SAND2018-9407R

General Requirements for Designing and Implementing a Cryptography Module for Distributed Energy Resource (DER) Systems

Sandia National Laboratories

SAND#

Module OT Project

James Baker, Patricia Cordeiro, Tom Doepke (NREL), Shamina Hossain-McKenzie, Christopher Howerter, Nicholas Jacobs, Deepu Jose, Christine Lai, and Jeffery Zhao

June 2018

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.

1 Introduction

Penetration of distributed energy resources (DERs) is rapidly increasing in the bulk power system (BPS); they are growing to be a significant portion of generation. As such, grid-support capabilities are being developed and implemented. However, as their presence increases, the impact of DERs on the BPS also increases. Therefore, if a disturbance occurs in the DER system, its effects could propagate throughout the BPS. These disturbances could range from equipment malfunctions to resource variability to cyber attacks. There are various emerging cybersecurity concerns in the realm of DERS, including the following:

- DER devices were originally designed to be static and, thus, do not address the emerging concerns and are not built with defenses.
- Presently, communications occur over public and poorly-secured networks.
- Grid attack surface is increasing with growth of DER systems and devices.
- Rise of advanced persistent threats (APTs), in which an adversary increases stealth, continuity, and complexity of attacks to achieve more sophisticated goals.
- Compromise of DERs, especially as penetration increases, would affect grid reliability and resilience that could lead to local power disruptions and/or BPS collapse.

Thus, cybersecurity is a major concern for DERs and must be addressed. When assessing DER cybersecurity, we must consider its impact to confidentiality, integrity, and availability (CIA). The grid is traditionally solely concerned with availability, the ability to “keep the lights on.” Nonetheless, as cyber attacks that aim to manipulate data (e.g., fake data injection, control input spoofing) increase, integrity must be prioritized as well. Remote access and automated functions render DER devices vulnerable to such attacks; furthermore, personally identifiable information (PII) data is also at risk due to the use of private networks (e.g., customer-owned DERs). Additionally, power usage patterns could also be revealed and indicate whether a home/building is occupied or not. Therefore, confidentiality must also be protected---alongside integrity and availability. It is important to prevent the release of sensitive data, including PII and topology information. Data manipulation must also be prevented; an adversary, if successful, could mask malicious actions (e.g., report normal status during attack), perform false data injection that can cause automated control actions to disrupt power system operation, and etc.

A defense-in-depth approach is needed to secure DER systems, providing different levels of security for different devices/processes. Solutions include proactive response mechanisms, intrusion detection systems (IDSs), segmentation, and etc. Specifically, for protecting confidentiality and integrity of data, encryption is a powerful technique. Various challenges exist for implementing cryptography, the main barriers being complexity and the lack of resources. However, research is progressing on developing lightweight and flexible application. This document will discuss general requirements needed for developing a distributed cryptography module for implementation in DER systems.

2 Composition of DER Systems

DER systems are comprised of different levels, which has been prevalently represented by the Electric Research Power Institute’s (EPRI’s) DER logical reference model that is extended from the National Institute of Standards and Technology’s (NIST’s) “Spaghetti Diagram” [1] [2]. This model is pictured in Fig. 1.

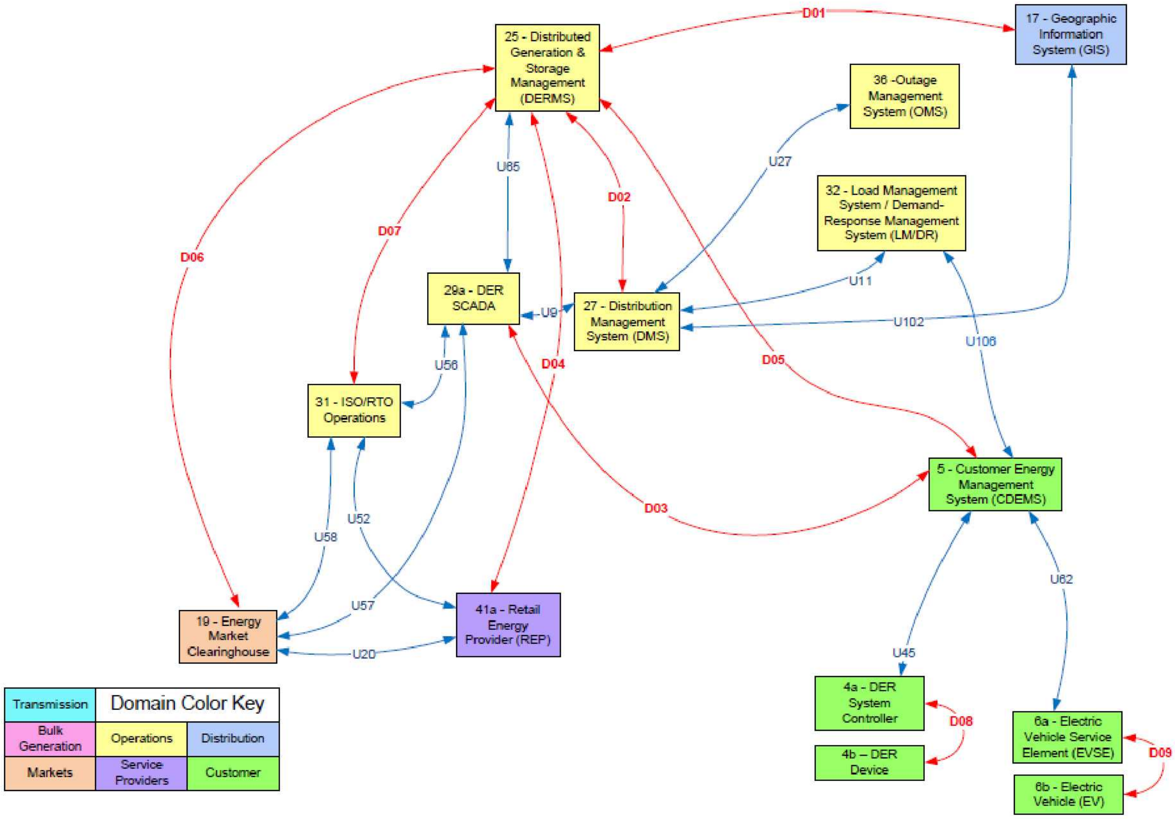
25 - Distributed Generation & Storage Management (DERMS)
17 - Geographic Information System (GIS)
36 -Outage Management System (OMS)
32 - Load Management System / Demand-Response Management System (LM/DR)
29a - DER SCADA
27 - Distribution Management System (DMS)
31 - ISO/RTO Operations
5 - Customer Energy Management System (CDEMS)
19 - Energy Market Clearinghouse
41a - Retail Energy Provider (REP)
4a - DER System Controller
4b – DER Device
6a - Electric Vehicle Service Element (EVSE)
6b - Electric Vehicle (EV)
D01
D02
D03
D04
D05
D06
D07
D08
D09
U85
U27
U11
U102
U106
U9
U56
U58
U52
U57
U20
U45
U62
Domain Color Key
Transmission
Bulk Generation
Operations
Distribution
Markets
Service Providers
Customer

Figure 1: EPRI's DER logical reference model *[2]*.

The connections in Fig. 1 represent logical interfaces; this provides a basis for understanding locations where encryption (for confidentiality and/or integrity) may be desired. DERs use a hierarchical control structure because utilities interact with DERs on a high level while individual DER systems manage themselves locally. Therefore, utility level communications have a much higher impact on the grid operations---though, they may already be secured due to North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) plan's regulations [3].

Current security practice is mandated by impact on grid reliability if a certain system is compromised. The NERC CIP plan provides details on these practices and informs the five EPRI tiers that describe the necessary functions and security requirements in terms of CIA for DER systems. Note that DER tends to be under MW / MVAR requirements for NERC CIP, so would generally be low impact under those regulations. The NERC CIP requirements are detailed further in Section 3.

According to EPRI's DER logical reference model shown in Fig. 1, each of the levels and their pertinent features can be summarized as follows [2]. Impact to Confidentiality (C), Integrity (I), and Availability (A), system impact, and Personally Identifiable Information (PII) is indicated for different interfaces in each of the levels.

Level 1: Autonomous DER Cyber-Physical Systems

- This level encompasses the independent cyber-physical DER systems, from photovoltaic (PV) systems to wind farms; the potential impact of exploiting one of the autonomous DER systems is minimal. Presently, there is not enough penetration to effectively dent system, though penetration levels are projected to be higher in the future.

- Some relevant characteristics regarding cyber security concerns include:
    - Does not include WAN communications.
    - Includes interface between DER controllers and physical devices.
    - Includes interface between electric vehicle supply equipment (EVSE) or charger and electric vehicle (EV).
    - Not physically protected (typically) or under jurisdiction of utility.
        - Vulnerable to local exploitation.

<u>Interfaces:</u>

- ❖ D08 – DER System Controller to DER Device
    - C = LOW, I = HIGH, A = HIGH, SYS. IMPACT = LOW
- ❖ Exception: functions that can bridge multiple Level 1 devices, such as firmware updates for all DER controllers.

Level 2: Facilities DER Energy Management Systems (FDEMS)

- Sites of DER, such as campuses, malls, virtual power plants, and etc.
- Manage multiple DER systems; potential impact could be minimal for small FDEMS to noticeable for large FDEMS.
    - Often general-purpose systems whose operating system (OS) networking and software contain well-known vulnerabilities.
    - FDEMS often connect to external systems such as utilities or market based ESPs.
    - Includes interface from FDEMS to DER.
    - Includes interface from FDEMS to EVSE.

<u>Interfaces:</u>

- ❖ U45 – DER System Controller to DER Device
    - For PII: C = HIGH, I = HIGH, A = LOW, SYS. IMPACT = MEDIUM
    - C = LOW, I = HIGH, A = HIGH, SYS. IMPACT = MEDIUM
- ❖ U62 – EV System Controller to EV Device
    - For PII: C = HIGH, I = HIGH, A = LOW, SYS. IMPACT = MEDIUM
    - C = LOW, I = HIGH, A = HIGH, SYS. IMPACT = MEDIUM

Level 3: Utility and Retail Energy Provider (REP) DER Information and Communications Technology (ICT)

- Encompasses utility and REP operations for power systems (e.g., Volt-VAr support, grid management); uses ICT to coordinate global behavior of FDEMS and DER.
- Potentially large impact to damage equipment or create BPS instability, communications over WAN potentially vulnerable.
- Other characteristics:
    - NOT real-time (typically).
    - Involves different types of interactions including market operations, monitoring, emergency control, power settings, scheduling, and etc.

Interfaces:

- U92 – Retail Energy Provider to FDEMS
  - C = High, I = Medium, A = Low, IMPACT = MEDIUM
- U106 – Load Management / Demand Response Management to FDEMS
  - C = High, I = Medium, A = Medium, IMPACT = MEDIUM
- D03– DER SCADA to FDEMS
  - C = LOW, I = HIGH, A = HIGH, IMPACT = High
- D05– DERMS to FDEMS
  - C = LOW, I = HIGH, A = HIGH, IMPACT = High

Level 4: Distribution Utility DER Operations Analysis

- Involves utility analysis of grid to determine if DER systems should modify operation to assist the grid, commands sent via Level 3.
- Power Flow situational awareness, contingency analysis, generation/load forecasts, and etc. are performed in this level.
- Large impact if compromised due to criticality to utility operations.
- Operations in this level are *internal* to distribution utility, and *might* fall under NERC CIP depending on system and how much impact it can have on grid operations [3].

Level 5: Transmission and Market Operations

- Larger utility environment, managing the bulk power system, and includes interactions with independent system operations/regional transmission organizations (ISOs/RTOs).
- Very large impact on power system; most likely requirements will fall under NERC CIP and any requirements needed for Level 4 may address Level 5 as well [3].

Each of the levels presented describe an interconnected, cyber-physical DER system and its interactions with the BPS. As discussed in each of the levels, various functions, devices, and interfaces are encompassed. Potential vulnerabilities and cyber attack impacts are also presented in terms of CIA, PII, and system impact. Another prominent resource is the NERC CIP requirements; it is presently the only national regulatory requirements for grid cybersecurity. These requirements encompass different cyber security standards that address 1) identifying critical cyber assets, 2) developing security management controls, 3) setting requirements for personnel and training, 4) implementing physical security, 5) managing systems security, 6) reporting incidents and response planning, 7) developing recovery plans, 8) managing configuration changes and vulnerability assessments, and 9) protecting information [3]. The various assets are given different levels of requirements based on their criticality and impact on the overall BPS. High, Medium, and Low impact levels are defined; these level descriptions and other details can be found in [3].

The NERC CIP requirements demonstrate the methodology and important factors that must be considered when assessing cybersecurity of a system. A similar, detailed analysis must be performed for DER systems to understand what devices, functions, and communications are critical to secure. In particular, for developing a distributed cryptography module for DER systems, it is important to carefully assess and select which assets to target for protection.

3 Introduction to Cryptography

With increased communication among DER systems, new opportunities for misuse will be accessible to potential cyber attackers and eavesdroppers. Cryptography presents a solution to these issues by enabling two parties, often referred to as Alice and Bob, to communicate without allowing an outside source, Eve, to understand what is being said. Ideally, the information (plaintext) is encrypted using a secret key, translated into ciphertext, and decrypted once it reaches its intended reader. Common applications include digital signatures, certificate authentication, and key management. However, it is important to note that cryptography is by no means a panacea for all security needs, but a powerful tool for ensuring the safety of one's data assets.

Symmetric cryptographic algorithms

Confidentiality is maintained through proper key management. If Bob and Alice keep their keys secret, Eve has no way of decrypting the data. When both parties share the same key for encryption and decryption, this is known as a symmetric cipher. These algorithms are often based on substitution and permutation functions and can further be categorized into stream and block ciphers. The former encrypts data one bit at a time and is based on the one-time pad, a cipher proven unbreakable; however, it is cumbersome due to the requirement that the key must be at least as long as the data encrypted [5]. For example, RC4 was a commonly used algorithm that could be found in 802.11 Wired Equivalent Privacy (WEP), a standard for Wi-Fi communication. Unfortunately, it was poorly designed, and messages between the client and access point were insecure [6].

Among block ciphers, the Advanced Encryption Standard (AES) is a widely used today. AES was announced in 2001 by the National Institute of Standards and Technology (NIST) after the Data Encryption Standard (DES) had been compromised. The organization chose the Rijndael algorithm out of 15 competing designs, and it is now deemed sufficient for use in protected classified information at a TOP SECRET level using its 192 or 256 key lengths [7]. The block cipher works by separating information into 128 bits (16 bytes). Info is encrypted with N rounds (10, 12, 14) depending on key length (128, 192, and 256) respectively. Each round consists of four layers – byte substitution, shift row, mix column, key addition. A simplified flow chart of the encryption can be seen in Fig. 2. There also exists lightweight cryptography algorithms, e.g., Blowfish and its successor, Twofish, and TEA (tiny encryption algorithm).

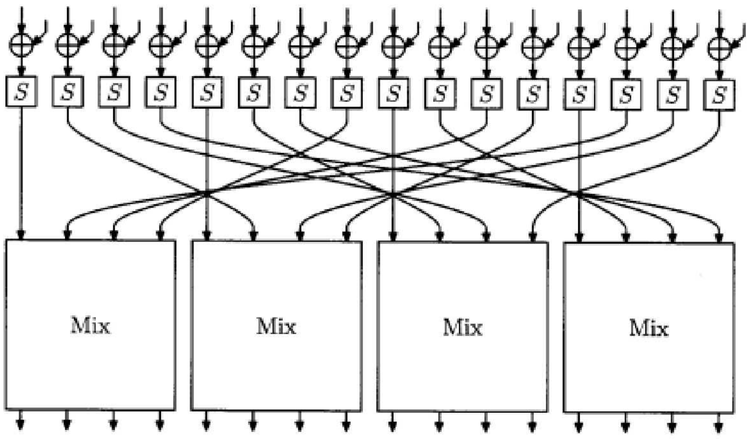

Figure 2: Single round of AES [8].

Asymmetric cryptographic algorithms

Integrity encompasses the accuracy and consistency of data over its intended life cycle. Thus, Eve must not be able to change the data if she manages to intercept it in its transit between Alice and Bob. When working with symmetric algorithms one must ensure that the connection is secure for key handling. Managing several keys at once also becomes an issue when there are numerous recipients. A common solution is implementing public key (asymmetric) encryption.

Asymmetric cryptography can be used for establishment of a shared secret, for encryption and decryption, and for signing and verification. In all these uses, each user has a key pair consisting of a private key and a corresponding public key. The public pieces of the key pairs are distributed by a trusted third party such as a certificate authority.

As seen in Fig. 3, when encrypting a message, Alice encrypts with the public key of the intended receiving party. Bob, who possesses the only private key corresponding to this public key, is the only party able to decrypt the message.

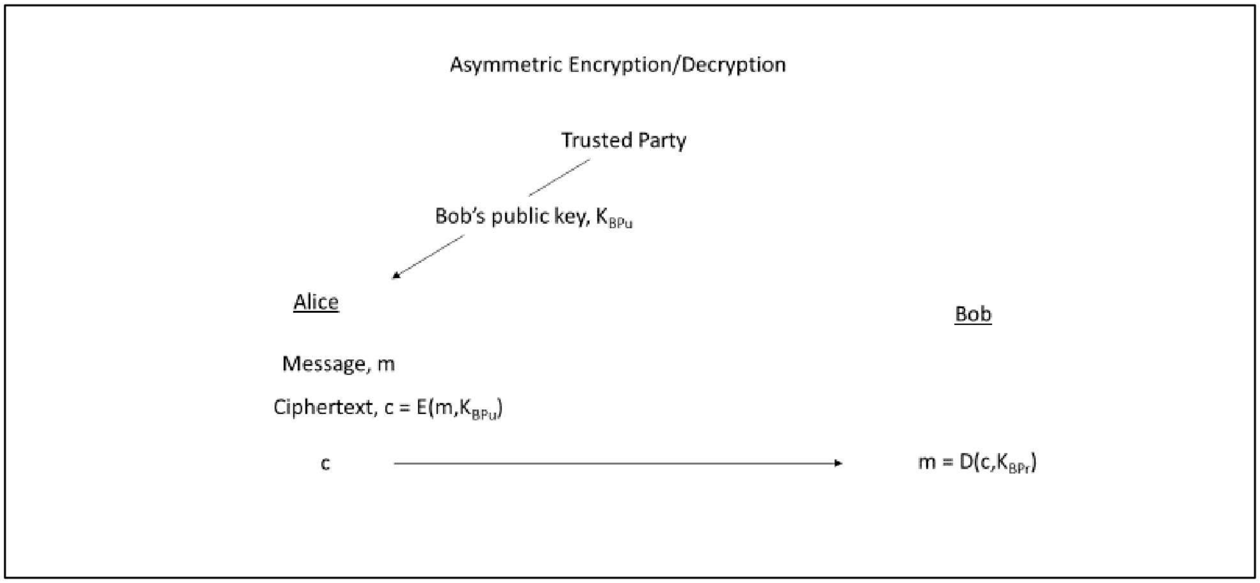
Asymmetric Encryption/Decryption
Trusted Party
Bob's public key, K_{BPu}
Alice
Bob
Message, m
Ciphertext, $c = E(m,K_{BPu})$
c
$m = D(c,K_{BPr})$

Figure 3: Public key encryption

In the signing and verification scenario seen in Fig. 4, Alice uses her private key to encrypt a hash of the message requiring signature. Bob, upon receipt of the message and signature, decrypts the signature using the public key of the sender, hashes the received message and compares the two for signature validation. Only Alice with the private key corresponding to the known public key could have correctly generated the given signature.

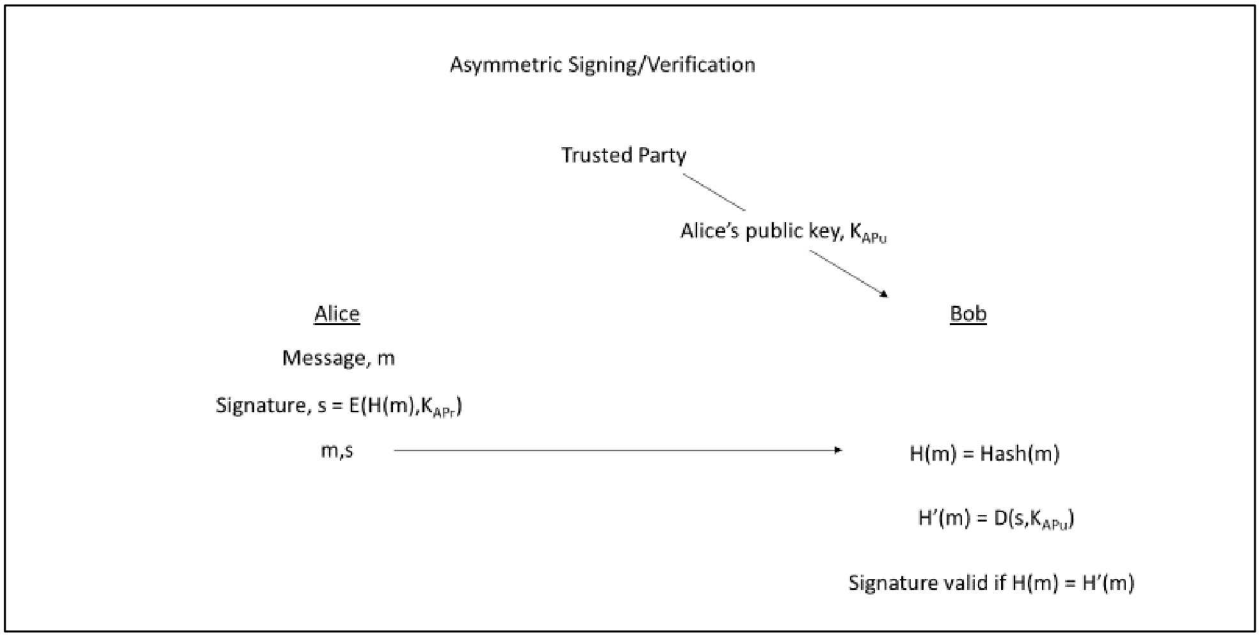
Asymmetric Signing/Verification
Trusted Party
Alice's public key, K_{APu}
Alice
Bob
Message, m
Signature, s = E(H(m),K_{APr})
m,s
H(m) = Hash(m)
H'(m) = D(s,K_{APu})
Signature valid if H(m) = H'(m)

Figure 4: Digital Signatures

RSA is the best-known example of asymmetric cryptography. This algorithm was named after its founders, Rivest-Shamir-Adleman, who publicly announced it in 1978. 1024- or 2048-bit keys are common for RSA and are still widely used today. The algorithm relies on the computational difficulty of integer factorization and is simplified in Fig. 5 as seen below.

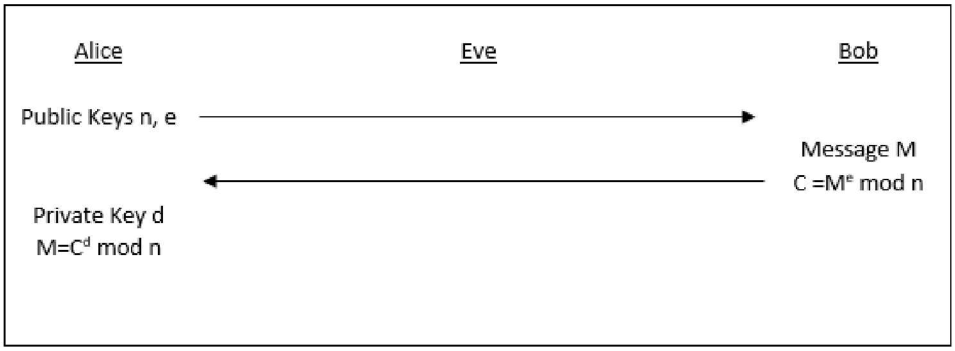

Figure 5: RSA Operation

Alice begins by choosing two large prime numbers p and q. Computers today can determine primes hundreds of digits long. Assuming a 1024-bit key (150 digits) and 1/log(n) probability of primality [9], there would be approximately $2.8*10^{147}$ values to choose from. Alice then multiplies the two values to obtain the product n, which is the first public key sent to Bob. The totient function, $\phi(n)$ is then computed, which yields the number of values coprime with n. Due to $\phi(n)$ being semiprime, this value is (p-1)(q-1). Another value is computed such that $1<e< \phi(n)$ and e is also coprime to $\phi(n)$. This is released as the second public key. Finally, a value, d, is computed such that $de=1+k\,\phi(n)$. This value is kept hidden for decryption. Using the public keys, Bob can encrypt the message using the formula $C=M^e\text{mod}(n)$ and Alice can decrypt using the formula $C^d=m(\text{mod}(n))$. It is important to note that while Eve may obtain the public keys n and e, and encrypted message M, she has no way of interpreting the information she has no way of interpreting the message without the key d.

Elliptic Curve Cryptography (ECC) is another algorithm using one-way functions to perform encryption/decryption and signing/verification operations with asymmetric cryptography. In the case of ECC, the one-way function is the discrete-log problem derived from multiplication of a point on an elliptic curve [10] [13]. Communicating parties agree on a particular curve, E, and a particular base point, P, and obtain each other's public key ahead of time. An example elliptic curve encryption scheme uses the El Gamal cryptosystem [11]. Elliptic Curve Digital Signature Algorithm (ECDSA) is also a commonly used signature/verification scheme; more details are provided in [12].

Bit Security Strength of Keys

As previously stated, 128- or 256-bit keys are common for symmetric encryption, however, longer keys are required for asymmetric to achieve same level of security (e.g., 1024- or 2048-bit for RSA, 256- or 384-bit for ECC). The number of bits of security is an indication of how much work is believed to be required to break a cryptographic algorithm with respect to the type of known attacks against the algorithm. For a discussion of security bit strength of cryptographic algorithms, see NIST Special Publication 800-57 [14].

Key establishment and identity binding methods are required

Symmetric ciphers require a secure method for sharing or generating shared secrets. Diffie–Hellman key exchange was one of the earliest examples of generating a shared secret over public channels. The algorithm uses one-way functions such that an eavesdropper is unable to determine the base secrets of the users. Asymmetric ciphers require distribution of public keys and a public key infrastructure is typically used to certify the identity of each key owner.

Enabling Symmetric Cryptography via Asymmetric Cryptography

Symmetric crypto schemes have the advantage of small key sizes and efficient computations when compared with typical asymmetric crypto schemes. Symmetric schemes, however, provide no method of securely sharing the required symmetric key. The common solution is to utilize the less efficient asymmetric algorithms with their asymmetric public/private key pairs to securely establish a shared symmetric key and then proceed with the more efficient symmetric cryptography.

In order to have confidence that a public key belongs to a given entity prior to using that key for establishing a shared secret, theoretically, the following PKI process is used to register, produce and verify a certificate carrying the entity's public key. The steps are as follows:

1. Entity (e.g. DER) provides proof of identity to Registration Authority (RA)
2. RA requests certificate for entity after authenticating identity

3a. Certificate Authority (CA) binds public/private key pair with identity

3b. CA distributes public portion of certificate to Verification Authority (VA)

4. Entity presents asymmetric-generated signature and public portion of certificate to other party (e.g. Utility)
5. Other party asks Verification Authority (VA) to verify certificate

6. VA responds with revocation status of certificate
7. The other party verifies entity’s asymmetric-generated signature based on verified (non-revoked) certificate

Mutual authentication requires that the other party take the exact same steps to prove its identity to the first entity. After mutual authentication, the communicating parties may establish a shared secret key via methods stated in their certificates and proceed with symmetric key encryption and decryption of their transactions.

4 Implementing Cryptography in DER Systems: Needs and Options

To enable cryptography in DER systems, especially as a distributed module, numerous factors must be considered in addition to key management, certificate authorities, and etc. described in the previous section. From interoperability, including obeying system requirements, to hardware implementation options, these crucial factors must be incorporated in the design of a cryptography module.

Interoperability

For a cryptography module in DER systems, interoperability is an obvious requirement---the module must be able to properly intercept communications and perform encryption and decryption processes. An important standard that details the technical specifications for, and testing of, the interconnection and interoperability between utilities/BPS and DERs is IEEE Std. 1547-2018: “IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces” [15].

The standard details the general requirements, remedial responses, power quality, testing specifications and requirements for design, and also provides production requirements and periodic testing. Therefore, a cryptographic module must abide by these requirements; IEEE 1547 should be consulted during design, testing, and production phases.

System Requirements

An important aspect within interoperability is that the cryptographic module is that the module does not violate any bandwidth, latency, or other critical requirements for DER system operation. An example of typical bandwidth and latency for grid devices is shown in Table 1, derived from [16]. By assessing the impact to bandwidth and latency---the cyber side impacts---the impact to the actual DER system operation, the physical side, can also be studied. We must ensure that the cryptographic module does not disrupt any operations.

	Bandwidth	Latency
Advanced Smart Meters	10 kbps	5 s
Grid Sensor	10 kbps	5 s
Recloser/SCADA devices	10 kbps	100 ms
Capacitor Banks	10 kbps	10 s
DER < 50kW	10 kbps	5 s
EV Charging	10 kbps	10 s

Relevant Protocols

SEP 2.0

The Smart Energy Profile (SEP) 2.0 is a protocol that was designed to replace the ZigBee Pro Smart Energy 1.x and manage energy communications between customer devices and energy service providers. The standard addresses many of the concerns of peak-load management by connecting smart energy devices to the Smart Grid. It operates under the premise of function-sets. These represent a minimum set of device behaviors needed to deliver functionalities such as demand response and load control, metering, and distributed energy resource management [17].

This standard was also designed to enable multiple link layer technologies such as WiFi, Bluetooth, and Ethernet, in addition to encompassing a wide range of bandwidth applications [18]. It has proven advantageous in that it can be used in several conformant products as seen in Kitu Systems, Inc.'s solutions in home energy management, smart appliances, and recently, electric vehicle supply equipment (EVSE). Their products are currently being implemented within California's Rule 21, which concerns the requirements for interconnecting, operating, and metering within several service territories (PG&E, SCE, DG&E) [19]. Due to the increasing penetration of solar, the use of "smart" inverters has been mandated by the program, and therefore features Kitu Convoy™ service platforms [20].

IEC 61850

IEC 61850 concerns the communication protocols for intelligent electronic devices (IEDs) for applications in power utility automation [4]. This standard rose out of a need to integrate technologies such as TCP/IP, high-speed wide area networks (WANs), and switched Ethernet, which were not readily conceived at the time of many early legacy substation designs. Furthermore, the development of the protocol has lent itself to incorporating IEDs that do not directly support its communication standards while leveraging the value of useful IEDs via server IEDs or compliant gateways [21].

DNP3 (IEEE 1815)

DNP3 (IEEE 1815) was created in 1993 by Westronic Inc. out of an effort to eschew having to use several proprietary utility protocols. Using IEEE 60870 as a baseline for research, the design team created the standard with an emphasis on bandwidth conservation and reliability [22]. The specification continues to be updated through the DNP Users Group, which strives to maintain compatibility and interoperability between devices currently and previously adopting the model. Due to its generic nature, this protocol has seen wide adoption outside of traditional power systems and within water, wastewater, transportation, oil and gas industries [23].

SunSpec Common Smart Inverter Profile (CSIP) / CA Rule 21 / IEEE 2030.5

As stated by the California Public Utilities Commission, "Electric Rule 21 is a tariff that describes the interconnection, operating and metering requirements for generation facilities to be connected to a utility's distribution system" [24]. Although only currently mandated in California, DER manufacturers and partners under the SunSpec Alliance have been moving to eventually adopt the recent modifications to Rule 21 as part of the Common Smart Inverter Profile (CSIP). The Rule 21 Smart Inverter process requires certification of all systems directly communicating with the utility, in accordance with IEEE 2030.5 specifications. Under these guidelines, use of security is mandatory between utility servers and clients and is within the utilities' domain of responsibility. The communications protocol implementation must include the following: [25]

- HTTP over TLSv1.2m
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 cipher suite with secp256r1 elliptic curve
- X.508v3 device certificate that chains to the Root-CA
  - SHA256 certificate hash, 160-bit Long-Form Device Identifier (LFDI), 11-digit decimal plus 1-digit checksum Short-Form Device Identifier (SFDI)
- PKI authentication
- LFDI for authorization
- Server ACL

Communications interactions are to be initiated by the client (e.g., DER device, inverter). They include the following:

- Pre-defined polling interval, randomized polling times:
  - Twice every 24h for new commands and curves
  - Once every 48h for inverter performance information
- Scheduling of future events
- Inverter status information

Main Takeaways from CA Rule 21 and SEP 2.0

Although IEEE 2030.5 formalized the SEP 2.0 protocol as a standard and provides guidance for the adoption of the SEP 2.0 protocol, it does not mandate a timeline for implementation in DERs. Rule 21 provides impetus for manufacturers to adopt SEP 2.0 and the associated cryptographic modules. However, the success of the security features is dependent on the establishment of a root Certificate Authority for DER devices, either through the SunSpec Alliance or other trusted third party. Moreover, specific device capabilities must be taken into consideration when deciding how to support cryptographic functions, and integration techniques should be standardized in order to prevent flaws in implementation. The creation of a standalone cryptographic module would help to eliminate unwanted variances in implementation and allow vulnerabilities to be managed separately from DER command and control, and therefore provide increased benefit to grid security as a whole.

Hardware Implementation Options

The need to research and develop a suitable cryptography module is motivated by the lack of existing security devices capable of mitigating the risk of foreseeable threats to DERs, and BPS by extension. While very few vendors offer devices on the market today that utilize cryptography to secure communication, the few that do, like products from Eaton, Siemens, and SEL, lack basic features such as HMACs, checksums, and secure firmware upgrades [26]. Thus, it is significant to consider what a more apt cryptography module would look like, and the different ways such a capability can be physically implemented into DER systems.

A low-cost option with little disruption to existing DER systems, is a **Bolt-On** solution. A Bolt-On implementation suggests a plug and play software solution onto existing legacy systems. However, considering a cryptography application will require additional computing resources, existing DER hardware is unlikely to support a Bolt-On solution.

Another low-cost option is the employment of an **embedded** solution, which introduces new security hardware to existing hardware in a DER system. Such an implementation is being utilized in other industries, leading to the development of a Trusted Platform Module (TPM) standard [27]. TPM forms a standard for secure embeddable cryptoprocessors that involve desired security features, as seen in Fig. 10 below.

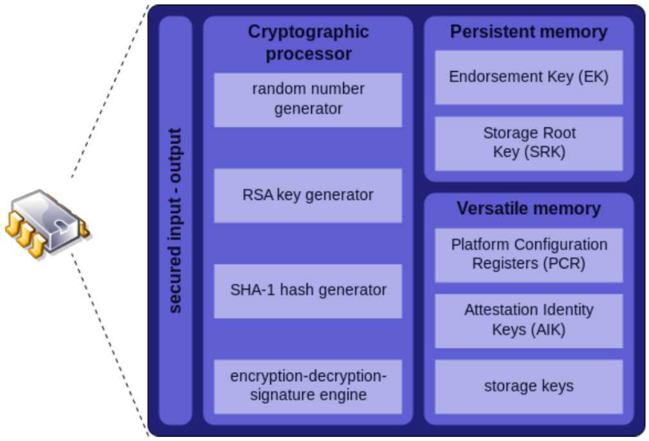

Figure 10: TPM security features [27].

However, while TPM embedded solutions are used in typical computing devices, such as servers and desktops, which are designed to provide expandability, no such expandability likely exists in legacy DER hardware. In addition, embedded solutions would require a high-level of customization for each variation of DER hardware.

A final hardware implementation option is **Bump-in-the-Wire** (BITW). BITW implementations insert devices into the communication lines of existing systems such that no legacy DER hardware needs to be manipulated. Fig. 11 below illustrates a system that is updated with BITW devices to enable encryption and decryption.

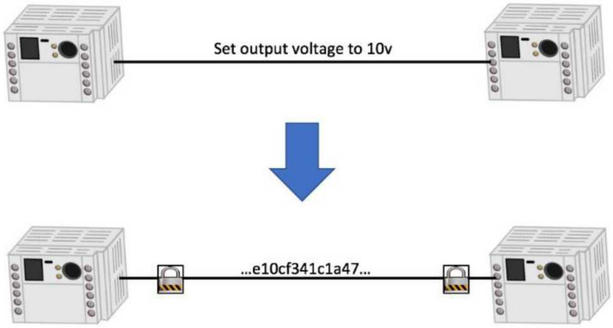

Figure 11: Example of BITW implementation of cryptography module.

The primary disadvantage of BITW implementations is the increase of latency in system communication due to the additional devices' processing time. However, careful design of the BITW device can render increase in latency to the overall DER communication system negligible. Furthermore, a BITW device will feature carefully selected hardware that complements cryptography and security needs, unlike existing

DER hardware. A BITW hardware implementation seems most appropriate for the research and development of a cryptography module for DER systems.

5 Practical Considerations for Cryptography in DER Systems

Beyond the implementation needs and options, as presented in the prior section, there are many practical considerations that must be addressed. This section will detail reliability, timing needs, and anti-tamper techniques that are crucial concepts that need to be considered when deploying a cryptographic module in DER systems.

Reliability

Although DER are not taken into account in traditional (eg. N-1-1) reliability calculations for bulk generation, rapid and consistent growth in DERs has already change how grid operators sustain system reliability. DER devices and technologies not only impact distributed generation, but also demand response, load, and transmission. [28] However, the data required to characterize and create requirements specific to the DER space is currently lacking [29]. We do know that the proliferation of smart devices is driving the electricity grid to have faster, sub-second response times that are beyond the capabilities of a human operator, and that timing discrepancies can have a severe impact on the operation of advanced grid components. Meanwhile, these smart grid devices are also passing increasingly large quantities of data across the network, often using unprotected, best-effort multicast techniques that prioritize reliability over security. Since one of the primary concerns with implementing encryption on a communications system is increased latency and potential data loss, timing requirements are crucial to these efforts.

Timing

Time accuracy and synchronization requirements vary widely over sections of the power grid and are dependent on the types of communications or actions being performed, including those operating over wide-area networks and wireless networks. For example, sampling of values for frequency event detection requires sub-microsecond time accuracy, whereas DER performance information can be polled with and millisecond time accuracy and latency. Table 1 below shows some typical time precision values for grid applications [30] [31].

Table 1: Time accuracy requirements for various grid applications

Application	Time Accuracy (s)
Clock	10^{-8}
Traveling Wave Fault Detection and Location	10^{-7}
Global Positioning System (GPS) Timestamping	10^{-6}
Synchrometrology (synchrophasors)	10^{-6}
Wide Area Protection	10^{-6}
Frequency Event Detection	10^{-6}
Anti-Islanding	10^{-6}
Droop Control	10^{-6}
Wide Area Power Oscillation Damping (WAPOD)	10^{-6}
Substation Local Area Networks (IEC 61850 Sample Values)	10^{-6}

Line Differential Relays	10^{-5}
Instrument Sampling	10^{-5}
Sequence of Events Recording	10^{-4}
Digital Fault Recording	10^{-3}
Substation Local Area Networks (IEC 61850 GOOSE)	10^{-3}
Phasor Measurement Reporting	10^{-2}
SCADA Measurements	10^{-1}

Anti-tamper Techniques

The final design for the Module-OT must have anti-tamper protection provided. These protections can take many forms and will be highly dependent upon the design of the device itself. In fact, many of the anti-tamper protections must be part of the module design from the beginning. Depending upon the overall architecture of the device, including memory, integrated circuits, data storage, and others, many techniques may be necessary [32].

Additionally, one should consider tamper prevention, tamper detection, tamper response, and tamper evidence techniques as part of the overall anti-tamper design. Since no security measures can ever truly defeat any/all attackers, having the ability to detect that an item has been tampered with is crucial. From there many responses should be available and in some cases automated for things like zeroization of the cryptographic system.

Many hardware related anti-tamper techniques exist such as making the enclosure difficult to open, applying coatings, specialized switches and circuitry. However, hardware attacks are not the only avenue of attack. Networking and software attacks are also used. Standard protections should be applied to ensure the network protocol stack is minimal and contains only protocols that are necessary to the function of the system. Also, anti-tamper software should be in place to cover things like updating of software/firmware load of any component in the system.

The National Institute for Standards and Technology (NIST) also has a set of recommended controls to include in Federal Information Systems [14]. Some of the relevant controls are provided in the highlighted text below (from [14]). These controls are high-level requirements that should be considered exemplary to what is needed for the Module OT system.

NIST Special Publication 800-53 (Rev. 4) [14]

Security Controls and Assessment Procedures for Federal Information Systems and Organizations

Control SA-18: Tamper Resistance and Detection

Control Description

The organization implements a tamper protection program for the information system, system component, or information system service.

Supplemental Guidance

Anti-tamper technologies and techniques provide a level of protection for critical information systems, system components, and information technology products against a number of related threats including modification, reverse engineering, and substitution. Strong identification combined with tamper resistance and/or tamper detection is essential to protecting information systems, components, and products during distribution and when in use.

Related to: PE-3, SA-12, SI-7

Control Enhancements

SA-18(1) TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SDLC

The organization employs anti-tamper technologies and techniques during multiple phases in the system development life cycle including design, development, integration, operations, and maintenance.

Supplemental Guidance: Organizations use a combination of hardware and software techniques for tamper resistance and detection. Organizations employ obfuscation and self-checking, for example, to make reverse engineering and modifications more difficult, time-consuming, and expensive for adversaries. Customization of information systems and system components can make substitutions easier to detect and therefore limit damage.

Related to: SA-3

SA-18(2) TAMPER RESISTANCE AND DETECTION | INSPECTION OF INFORMATION SYSTEMS, COMPONENTS, OR DEVICES

The organization inspects [Assignment: organization-defined information systems, system components, or devices] [Selection (one or more): at random; at [Assignment: organization-defined frequency], upon [Assignment: organization-defined indications of need for inspection]] to detect tampering.

Supplemental Guidance: This control enhancement addresses both physical and logical tampering and is typically applied to mobile devices, notebook computers, or other system components taken out of organization-controlled areas. Indications of need for inspection include, for example, when individuals return from travel to high-risk locations.

Related to: SI-4

6 Conclusions

This document seeks to provide a basis for designing and implementing a cryptographic module for securing DER systems. DER system composition and security needs were discussed; the need for cryptography was examined and motivated. Cryptography basics, including algorithm and implementation, was provided. Next, specific module implementation options and needs were described, from interoperability to hardware. Finally, for actual deployment, some practical considerations such as anti-tamper techniques were discussed.

These requirements are general and a starting point for designing a suitable cryptographic module. Further research will build on these concepts to realize a secure, flexible distributed cryptography module design and implementation.

References

[1] The Smart Grid Interoperability Panel-Smart Grid Cyber Security Committee, "NISTIR 7628 Rev. 1: Guidelines for Smart G Cybersecurity," National Institute of Standards and Technology, 2014.

[2] F. C. a. A. Lee, "Cyber Security for DER Systems," Electric Power and Research Institute, 2013.

[3] North American Electric Reliability Corporation, "Critical Infrastructure Protection Standards," [Online]. Available: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx. [Accessed June 2018].

[4] "IEC/IEEE International Standard - Communcation networks and systems for power utility automation," IEC/IEEE 61850, 2016.

[5] "Perfect Secrecy of the one-time pad," Univeristy of Maryland, Maryland.

[6] W. Stallings, "The RC4 Stream Encryption Algorithm," Cryptography and Network Security, 2005.

[7] N. S. Agency, "CNSS Policy No. 15, Fact Sheet No. 1 National Policy on the Use of the Advanced Encryption Standard (AES Protect National Security Systems and National Security Information," 2003.

[8] B. S. N. Fergusen, in *Practical Cryptography*, Wiley Publishing, 2003, p. 55.

[9] H. Riesel, "Progress in Mathematics Vol, 126," in *Prime numbers and computer methods for factorization*, Birkhäuser Bos 1994.

[10] M. Musson, "Attacking the Elliptic Curve Discrete Logarithm Problem," Acadia University, 2006.

[11] "Elliptic Curve ElGamal Cryptosystem," [Online]. Available: https://www.youtube.com/watch?v=6bGxLE9rIAY. [Accessed June 2018].

[12] "Elliptic Curve Digital Signature Algorithm," [Online]. Available: https://en.wikipedia.org/wiki/Elliptic_Curve_Digital_Signature_Algorithm. [Accessed June 2018].

[13] H. Knutson, "What is the math behind elliptic curve cryptography?," [Online]. Available: https://hackernoon.com/what-i the-math-behind-elliptic-curve-cryptography-f61b25253da3. [Accessed June 2018].

[14] National Institute of Standards and Technology, "NIST Special Publication 800-53 (Rev. 4)," [Online]. Available: https://nvd.nist.gov/800-53/Rev4/control/SA-18..

[15] 1. R. W. Group, "IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces," IEEE Standards Association, 2018.

[16] U.S. Department of Energy Office of Electricity Delivery and Energy Reliability, "Modern Distribution Grid Decision Guide Volume III," DOE, 2017.

[17] "IEEE Adoption of Smart Energy Profile 2.0 Applciation Protocol Standard," IEEE Std. 2030.5, 2003.

[18] F. Sioshansi, "Innovation and disruption at the grids edge how distributed energy resources are disrupting the utility business model," Academic Press, Amsterdam, 2017.

[19] C. S. I. I. W. Group, "IEEE 2030.5 Common California IOU Rule 21 Implementation Guide for Smart Inverters, Version 1.0, 2017.

[20] G. Lum, "Kitu Systems Background IEEE 2030.5 Revision 2 Status CSIP Implementation Guide Status," 2017.

[21] D. Dolezilek, "IEC 61850: What You Need to Know About Functionality and Practical Implentation," Schweitzer Engineeri Laboratories, Inc., 2010.

[22] "IEEE Standard for Electrical Power Systems Communications-Distributed Network Protocol (DNP3)," IEEE Std.1815-2012 (Revision of IEEE Std. 1815-2010), 2012.

[23] D. U. Group, "A DNP3 Protocol Primer," 2005. [Online]. Available: https://www.dnp.org/AboutUs/DNP3%20Primer%20Rev%20A.pdf. [Accessed 27 June 2018].

[24] California Public Utilities Commission, "Rule 21 Interconnection," July 2017. [Online]. Available: http://www.cpuc.ca.gov/Rule21/.

[25] Common Smart Inverter Profile Working Group, "Common Smart Inverter Profile - IEEE 2030.5 Implementation Guide fo Smart Inverters," March 2018. [Online]. Available: https://sunspec.org/wp-content/uploads/2018/03/CSIPImplementationGuidev2.003-02-2018-1.pdf.

[26] National Renewable Energy Laboratory, "DRAFT Module OT Research White Paper," 2018.

[27] TCG, "TPM Main Part 1 Design Principles," Trusted Computing Group, Inc., 2011.

[28] U.S. Department of Energy (DOE), "The Quadrennial Energy Review (QER) 1.2," January 2017. [Online]. Available: https://www.energy.gov/sites/prod/files/2017/02/f34/Quadrennial%20Energy%20Review--Second%20Installment%20%28Full%20Report%29.pdf.

[29] Federal Energy Regulatory Commission (FERC), "Distributed Energy Resources - Technical Considerations for the Bulk Po System," February 2018. [Online]. Available: https://www.ferc.gov/legal/staff-reports/2018/der-report.pdf.

[30] North American Synchrophasor Initiative (NASPI) Time Synchronization Task Force, "Time Synchronization in the Electric Power System," March 2017. [Online]. Available: https://www.naspi.org/sites/default/files/reference_documents/tstf_electric_power_system_report_pnnl_26331_marc 017_0.pdf.

[31] National Institute of Standards and Technology (NIST), "Timing Challenges in the Smart Grid," January 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-08.pdf.

[32] E. Dubrova, "Anti-Tamper Techniques," Royal Institute of Technology, Stockholm.

[33] International Electrotechnical Council, "Part 12: Resileince and security recommendations for power systems with distributed energy resources (DER) cyber-physical systems," IEC, 2016.

[34] NIST, "Recommendation for Key," 2012. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-57p1r3.pdf. [Accessed 2018 June].