- Private key access control - Who can use it to sign?
- Certificate signing
- Certificate management (renewing, updating, removing)
- Dependence on a large set of certificate authorities
- Certificate revocation check (e.g. OCSP, CRL, OCSP stapling)

The unified security recommendations, however, do not address the different implementations of PKI for these communication protocols. For example, IEEE 1815/DNP3 SA adopts CRLs or OCSP—while IEEE 2030.5 does not. Arguments for the use of CRLs include the revocation of a compromised device, while the arguments against CRLs includes the lack of reliable infrastructure (e.g. intermittent connectivity and/or accurate time references) for CRLs or OCSP in the IoT space. OCSP stapling is meant to help, by allowing the server to attach a "pre-generated" OCSP response into the TLS handshake, to prove that its certificate is not revoked. An optional support for CRLs is recommended, so that there are explicit requirements for future device-certification revocation – a process not currently supported but that could be part of future enhanced operational security.

The current PKI model for IEEE 2030.5 assumes a non-revocable and non-expiring device certificate for identification and authentication[43]. Based on feedback from stakeholders in the DER community, there are use cases that can benefit from a PKI that allows for finite time authorization and support of revocation. The support for revocation per the Recommendations for Trust and Encryption in DER interoperability Standards recommends DER stakeholders "create a procedure

[43] https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-02-2018-1.pdf

to systematically report and address a revoked certificate." A proposed new PKI model proposes to augment the existing IEEE 2030.5 PKI model with functionalities that can cater to these use cases and more.

6.6.1 Public Key Infrastructure

The following enumerates the basic PKI assumptions for IEEE 2030.5.

- The root CA and/or subordinate CA's issue device certificates.
- All devices have a device certificate issued by an official CA provider.
- X.509 digital certificate with an infinite lifetime be used to identify servers and clients.
- All devices have a copy of the root CA public key.
    - This key is obtained out of band (e.g. directly from the root CA or other trusted source).
    - This key is used to validate the certificate chain exchanged during the TLS handshake.
- The device certificates are used for mutual authentication of the client and server during the TLS handshake.
- These device certificates are used for identity-based Access Control to server resources.
    - For IEEE 2030.5, the Long Form Device Identifier (LFDI) and the Short Form Device Identifier (SFDI) that are used in some function sets are based on a SHA-256 hash of the device's certificate.

6.6.2 Problem Statement

The current PKI model for IEEE 2030.5 assumes a non-revocable and non-expiring device certificate used for identification and authentication.

6.6.3 Basis of PKI Model

The basic concepts of the new PKI Model come from *IEEE 802.1AR: IEEE Standard for Local and Metropolitan Area Networks – Secure Device Identity*[44]. This standard introduces the concept of DevID's, **Dev**ice **ID**entifiers, consisting of a public-private key pair and an associated certificate. There are two types of DevID's: IDevID and LDevID.

[44] IEEE Standard for Local and metropolitan area networks - Secure Device Identity," in *IEEE Std 802.1AR-2009* , vol., no., pp.1-77, 22 Dec. 2009 doi: 10.1109/IEEESTD.2009.5367679
keywords: {computer network security;cryptographic protocols;IEC standards;IEEE standards;ISO standards;local area networks;metropolitan area networks;data reception;authentication protocol;initial manufacturer-provisioned DevID;cryptography;secure device identifier;local area network;metropolitan area network;information exchange;information technology;ISO-IEC-IEEE 8802-1AR standard;IEEE Standards;Authentication;Local area networks;Metropolitan area networks;Object recognition;Protocols;802.1AR-2009;access control;authentication;authorization;certificate;LANs;local area networks;MAC security;MANs;metropolitan area networks;PKI;port-based network access control;secure association;secure device identifier;security;X.509;access control, authentication, authorization, certificate, LANs, local area networks,;MAC security, MANs, metropolitan area networks, PKI, port-based network access control, secure;association, secure device identifier, security, X.509},
URL: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5367679&isnumber=5367678, accessed Jan 30, 2020

6.6.3.1 IDevID – Initial Device Identifier

This identifier is cryptographically bound to the DER device and is installed at manufacture time into the device.

- The main use is to provide an authenticated identity.
- It is equivalent to the birth certificate of the device.
- It does not expire.
- It cannot be revoked.
- The current IEEE 2030.5 device certificate is equivalent to an IDevID.

6.6.3.2 LDevID – Local Device Identifier

This identifier is cryptographically bound to the DER device but can be installed in the field.

- The main use is to provide authorization.
- It is equivalent to a driver's license for the device.
- It has a finite lifetime.
- It can be revoked.
- The current IEEE 2030.5 specification does not support the use of an LDevID.

6.6.4 New PKI Model Proposal

The New PKI Model[45] proposes to augment the existing PKI Model with the LDevID functionality. This will ensure backward compatibility. This proposal is based on the IEEE 802.1AR: Secure Device Identity recommendation.

6.6.4.1. IEEE 2030.5 Client Device Operation

The client device is assumed to have an IDevID and possibly an LDevID.

- If the device only has an IDevID, use it for TLS communications with the server. This mode of operation maintains backwards compatibility with the current PKI.
- If the device has both an IDevID and a LDevID, it uses the LDevID for TLS communications with the server.
- If LDevID is used, there must be a process for renewing an expired LDevID.

6.6.4.2. IEEE 2030.5 Server Device Operation

The server device is assumed to have an IDevID and possibly an LDevID.

- If the device only has an IDevID, this is used for TLS communications with the client.
- If the device has both an IDevID and a LDevID, LDevID is used for TLS communications with the client.
- If LDevID is used, there must be a process for renewing an expired LDevID.
- If the server receives an IDevID from a client, it MAY choose to accept or reject the connection based on policy. (This flexibility would allow the server to decide whether backwards compatibility is desired (accept) or not (reject)). It is expected that new systems

[45] G. Lum, personal communication, March 14 2019

reject for added security, while old systems with already fielded devices would accept. Fielded clients probably have no mechanism to update, replace, or install new certificates). To augment security without breaking backward compatibility, it is recommended to include a mechanism[46] to indicate the availability of an LDevCert in the IDevCert. This would allow the server to reject a possible compromised LDevID, knowing that the client has LDevID certificate available. For example, a simple Boolean value:

```
id-ce-lDevCert OBJECT IDENTIFIER: = {id-ce XX}
lDevCert BOOLEAN DEFAULT FALSE
```

where the id-ce anchor for the extension could as an example, be a SunSpec PEN number, would allow an endpoint to process unknown extension.

- If the server receives an LDevID from a client, it SHALL validate the certificate before authorizing access.

6.6.4.3. IEEE 2030.5 Device Identity

Access to IEEE 2030.5 server resources is determined by the identity of the client requestor. The identity is based on the Long-Form and Short-Form Device Identifiers, which are derived from the SHA-256 hash of the client's certificate. In theory, the server maintains an ACL for each resource it hosts. The ACL consists of a list of LFDI or SFDI entries authorized to access that resource.

The New PKI Model should use the same LFDI/SFDI model for access control. However, the LFDI/SFDI is derived from the IDevID and TLS communications with the server uses the LDevID. For the server to perform its identity-based access control function, this means the LDevID must contain the LFDI/SFDI information of the IDevID. Perhaps this can be done by changing the Subject to be non-empty for device certificates and using the LFDI of the IDevID as the common name (CN) of the LDevID subject field.

6.6.4.4. Provisioning LDevID

The provisioning of an LDevID into a device should be in scope of IEEE 2030.5. It may be done at installation time, through manual truck-rolls, or remotely. Regardless of the method used, provisioning should account for the following:

- It must be done in a secure way to prevent hacking, cloning, etc.
- The LDevID must be securely bound to the correct device. There should be checks to ensure an LDevID for device A cannot be installed into device B. Devices should reject an LDevID if it is not compatible with its IDevID.
- Only the entity that has access to the IDevID of a device should be able to request/obtain an LDevID for that device. This must also be pseudo-randomly generated and unique between devices.

Revocation mechanisms only apply to LDevID. IDevIDs are permanent and non-revocable. Standard methods of revocation like OCSP stapling for server side LDevID is recommended. This will prevent high OCSP traffic for the same server certificate, and clients don't need to go online for checking.

[46] https://tools.ietf.org/html/rfc5280#page-26

6.6.5 Root Certificate and Registration Process Recommendation

To establish root of trust for certificates, a single neutral, third-party operated root CA for all utilities, electric power aggregators, and OEM vendors is recommended. If this approach were not taken, multiple trust chains would be mapped to different trust anchors and there would be greater overhead and less interoperability of DER devices (since not all utility or aggregator servers could talk to all DER). However, broader discussion on the feasibility of a single CA needs to occur between utilities and implementors to decide if this is a recommended path going forward. An alternative could be for each utility (and possibly implementors) operate its own CA, with acknowledgement that DERs are not bloated operating systems with a hundred certificate stored on hand. A large certificate store may also encourage system owners to add a backdoor (secure or insecure) for their own remote monitoring and control that can be easily exploited.

Work being done by blockchain technologies and trustless protocols to build networks of trust without a central trust as provided by the CA is still in a nascent stage. Issues such as scalability and reliability need to be addressed before it is utilized in DER systems.

The basis for creating an identity for a device that can be verified for communications between DER and utility in the PKI is through a registration process. It is recommended that the registration process be adequately protected to prevent the introduction of rogue devices. Certificates exchanged during TLS should be used for authentication (i.e. identifying the client). Other mechanisms like access control policy should be used for authorization (that is, allowing or denying general access).

6.7 Impact of Security Features Implementation on DER Hardware

Impact to real-time operation of DER systems from newly imposed security requirements must be within prescribed limits for communication-based control of devices supplying grid-support functions. Cryptographic functions such as those recommended for DER systems are implemented either in software or directly on specialized hardware. Systems without cryptographic hardware should rely heavily on standard software libraries to support encryption, authentication, and hashing operations executed on the CPU. Software secured with the use of custom code is typically more vulnerable to attack than those that rely on standard libraries. Several experiments were conducted to determine the communication latency associated with adding software-based security features to DER networks.[47] The results indicate that the proper implementation of these security features did not impact DER-based grid control systems but improved the security posture of the devices and networked system. However, further analysis into other aspects like the CPU usage, delays in processing other inputs or outputs, device temperatures, hardware issues like other errors, warnings, or other messages are factors to be considered.

6.8 Review of Latency in Emulated DER Power-Communication Environment

Recent research assessing a DER communication network implementing network segmentation, encryption, and a moving target defense security feature in a power communication co-simulation environment, evaluated the impact of increased latency attributed to these features to power system

[47] I. Onunkwo, P. Cordeiro, B. Wright, N. Jacobs, C. Lai, J. Johnson, T. Hutchins, W. Stout, A. Chavez, B. T. Richardson, K. Schwalm, "Cybersecurity Assessments on Emulated DER Communication Networks," SAND2019-2406, March 2019.

operations and performance. Cipher-specific round trip times for cryptographic algorithms with TLS transport security are shown in Figure . Results from the emulated system using low cost embedded devices indicate adding encryption does not adversely impact DER-based grid control systems. It is noted that the complexity level of the emulated system was not necessarily representative of hardware implemented in the field, as communication times for traffic traversing many hops in large physical networks may be much greater than those shown in Figure . What is significant is that the change in roundtrip time due to addition of encryption is on the order of milliseconds. Other research[48] supporting the implementation of cryptographic hardware (ModuleOT) to secure DER communication indicated that the latency attributed to encryption is well below the IEEE 1547-2018 limits for DER latency.

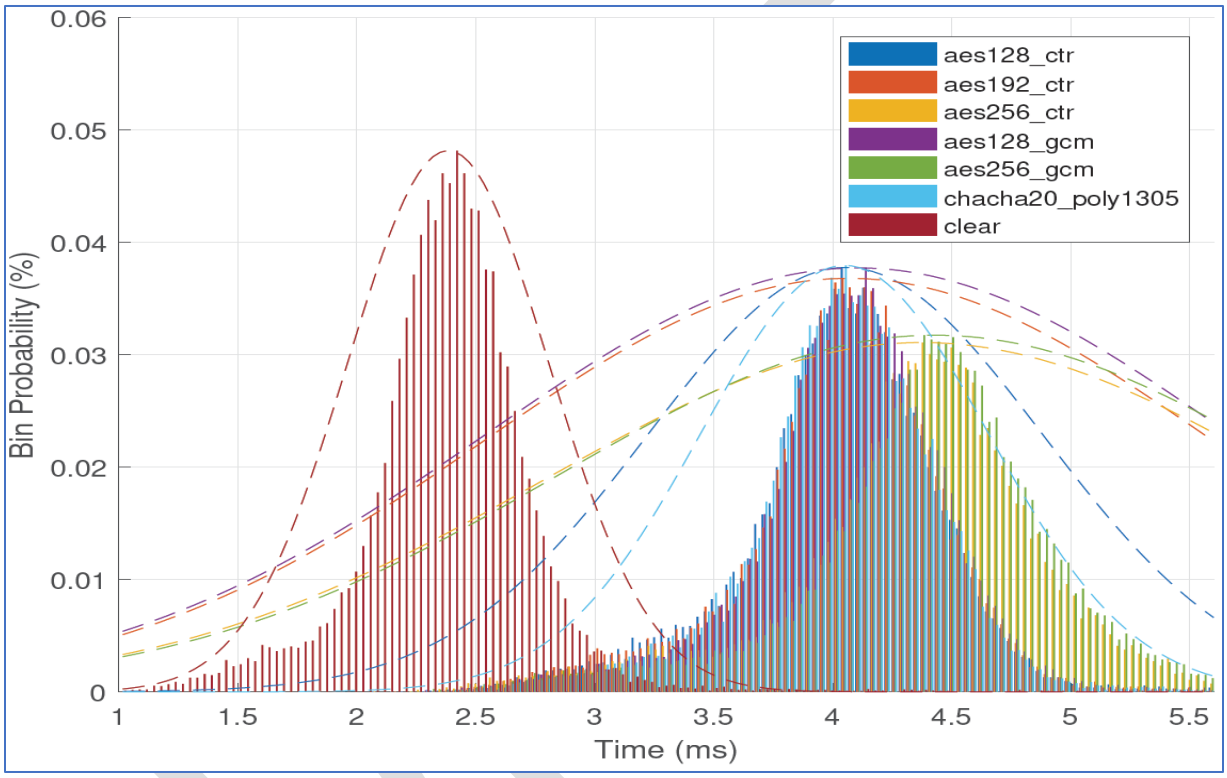

Figure 5: Histogram of round-trip Modbus communication times, given unique TLS symmetric ciphers and cipher modes

6.9 Next Generation Solutions

There has been discussion amongst stakeholders to develop even more advanced security capabilities for a future distributed smart grid. A solution such as named data networking (NDN) uses an alternative to Internet Protocol (IP) model of communication[49] to support cyber secure multi-party communications and control using any communication link. In the NDN (e.g. using the publish-subscribe architecture), the data itself is signed and named according to predefined trust rules and schemas, thereby, providing data-centric security and name-based trust schemas. These

[48] Cordeiro, Patricia G., Onunkwo, Ifeoma, Jacobs, Nicholas, Jose, Deepu, Wright, Brian J, & Hossain-McKenzie, Shamina. *Module OT Laboratory Test Procedure.*. United States. doi:10.2172/1592860.

[49] L. Zhang, D. Estrin, J. Burke, V. Jacobson, J. Thornton, D. K. Smetters, B. Zhang, G. Tsudik, k. claffy, D.Krioukov, D. Massey, C. Papadopoulos, T. Abdelzaher, L. Wang, P. Crowley and E. Yeh, "Named DataNetworking (NDN) Project," PARC: A Xerox Company, Palo Alto, CA, US, 2010.

secure designs must be scalable and employ effective embedded systems to enable applications reliably achieve data authenticity, confidentiality, and availability with fully secure end-to-end communication in any pattern (one to many, many to one, and any to any). It is advised to incorporate these new cybersecurity R&D efforts into future solution sets as the industry matures.

7 CONCLUSION

A future filled with hundreds of millions of interoperable DER systems is fast approaching. In preparation, efforts were made to explore and document security-related limitations. Critically, a lack of standardized cryptographic solutions is likely to pose future concerns for the authentication, authorization, integrity, confidentiality, and availability of DER systems. In response, recommendations are made to identify and potentially modify data-in-transit guidelines for IEEE 2030.5, IEEE 1815, SunSpec Modbus, and IEC 61850-8-1/8-2 addressing mutual authentication, authorization, data integrity, availability, and key management. These recommendations for production systems include:

1. Using cybersecurity standards and avoiding any proprietary security technologies
2. Adopting modern cipher suites possessing strong security protections
3. Requiring at least TLS 1.2 and recommend TLS 1.3 for all DER communications
4. Requiring mutual authentication between all systems and devices
5. Requiring authorization of interactions based on Role-based Access Control (RBAC)
6. Protecting private keys and long-term symmetric keys that prove the identity of each entity
7. Requiring key management through PKI with certificate revocation
8. Requiring network and system management through SNMP or similar standards
9. Requiring secure DER gateways for separation of security domains and protocol translations, including for cloud integration
10. Investigating the potential to incorporate proven new options for multi-party communications such as NDN

Key stakeholders have been discussing the advancement of security capabilities for the future envisioned distributed smart grid. To secure their vision, they will need to include strong encryption capabilities, in support of DER communication protocols. The use of hardware security modules and firmware signing as underlying prerequisite to maintaining DER communication security is exigent. It's also important that system owners keep pace with these developments by routinely upgrading, updating, and patching systems. Physical measures to protect the DER most also be considered. Moving forward, it's advised that cybersecurity research and development investments continue to be made in advancing the field, for instance, in the development of new multi-party communication models. Per NIST, compiling research needs for smart grid security advancement, including device-, system-, and network-level topics, cryptography, and federated and cross-domain systems must be actively undertaken by DER stakeholders.

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Charles Hanley	8810	cjhanle@sandia.gov
Jennifer Depoy	5620	jdepoy@sandia.gov
Summer Ferreira	8812	srferre@sandia.gov
Brian Gaines	9366	bgaines@sandia.gov
Jason Stamp	5623	jestamp@sandia.gov
Jay Johnson	8812	jjohns2@sandia.gov
Ifeoma Onunkwo	9366	ionunkw@sandia.gov
Legal Technology Transfer Center	11500	
Technical Library (electronic copy)	01977	sanddocs@sandia.gov

Hardcopy—External

Number of Copies	Name	Company Name and Company Mailing Address
1	Thomas Rueckert	U.S. Department of Energy 1000 Independence Avenue SW Washington, DC 20585
1	Jeremiah Miller	U.S. Department of Energy 1000 Independence Avenue SW Washington, DC 20585
1	Kemal Celik	U.S. Department of Energy 1000 Independence Avenue SW Washington, DC 20585

This page left blank

This page left blank

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.