SANDIA REPORT
SAND2023-09882
Printed October 2023

Sandia National Laboratories

Advanced Reactor Control Systems Authentication Methods and Recommendations

Benjamin Karch, Romuald Valme, Minami Tanaka, Christopher Lamb

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

In the dynamic landscape of Operational Technology (OT), and specifically the emerging landscape for Advanced Reactors, the establishment of trust between digital assets emerges as a challenge for cybersecurity modernization. This report reviews existing approaches to authentication in Enterprise environments, and proposed methods for authentication in OT, and analyzes each for its applicability to future Advanced Reactor digital networks. Principles of authentication ranging from underlying cryptographic mechanisms to trust authorities are evaluated through the lens of OT. These facets emphasize the importance of mutual authentication in real-time environments, enabling a paradigm shift from the current approach of strong boundaries to a more malleable network that allows for flexible operation. This work finds that there is a need for evaluation and decision making by industry stakeholders, but current technologies and approaches can be adapted to fit needs and risk tolerances.

ACKNOWLEDGEMENTS

This research was funded by the U.S. Department of Energy Office of Nuclear Energy Cybersecurity research and development program under milestone M3CT-23SN1104045.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

This page left blank

EXECUTIVE SUMMARY

Advanced Reactor (AR) control systems will require robust and reliable authentication mechanisms to ensure the security of energy infrastructure and the identity of digital assets within their digital environment. Our team provides a comprehensive review of various existing approaches and proposals across industries for their applicability to ARs. Many existing approaches today for authentication can be found through Enterprise networks. Our team describes these systems and analyzes them for their many qualities as well as potential vulnerabilities. Often protocols can extend into Operational Technology (OT) environments through modification. This report highlights such occurrences and the changes that must occur. In machine-to-machine (M2M) authentication both sides of communication are user-less, which is the main deviation from traditional authentication methods. Various protocols and procedures are discussed that can verify digital asset identities regardless of this differentiation.

Contemporary industrial control systems have complex networks with various endpoints. This report discusses recommendations for securing such networks with authentication. The team incorporates various features from research on existing and future technologies. The Key Distribution Center (KDC) and Authentication Server (AS) are shown to prevent attempted impersonations and provide privacy for messages and content being shared. Certificates and digital signatures are capable of being used in novel ways with Blockchain technology for redundancy and to ensure mutual authentication. The potential benefits of using these technologies are communicated in depth to provide the reader with a full understanding of what is available with existing techniques.

A thorough analysis of cryptographic processes is necessary to understand the performance of these facilities. Cryptography underlies all authentication procedures and the algorithms available each have unique qualities. These techniques have differing resource needs from hardware devices. Hardware devices exist in constrained environments where their timing requirements are strict. However, over time these hardware devices have become more capable of running difficult operations due to advances in technology. This has given rise to new opportunities, allowing engineers and developers to create innovative security applications.

In conclusion, this report finds that the use of asymmetric cryptography and Public Key Infrastructure (PKI) based approaches to authentication offer advantages that are well-poised for AR digital networks, an approach that deviates from many widely adopted authentication protocols used in Enterprise networks. Additionally, it is recommended to incorporate a ticketing system that allows for authentication to be tracked and audited within the AR network, ensuring that digital assets do not maintain authenticated communication sessions for lengths of time or amounts of data that creates an ad-hoc reversion to an inherent trust model by lack of reauthentication. Finally, because blockchain distributed ledgers provide an opportunity to include information that is not confidential, but still important to authentication (e.g., public keys, digital certificates), in a distributed and integrity-controlled manner, it is recommended that this be included in an authentication paradigm for ARs.

ACRONYMS AND TERMS

Acronym/Term	Definition
3GPP	3rd Generation Partner Project
AAS	Authentication and Authorization Service
AKA	Authentication and Key Agreement
API	Application Programming Interface
AR	Advanced Reactors
AS	Authentication Server
ASCON	Automatic Switched Communications Network
AUTN	Authentication Token
AV	Authentication Vectors
AWS	Amazon Web Services
CA	Certificate Authority
CLI	Command Line Interface
CON	Data Concentrators
CPU	Central Processing Unit
DT	Digital Twins
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
EMS	Energy Management System
ESMIG	European Smart Metering Industry Group
HAN	Home Area Network
HSS	Home Subscriber Server
IAEA NSS	International Atomic Energy Agency Nuclear Security Series
ICS	Industrial Control Systems
ID	Identification
IDE	Integrated Development Environment
IdP	Identity Provider
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IT	Information Technology
JWT	JSON Web Token
K	Encryption Key
KDC	Key Distribution Center
KGC	Key Generation Center

Acronym/Term	Definition
LTE	Long-Term Evolution
M2M	Machine-to-Machine
MAC	Message Authentication Code
MFA	Multi-Factor Authentication
MID	Machine Identity
MIT	Massachusetts Institute of Technology
MITM	Man-in-the-Middle
ML	Machine Learning
MSP	M2M Service Provider
NAN	Neighborhood Area Network
NIST SP	National Institute of Standards and Technology Special Publications
NPP	Nuclear Power Plant
OAuth	Open Authorization
ODIC	OpenID Connect
OT	Operational Technology
OTP	One-Time Password
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PSK	Predefined Pre-Shared Key
PUF	Physically Unclonable Functions
RSA	Rivest-Shamir-Adleman
SAML	Security Assertion Markup Language
SCADA	Supervisory Control and Data Acquisition
SIM	Subscriber Identification Module
SMR	Small Modular Reactors
SP	Service Provider
SPN	Service Principal Name
SQN	Sequence Number
STS	Security Token Service
TCP	Transmission Control Protocol
TGS	Ticket Granting Server
TGT	Ticket Granting Ticket
TLS	Transport Layer Security
TPM	Trusted Platform Module
TTL	Time to Live

Acronym/Term	Definition
UE	User Equipment
WAN	Wide Area Network
XMAC	Expected Message Authentication Code
XRES	Expected Response Value
ZTA	Zero Trust Architecture

This page left blank

1. INTRODUCTION

In today's rapidly advancing digital landscape, the integration of digital devices within Industrial Control Systems (ICS) and Operational Technology (OT) environments is unavoidable and presents opportunities for significant economic advantages and increased autonomy. Communications between and coordination among these devices is an important part of efficiently operating the next generation of nuclear power generation. However, this increase in communications and use of digital devices presents challenges to maintaining safe practices as potential threats to security shift from purely physical into this digital landscape. Critical infrastructure applications have become a high value target for cyber-attacks because of the potential for severe physical consequences (e.g., BlackEnergy [1]. Whether cyber-attacks are aimed at producing a physical impact or are extortionary in nature, it is critical that the services provided by OT environments be resilient enough to prevent attack or at least maintain operations.

A core foundation of secure and reliable communication in all digital networks is the authentication of devices. Authentication in digital systems refers to the process of "verifying the identity of a user, process, or device," [2]. Traditionally, OT environments have relied on a paradigm of trust, where a well-defined boundary protects the internal network from external threats. Data should not cross this boundary, and therefore a secure posture is assumed of all devices that have been installed within the boundary. These strict boundaries are described, for example, in IAEA NSS 27-G [3], and shown in Figure 1.

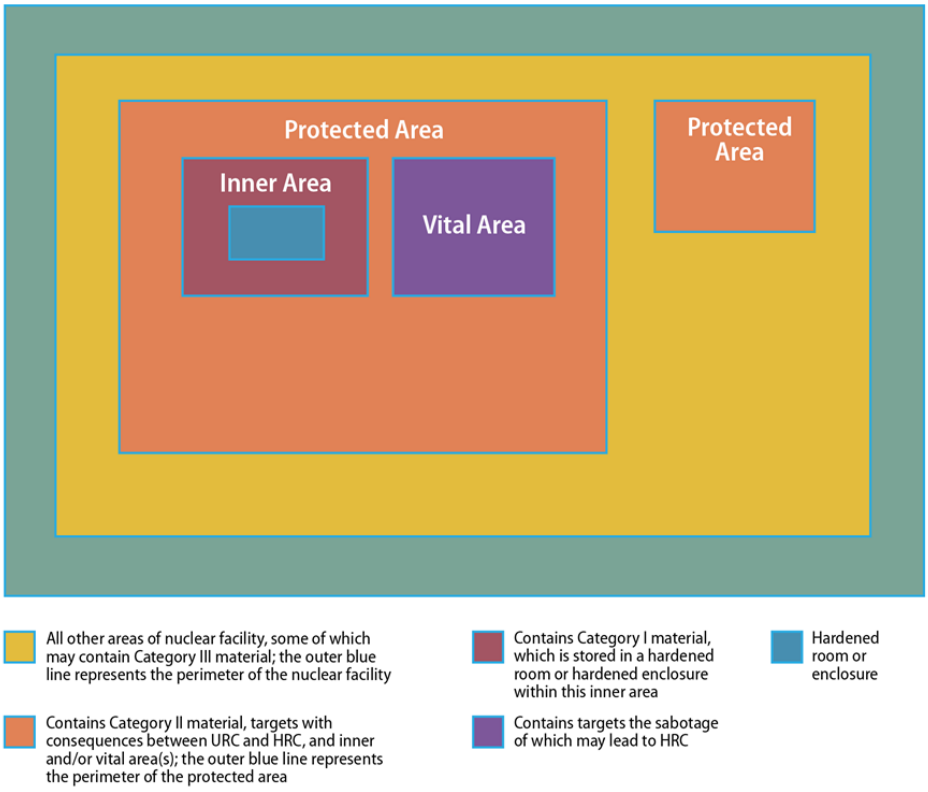

Figure 1. IAEA NSS 27-G boundaries [3]

Recent industry trends in Advanced Reactors (ARs) and Small Modular Reactors (SMRs) require that these strict boundaries become more malleable to enable remote monitoring, operation, and

wireless technology implementations. An example use case where these strict boundaries may restrict advancements in ARs is the use of wireless technologies, which AR vendors have expressed heavy interest in to aid in reduced costs for wiring. Wireless technologies inherently remove strict physical boundaries, leading to an increased need to autonomous authentication of digital assets within the plant, as communications cannot be verified to be within the same physical location. Additionally, the White House has released cybersecurity priorities [4] for which the migration from these traditional network architectures toward Zero Trust Architectures (ZTA) has been heavily emphasized. Modern approaches to network designs that are traditionally pioneered by Enterprise environments require the adoption of modern cybersecurity protections, including the authentication and verification of devices and data within a network.

This report places a strong emphasis on authentication mechanisms and protocols that currently exist within IT / Enterprise systems. Because there currently does not exist an authentication protocol specifically tailored for NPP digital networks or even OT environments, a review of existing IT methodologies is prudent to gain a contextual understanding of the state of the art of digital authentication and the subcomponents of these methodologies that would be appropriate or inappropriate for inclusion within an AR digital network.

2. BACKGROUND

Over the years, cyber-attacks on critical infrastructure have increased in both prevalence and sophistication, posing significant risks to critical infrastructure and national security if network boundaries are removed without the addition of strong cybersecurity controls. The current approach of existing fleet Nuclear Power Plant (NPPs) of an "airgap," where ICS networks are isolated from external connections, is perceived as a safeguard against cyber-attacks. However, requirements of AR and SMR vendors have rendered the personnel and lack of remote capabilities an economic challenge.

In the Information Technology (IT) realm, authentication methods have evolved primarily to fill the function of verifying a user identity before the user is given access to a machine or resource. However, the use cases and needs of IT and OT are fundamentally different. OT systems operate around the clock and generally without a user present, given that the objective of these devices is to automate a process. Thus, traditional authentication methods, like passwords or biometric identification, are neither feasible nor appropriate for authentication of devices within an AR.

To address these challenges, this report reviews current accepted approaches to authentication in IT and proposed authentication paradigms specific to OT. Based on the review and analysis of these approaches, this report offers recommendations for a future standardized method by which digital devices within ARs can mutually authenticate. These recommendations aim to establish an autonomous and trustworthy communication framework that allows for flexible network structure while minimizing security requirements that might otherwise impede data transfer and utilization within the AR network or its potential connection to the internet.

As the need for interconnected and automated NPPs continues to grow, it is imperative to develop and implement robust machine-to-machine (M2M) authentication methodologies that not only provide cybersecurity protections but allow for innovation in NPP design and maintenance. Robust and secure future generations of NPPs present an opportunity for safe and green energy production and combatting climate change.

This page left blank

3. EXISTING APPROACHES

3.1. Enterprise Protocols

For modern Enterprise environments, authentication stands as a foundational aspect ensuring the security and integrity of data, services, and digital assets. These Enterprises have served as a pioneering force in the development and adoption of authentication methodologies, with a primary focus on verifying the identities of users and systems within their networks. These inherent demands for authentication have given rise to well established practices and standardized protocols that form the basis of secure communications within IT networks.

The motivation for establishing these authentication mechanisms has typically stemmed from the need for a business entity to protect its financial posture. For example, the network of an Enterprise must ensure that only authorized users can access important business information and intellectual property. Additionally, businesses that provide a service over a digital network must ensure that the service can only be accessed and leveraged by users who are verified to be paying customers. As a response to these needs, a variety of authentication methods have been developed, tested, and subsequently refined, many catering to specific use cases and diverse security requirements.

While many of the authentication protocols used find their roots in the need to establish a confidential communications channel, they provide the potential to be applied as an authentication method as well. For example, Transport Layer Security (TLS) serves the main purpose of protecting information in transit between two digital assets (a client and server) on the Transmission Control Protocol/Internet Protocol (TCP/IP) stack. However, TLS offers a robust authentication procedure that can be disabled, one-way, or mutual for authentication using digital certificates.

The prevalence and level of standardization for authentication methods within traditional IT environments mean that they are a highly useful benchmark for comparing and developing against for an OT authentication procedure. However, some additional considerations must be made when evaluating the applicability of IT authentication methods for OT. As mentioned previously, the use case for these methods usually involves at least one system with a human in the loop. This assumption is not applicable to OT systems. Additionally, the protocols are often highly intertwined or reliant on the TCP/IP stack, limiting their adaptability to different networking layers. A robust authentication framework for OT environments would ideally be agnostic of the underlying OSI model networking layers, to allow for interoperability of devices that may be implemented using a variety of networking paradigms and communication protocols.

This section provides a comprehensive review of commonplace authentication mechanisms commonly implemented in Enterprise/IT networks. These protocols are reviewed and analyzed for the applicability within an OT network. Using insights from well-established industry standard authentication methods allows for informed decisions when making recommendations or designing future methods for authentication within and between OT environments.

3.1.1. Kerberos

Kerberos is an authentication system created by Massachusetts Institute of Technology (MIT). It is used in many enterprise products such as Google Cloud and Microsoft Active Directory to ensure proper access rights and security. It typically uses symmetric key cryptography. Through Kerberos, services are free from having to maintain their own user account records by utilizing a service whose sole purpose is to authenticate. Both user and service must implicitly trust the Kerberos Authentication Server (AS) [5]. The user and the service must also have a shared secret key

registered with the AS. These keys are typically called long-term keys. They have a predetermined time to live (TTL) of about a few weeks or months.

The start of a Kerberos session begins when a client needs to request an item or resource from a server. As seen in Figure 2the client sends its User ID and requested service, which prompts a response from the AS. The AS sends an encrypted Ticket Granting ticket (TGT) and session key to the client. This is encrypted with the client's password. The client then sends the TGT and session key to the Ticket Granting Server (TGS), which responds once validated with a service ticket and session key. The client then uses the service ticket and session key to authenticate to the server and obtain the requested resource, as shown in Figure 2. Kerberos architecture.

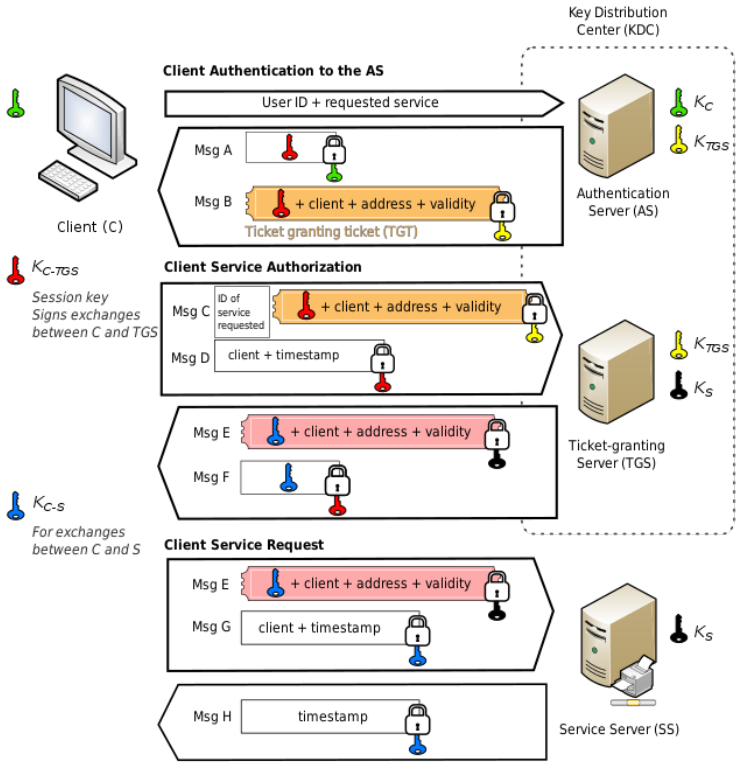

Figure 2. Kerberos architecture [6]

The Key Distribution Center (KDC) as seen in Figure 2is the combination of the TGS and the AS. The TGS is used to add an extra layer of indirection so that the user only needs to enter a password once. Before accessing any regular service, the user requests a ticket from the AS to talk with the TGS. When requesting a new service, the client does not have to reauthenticate with the AS. It can simply use the TGT it has to go through the process. The client's password is only used when authenticating to the AS, preventing potential Man-in-the-Middle (MITM) attempts to steal the password.

In Kerberos, a client can send two types of requests to the KDC. These two requests are to the AS and TGS. If authorized, these requests grant the user tickets. The AS grants a user an initial TGT by which they can authenticate to the TGS to grant service tickets [5]. In a typical Kerberos implementation, the TGT has a longer duration compared to service tickets. The duration of Kerberos tickets is typically expressed in seconds and can vary depending on the security requirements and policies of the organization. Commonly the default duration for a TGT is 10

hours (36,000 seconds), while service tickets have a shorter duration around 8 hours (28,800 seconds). These values, however, are not fixed and can be adjusted by the KDC administrator. Before ticket expiration, a user can also issue a renewal request for a ticket.

There are three main keys that are used within Kerberos. The long-term key of the service K_s, the TGS's key K_{TGS} and the reply-encrypting key, which is the long-term key of the client K_C as seen in Figure 2 . Each of these keys is of a particular encryption type (enctype). Each request made allows the client to provide a list of enctypes that the server is willing to accept. The supported enctypes can be seen in Table 1. The variety of enctypes provide developers with a wide range of options when implementing advanced reactors. There are also two session keys that are for signing exchanges between the client and TGS and the client and service server.

Table 1 - Kerberos supported encryptions [7]

Encryption Type	Description
des3-cbc-raw	Triple DES cbc mode raw (weak)
des3-cbc-sha1 des3-hmac-sha1 des3-cbc-sha1-kd	Triple DES cbc mode with HMAC/sha1 (deprecated)
aes256-cts-hmac-sha1-96 aes256-cts aes256-sha1	AES-256 CTS mode with 96-bit SHA-1 HMAC
aes128-cts-hmac-sha1-96 aes128-cts aes128-sha1	AES-128 CTS mode with 96-bit SHA-1 HMAC
aes256-cts-hmac-sha384-192 aes256-sha2	AES-256 CTS mode with 192-bit SHA-384 HMAC
aes128-cts-hmac-sha256-128 aes128-sha2	AES-128 CTS mode with 128-bit SHA-256 HMAC
arcfour-hmac rc4-hmac arcfour-hmac-md5	RC4 with HMAC/MD5 (deprecated)
arcfour-hmac-exp rc4-hmac-exp arcfour-hmac-md5-exp	Exportable RC4 with HMAC/MD5 (weak)
camellia256-cts-cmac camellia256-cts	Camellia-256 CTS mode with CMAC
camellia128-cts-cmac camellia128-cts	Camellia-128 CTS mode with CMAC
des3	The triple DES family: des3-cbc-sha1
aes	The AES family: aes256-cts-hmac-sha1-96, aes128-cts-hmac-sha1-96, aes256-cts-hmac-sha384-192, and aes128-cts-hmac-sha256-128
rc4	The RC4 family: arcfour-hmac
camellia	The Camellia family: camellia256-cts-cmac and camellia128-cts-cmac

Some benefits of Kerberos are:

- **Mutual authentication**: Both the service provider (SP) and the client must be authenticated This mutual authentication creates an extra layer of security.

- **Single Sign-on**: Eliminates the use of passwords for services, removing the problem of multiple services having the same password, which makes the system more secure and the lives of users easier [8].
- **Widely Supported**: Kerberos has been adopted by all major operating systems and is well known as an industry standard.
- **Ticketing System:** Limited time period is applied to tickets. The ticket's validity in the system expires once time is up. Tickets have a strong authentication process, which prevents stolen tickets from being used.
- **Password Management**: Passwords are never sent over the network unencrypted, mitigating the risk of eavesdropping/MITM.

Kerberoasting is a technique by which an adversary can gain access to the password of service accounts. It mainly involves exploiting low-complexity passwords and an architecture flaw that allows any authenticated domain user to start a TGS request for any service on the network. To perform Kerberoasting an adversary must have access to an authenticated user account. An attacker first enumerates the active directory to identify service accounts and their associated service principal name (SPNs). This SPN is used to craft a message to the TGS. Using the SPN of the service and user account an adversary can communicate with the TGS and receive a TGT for the service. Once obtained, an attacker then extracts the encrypted service account hash and attempts to brute force the hash offline using common tools like Hashcat or JohnTheRipper [9].

Kerberoasting does have a few drawbacks, however. For one the technique requires an adversary to have already compromised a user account. This typically can be achieved through methods such as social engineering. Host-based SPNs are also invulnerable to Kerberoasting attacks because of their long and intricate keys. These keys are also changed roughly every 30 days.

Often a system may be misconfigured to not mandate pre-authentication. Without this configuration settings any attacker on the network can query the KDC for a TGT. For this attack an adversary must first obtain a list of users that have pre-authentication disabled if any. They can then utilize the user's info to query the TGS for a TGT.

If at any time an adversary acquires a valid ticket, they can use it as an alternative means of authentication. This can be used to authenticate to a service or the TGS. They would be gaining access in spite of the intended user credentials and authentication process. This form of attack is called Pass The Ticket. Tickets that grant access to services are typically silver tickets and those to the TGS are gold tickets as they may be used to generate tickets to multiple services [10].

In 2021, a system was proposed using Kerberos in ICSs. This system provides these ICS environments with a robust security model. The Siemens S7 protocol was used as a template and was upgraded to support cryptographic and secure procedures. The upgrades involve incorporating Kerberos' ticket-based system to support the exchange of permissions and keys [11]. This allows for all services and processes to now incorporate a level of confidentiality and integrity. As seen in Figure 3 the authentication takes place between the ICS clients and Programmable Logic Controller (PLCs). An ICS client now needs to authenticate to a central Authentication and Authorization Service (AAS) to obtain a client and server ticket. The client ticket contains the necessary information to access a PLC, and the server contains the same for the PLC. Each endpoint serves as a policy enforcer for the other. Through this ticket, the client is granted access to the PLCs data and information. In K7, tickets are used to send session security attributes. These attributes include but are not limited to session keys, cryptographic primitives, and permissions.

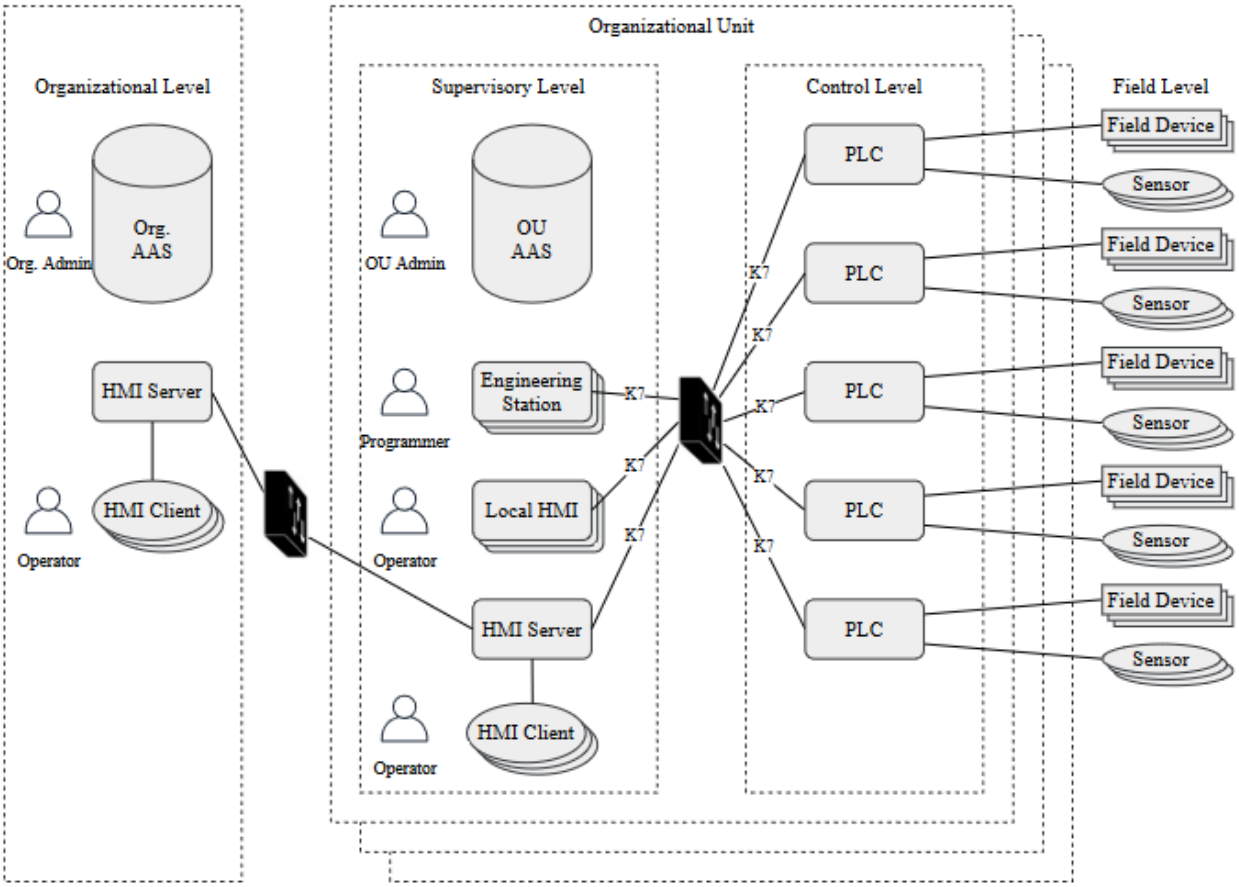

Figure 3. K7 ICS topology [11]

During installation each device in the system registers a long-term symmetric or public key with the AAS. The access permissions of each device are also set in the AAS by a security administrator. PLCs may need to undergo device augmentation attaching a converter that translates the K7 protocol to the legacy S7 protocol and vice versa. As a result of this upgrade, ICS environments receive many benefits. Some of these benefits are outlined in Figure 4. Though the benefits are many, this kind of system is still potentially vulnerable to a supply chain attack, where an adversary infiltrates the installation process of some device and gains access to or modifies the key being exchanged with the AAS.

Requirement\Protocol	S7	IPSec	K7
Unique Identity	✗	✓	✓
Mutual Authentication	✗	✓	✓
Authorization	✗	✗	✓
Central Management	✗	✗	✓
Integrity	✓	✓	✓
Replay Protection	✓	✓	✓
Downgrade Protection	✗	✗	✓
Confidentiality	✗	✓	✓
Scalability	✓	✓	✓
Hybrid Support	N/A	✓	✓
Recoverability	✓	✓	✓
Domain Separation	✗	✗	✓
Hierarchical Structures	✗	✗	✓
Ease of Use	✓	✓	✓
Flexibility	N/A	N/A	✓

Figure 4. Protocol features and benefits [11]

3.1.2. Amazon Cognito

Amazon Cognito is an identity platform for websites and applications. It is a directory, AS, and an authorization service for Open Authorization (OAuth) 2.0 access tokens and Amazon Web Services (AWS) credentials. Authentication and authorization processes via Amazon Cognito require user information from an organization's directory, the built-in user directory, and from consumer identity providers (IdP) like Amazon, Apple, Google, or Facebook. Amazon Cognito consists of two kinds of pools: user and identity.

User pools authenticate and authorize as an independent directory and OpenID Connect (OIDC) IdP and an intermediate service provider (SP) [12]. An organization's Security Assertion Markup Language (SAML) 2.0 and OIDC IdP brings user identities to Amazon Cognito and the associated website or application. Authenticated JavaScript Object Notation (JSON) Web Tokens (JWT) can be issued directly to a web server, application, or Application Programming Interface (API). Users can sign in to the website or application directly through Amazon Cognito or federate through a third-party IdP. Amazon Cognito user pools accept tokens and assertions from third-party IdPs and collect the user attributes into a JWT that it issues to the website or application. Amazon Cognito draws from the OIDC to generate JWTs for authentication and authorization. The JWT is signed using the RS256 algorithm, which is composed of a private key used to sign the payload and a public key used to check the validity of the payload and allows access to backend information. User pool processes can be seen in Figure 5.

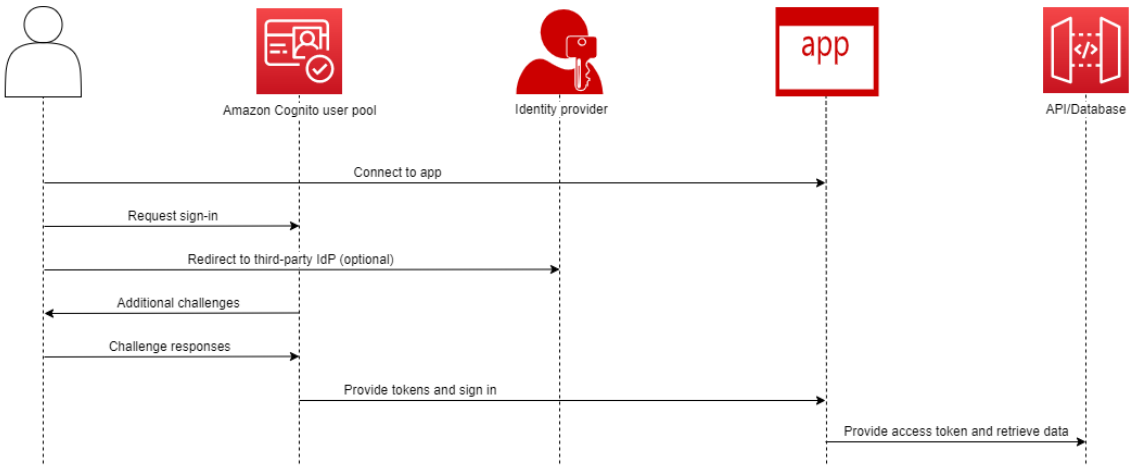

Figure 5. Amazon Cognito user pools [12]

The following features are accessible when local users are authenticated:

- A web front that authenticates, authorizes, and manages the users in the user pools
- Multi-Factor Authentication (MFA) with a One-Time Password (OTP)
- Security against compromised user accounts
- Migration of external directories into Amazon Cognito

The OAuth 2.0 and OIDC tokens issued by Amazon Cognito allow:

- An ID token for authentication with associated user information to create a profile
- An access token in the API to be accepted with the OIDC
- AWS credentials to be retrieved from an Amazon Cognito identity pool.

The alternative to user pools are identity pools. An identity pool is a "collection of unique identifiers, or identities, that are assigned as users or guests and are authorized to receive temporary AWS credentials" [12]. Identity pools authorize authenticated or anonymous users to access AWS resources. Users can be authenticated with a trusted IdP or a SAML 2.0 service. They also provide the option to issue credentials for guest users with unauthenticated identities. Identity pools use both attribute-based and role-based access control to manage the users. They can accept authentication from the organization's directory or consumer IdP .When proof of authentication is presented to an identity pool in the form of the "trusted claims from a SAML 2.0, OIDC, or OAuth 2.0 social IdP, you associate your user with an identity in the identity pool" [12]. The token that the identity pool creates for the identity can retrieve temporary session credentials from AWS Security Token Service (STS). Identity pool processes can be seen in Figure 6.

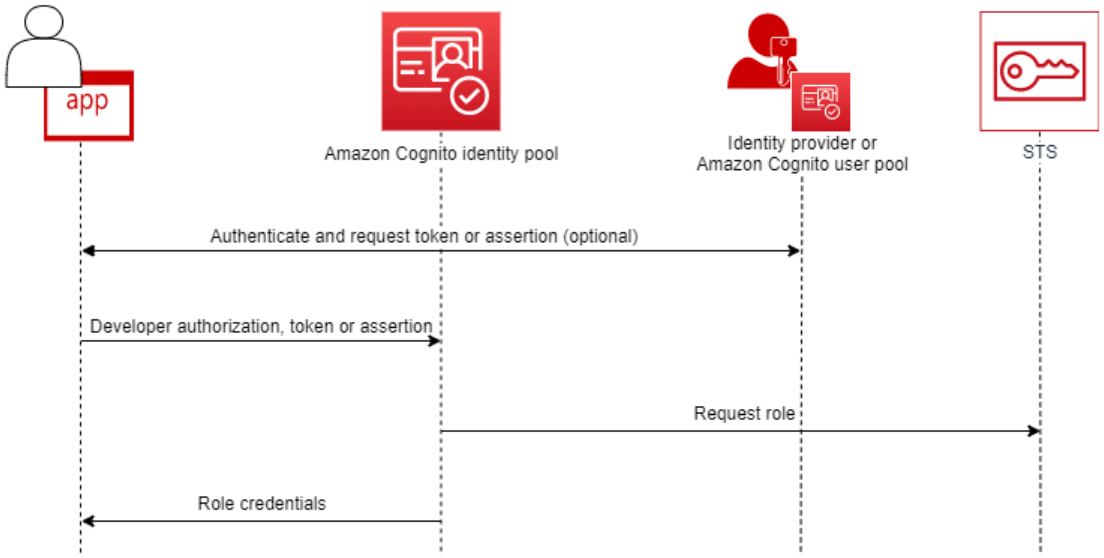

Figure 6. Amazon Cognito Identity Pools [12]

Amazon Cognito's value for NPP systems can be found in the development of Digital Twins (DT). AWS Internet of Things (IoT) TwinMaker makes it easier for developers to create DTs of real-world systems such as buildings, factories, production lines, and ICSs. A DT allows collecting varied information across the physical asset's complete lifecycle and meticulously crunch it to promote better system design, improve quality management, create high-performance systems, offer connected informational/operational intelligence, streamline diagnostics, provide predictive maintenance, and create opportunities for future smart control systems. The security improvements when developing a DT with AWS IoT TwinMaker can be found when creating Amazon Cognito user and identity pools for authentication and authorization when developing DTs via TwinMaker. Proper authentication and authorization configurations protect the data of the DT from bad actors seeking to gain access and steal (or exploit) private information while providing centralized access controls.

Amazon SageMaker is a "leading data mining software platform. It helps data miners and developers prepare, build, train, and deploy high-quality machine learning (ML) models" [13]. This software provides several tools for the data mining process including, but not limited to:

- **Data Wrangler**: Reduces time to aggregate and prepare data for mining from weeks to minutes.
- **Studio**: Provides a single, web-based visual interface where data scientists can perform ML development steps, which improves the data science team's productivity. SageMaker Studio gives complete access, control, and insight into each step as data scientists build, train, and deploy models.
- **Distributed Training Libraries**: Use partitioning algorithms to automatically split large models and training data sets for modeling.
- **Debugger**: Optimizes ML models by capturing real-time training metrics, such as sending alerts when anomalies are detected. This helps to fix inaccurate model predictions immediately.

In addition to the value found in DT development, AWS SageMaker helps build, train, and deploy ML models for any use case with fully managed infrastructure, tools, and workflows that can be incorporated into the DTs to make them entirely autonomous with bidirectional data flows. Incorporation of this software enables more people to innovate with ML through Integrated Development Environments for engineers as well as simpler no-code interfaces for business analysts, processes large amounts of structured and unstructured data for ML, reduces training time, and automates ML practices and governance across organizations supporting transparency and audit ability. The security improvements when data mining with SageMaker can be found when creating Amazon Cognito user and identity pools for authentication and authorization alongside SageMaker. Proper authentication and authorization configurations protect the data from data mining from bad actors seeking to gain access and steal (or exploit) private information.

Security and reliability were in mind when Amazon Cognito was originally designed, but like any cloud service, it is important to ensure that everything is correctly configured. If the service is not configured correctly, it could lead to misconfiguration in turn resulting in greater exposure to vulnerabilities. These misconfigurations can allow unauthorized access to user accounts or sensitive data, compromise to the confidentiality or integrity of data, and damage the reputation of the organization. Examples of misconfigurations in Amazon Cognito includes improper access controls, lack of authorization, misconfigured user data permissions, and a lack of MFA, etc.

Misconfiguration vulnerabilities include, but are not limited to:

- **Zero Click Account Takeover**: This attack occurs when the email attribute updates before verification. AWS has introduced a new security configuration to mitigate this issue but if the original attribute value remains active when an update is pending explicitly enabled, then the email attribute will not be updated to the new email address until it is verified.
- **Unauthorized Privilege Escalation**: Through writable user attributes, this attack occurs if a user modifies their own attributes to grant themselves additional permissions. If the user is an attacker, they would be able to change their role to admin. Using the API, one can alter some of the user attributes, including roles.
- **Authentication Bypass**: This attack occurs due to enabled signup API action. If the signup API is not properly disabled, the misconfiguration could allow unauthorized account creation by attackers. When creating a new user pool, self-registration may be enabled by default, allowing users to sign up for an account on their own.
- **Temporary Credentials Fetching**: As an authenticated user, this attack can occur via the AWS STS to generate temporary credentials for an IAM role with the necessary permissions to access AWS resources. Proper security measures should be implemented to ensure the user has necessary permissions, access controls, and audit logs should be in place to monitor and track access to resources using the temporary credentials.

Guidelines for proper configuration includes ensuring that any sensitive information is removed from the responses sent by the server, toggling the "sign up" feature off, disabling the unauthenticated role, checking the authenticated and unauthenticated roles to ensure that only the minimum necessary access is granted, carefully monitoring all user attributes, and removing writing permission if it's not required.

3.1.3. Telecommunications Standards

The 3rd Generation Partnership Project (3GPP) [14] is responsible for standardizing modern and widely used telecommunications protocols, notably 4G (Long-Term Evolution) LTE and 5G. The authentication procedures for these protocols are crucial, as network providers must be able to authenticate devices that use the network to ensure security and relieve potential loss of revenue by unauthenticated devices using network services. Before the introduction of stronger authentication procedures for mobile networks and Subscriber Identification Module (SIM) cards, some networks were losing the equivalent of millions of dollars of revenue due to cloning fraud, which made up approximately 15% of network traffic [15]. Thus, this industry has had a notable need for strong authentication of devices and users on telecommunications networks, and cloning fraud has become negligible in modern LTE and 5G networks.

In LTE [16], the authentication procedure aims to authenticate the identity of User Equipment (UE) (i.e., a cell phone) and use the procedure as a basis for establishing secure and authorized network access. The procedure for authentication is initiated by the UE (the main target of authentication) and is managed by the servicing network. This process involves several steps, which are referred to as the Authentication and Key Agreement (AKA) mechanism.

The authentication process is initiated by a UE attempting to connect to an LTE network. The servicing network will then issue an Authentication Request message to the Home Subscriber Server (HSS). This message will include both the International Mobile Subscriber Identity, which serves as a unique identifier for the UE, and a random challenge, referred to as RAND. Upon receiving the Authentication Request, the HSS generates multiple authentication vectors (AV) consisting of the RAND, an authentication token (AUTN), and the expected response value (XRES). This is computed using the RAND, a sequence number (SQN), and the encryption key (K). The HSS sends these vectors back to the serving network.

The UE is provided by the serving network with the RAND and AUTN selected from a chosen AV, which are used in conjunction with K to compute the result RES. The UE also verifies the HSS by comparing the message authentication code (MAC) with its computed expected message authentication code (XMAC). The RES is passed to the serving network, which compares RES with the XRES. A successful comparison of RES and XRES results in the authentication of the UE to the network and allows the UE to join the network after some additional exchanges to establish integrity and Ks to be used in further communications. This process is shown in detail in Figure 7.

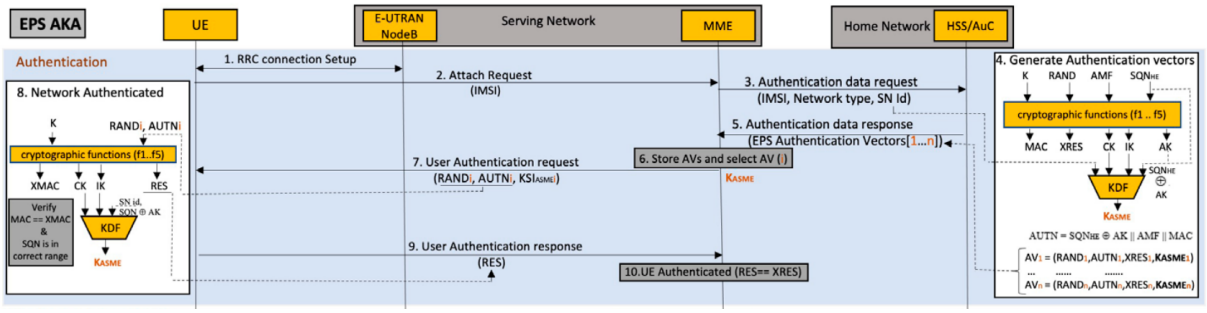

Figure 7. LTE AKA [17]

In the 5G standard, several changes have been introduced to enhance the authentication protocol and procedure compared to LTE. These changes aim to improve security, support new use cases, and accommodate the evolving requirements of 5G networks. 5G allows for multiple authentication

mechanisms (5G AKA, Extensible Authentication Protocol (EAP)-AKA prime, and EAP-TLS), all of which provide improvements on perceived weaknesses in the LTE authentication protocols. For example, the HSS is always informed of the results of UE authentication that occur in the serving network, proof of authentication is provided in an Authentication Confirmation message. Previously, the HSS provides multiple AVs to the serving network, but was not updated with UE authentication decisions. Additionally, AVs are restricted to one vector per authentication to ensure that the HSS is involved in the authentication and verification of each UE. Further, these mechanisms ensure there is a stronger mutual authentication that occurs between the UE and the HSS. For example, EAP-TLS bases this mutual authentication on trust of public key certificates.

5G provides security increases over LTE authentication mechanisms, though there are still some concerns regarding the architecture and security that may restrict its applicability to an OT environment. For example, the AKA mechanisms rely on a pre-shared key K of 128-bits, and symmetric cryptography based on 128-bit ciphers [18]. Recovery of these keys from the HSS could result in many attacks such as cloning, network spoofing, and loss of confidentiality in communications.

The service networks rely on a centralized server for the authentication of each UE (potentially a single point of failure), and the UE do not necessarily authenticate each other. Given the current status of regulation on digital communications in NPPs, the indirect connections may "include 'air-gapped' systems, CDAs behind a one-way security boundary device, or 'sneaker nets' by which data or software is manually carried from one digital device to another and transferred using physically transportable storage medium, such as floppy disks, thumb drives, portable hard disks, or other modes of data transfer" [19], this would mean that each AR must establish an HSS to maintain device identities and perform authentication procedures of devices within the network. Assuming that the requirement for control system communications to be maintained within the physical location is removed, this could open two possibilities:

- Advanced Reactor operators establish one private LTE / 5G compliant network, which each plant is able to connect to. This likely requires a large capital expenditure in the initialization of the network and the purchase of network equipment. Additionally, operators will need to implement and maintain robust network security measures to ensure the integrity of the authentication services and secrecy of pre-shared keys.
- Devices within the plant could connect to existing network providers. This allows for the operators to forgo the expenses involved in instantiating and maintaining the network and allow for security services to be rendered by experienced parties. Operators must be comfortable with the security posture of these providers before transferring this liability.

3.2. Operational Technology

For OT environments, where physical and digital process are conjoined, the concept of digital authentication cannot be directly applied from the areas where it has been typically pioneered. This is due to the unique needs and structure of digital networking within the cyber-physical environment. The landscape of current OT use cases and proposed digital control systems for Advanced Reactors contains a diverse set of devices, protocols, and applications; and therefore, demands a unique and nuanced characterization and design of authentication methodologies specifically tailored to machine to machine interactions.

Contrasting the cohesive nature of authentication methods used in IT environments, OT's varied applications have given rise to a wide range of disjointed efforts for authentication of digital assets.

This section provides a review of many proposed machine-to-machine (M2M) authentication methods for OT, highlighting the need for a harmonized approach to authentication and a unification of the wide range of OT networks.

This section aims to review and analyze proposed M2M authentication methods and protocols and analyze their applicability to Advanced Reactor networks' demands for higher automation, wireless communications, and remote monitoring and control. A comprehensive review of the current landscape provides a foundation on which recommendations for improvement and development of secure authentication and communication in OT environments can be constructed.

3.2.1. Using Machine to Machine Authorization

In the case of M2M communications, the authorization process attempts to establish trust by authorizing the client device, rather than a user. The client is "simply an application, process or even an autonomous system. For these scenarios, typical authentication schemes like username + password, social logins, etc. don't make sense" [20]. In the client credentials grant, the client can request to receive an access token for a protected resource with a client ID, client secret, along with the audience and other claims. A client credentials grant can be seen in Figure 8.

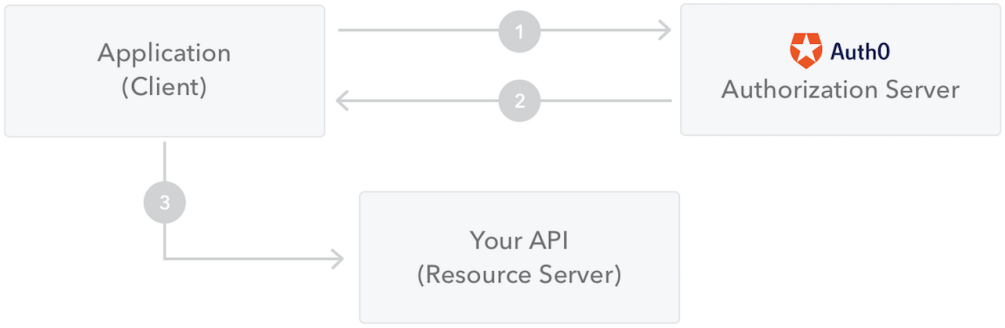

Figure 8. Client credentials grant from OAuth 2.0. [20]

In Auth0, to use the client credentials grant, administrators can create a new M2M application from the dashboard. The requirements to create the M2M application through the Auth0 dashboard includes at least one API. The APIs can be enabled or disabled in the API tab of the application. Granular permissions for M2M communications may also be configured using Hooks (Hooks are Auth0 terminology for self-contained functions) in Auth0. Via Node.js code, the actions of Auth0 are customizable and may extend the functionality of the Auth0 base platform. Hooks can be managed through the Auth0 Management Dashboard interface if needed.

Common use cases for M2M communications include, but are not limited to:

- **Backend-to-Backend (Services/Daemons)**: To authorize log storage from different services in the network, the client credentials grant provides each client with a client ID and a client secret.
- **IoT Devices**: To avoid intrusions, along with a password protected WiFi network, the client credentials grant provides each IoT device with a client ID and a client secret.

- **Command Line Interface (CLI) Clients**: For larger system use with greater automation processes, client credentials can grant client IDs and client secrets to CLI apps along with administrator supervision.

By assigning client IDs and client secrets to devices, the devices are then trusted and are not exposed to outside interaction.

3.2.2. A Framework of M2M Authentication in Smart Grid: A Two-Layer Approach

To improve the efficiency and reliability of power grids, the European Union "initiated its smart grid projects in 2003, and the U.S. Department of Energy started the Grid 2030 project almost at the same time" [21]. Under the Energy Independence and Security Act of 2007, the National Institute of Standards and Technology (NIST) coordinated the development of managing information to achieve interoperability of smart grid devices. The European Smart Metering Industry Group developed architectures and open standards for metering and communications to achieve both interoperability of smart meters and smooth integration of new energy management technologies and services. The smart grid envisions an interconnected power distribution network to ultimately streamline "production, transmission, monitoring, and gain control of electricity with two-way communications and power flows" [21].

Smart grid security involves the protection of both communication networks and the power grids because the two systems must operate efficiently before a smart grid can provide power. There have been four attack categories identified in smart grid communications including "interruption, interception, modification, and fabrication" [21].

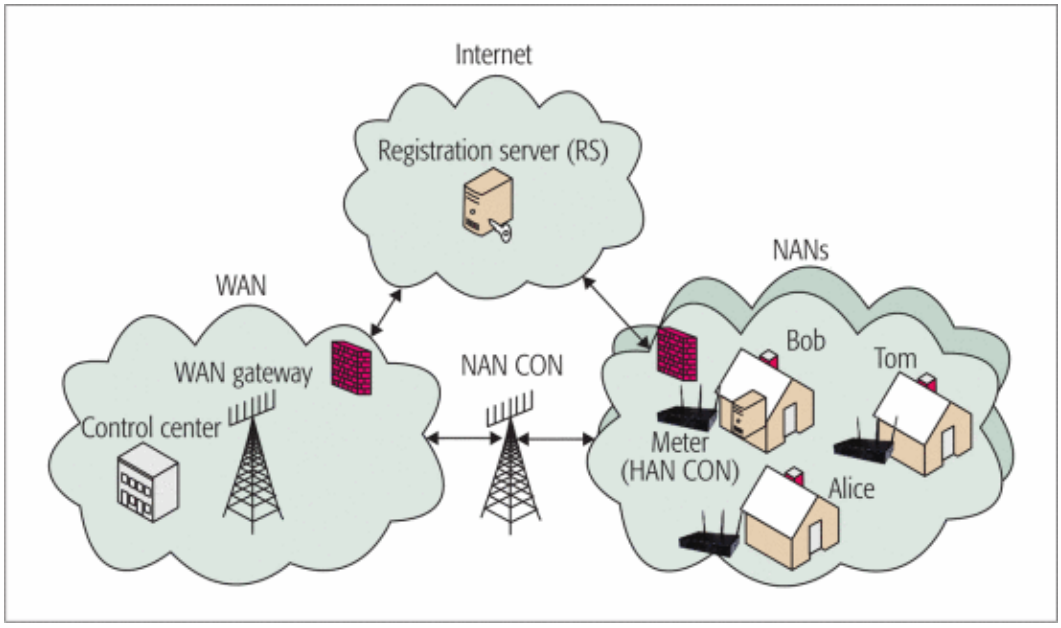

Figure 9. A simplified smart grid communications network model. [21]

As shown in Figure 9, a home area network (HAN) is a type of local area network with the purpose of facilitating communications among digital appliances inside or within close vicinity of a home. A neighborhood area network (NAN) is defined as a last-mile outdoor access network that connects smart meters and distribution automation devices to wide area network (WAN) gateways. The

energy management system (EMS) and supervisory control and data acquisition (SCADA) system in a control center of smart grid monitor and control current power delivery systems continuously to maintain the whole system working in a secure and reliable state. Data concentrators (CONs) collect information and data, often from multiple clients, before forwarding the data to the electric utility in a one-shot manner to enhance use efficiency of radio resources.

To minimize authentication overhead, a "channel power profile is particularly suitable for use as a channel signature" [21]. The channel power profile estimation provides secure M2M communications among smart meters, achieving:

- Channel diversity.
- Insensitivity to unknown channels.
- Use of both narrowband single-carrier and wideband multi-carrier communication systems.
- Enhancements to authentication performance due to antenna diversity.

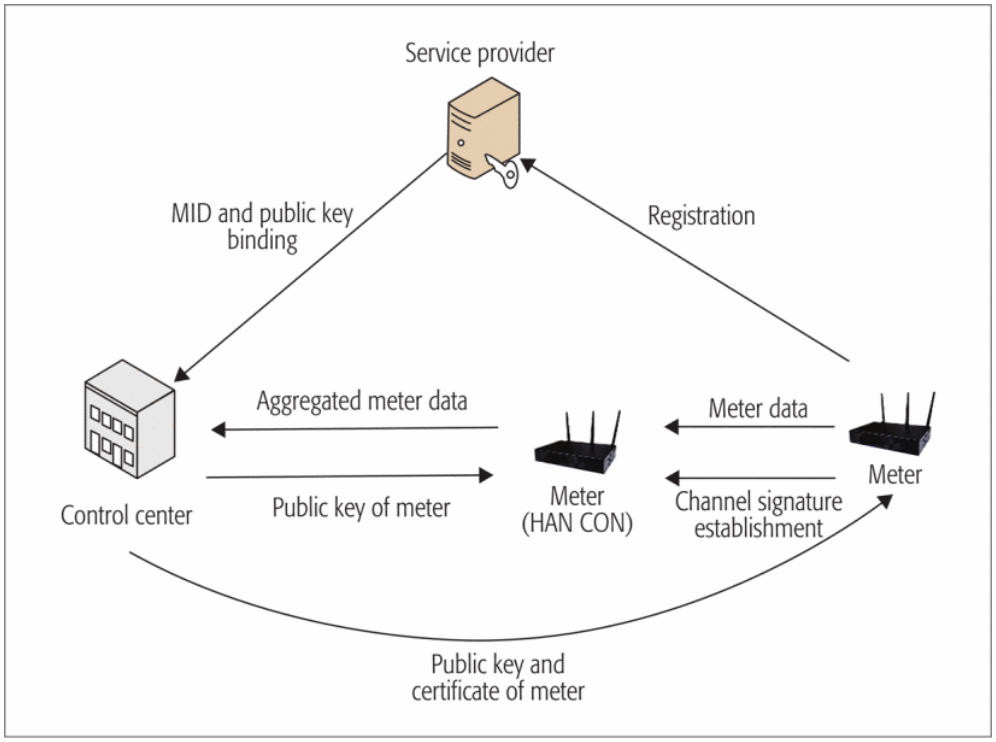

Figure 10. Message flows in the M2M authentication process. Using the two-layer approach, the public key infrastructure and channel signatures are adopted for global and local authentication of the advanced metering infrastructure, respectively. [21]

Figure 10 depicts the message flows in the M2M authentication framework for smart meters. There are three distinctive phases: global authentication, local authentication, and data transmission. The global authentication phase includes the registration, machine identity (MID) and public key binding, and public key certificate of a meter. The local authentication phase includes the channel signature establishment. The data transmission phase performs meter data collection and aggregation.

3.2.3. An Anonymous Authentication Scheme for Multi-Domain M2M Communication in Cyber-Physical Systems

Qiu et al [22] propose an authentication scheme for cyber physical systems that relies on a certificateless cryptography scheme. In this scheme, a Key Generation Center (KGC) provides users (or a device) with a partial private key, and the user uses this along with a generated random secret to compute its full private key and corresponding public key. The primary advantage to such a system is that because the full private key is not known to the KGC at any time, it is a possible solution to the key escrow problem. Key escrow in this case, refers to the issue that arises by a single party generating, issuing, or maintaining copies of private keys to multiple or all devices within a common environment [23]. This could result in a single point of failure in which the compromise of one system could result in the compromise of many other systems. The proposed multi domain architecture for the authentication scheme is shown in Figure 11

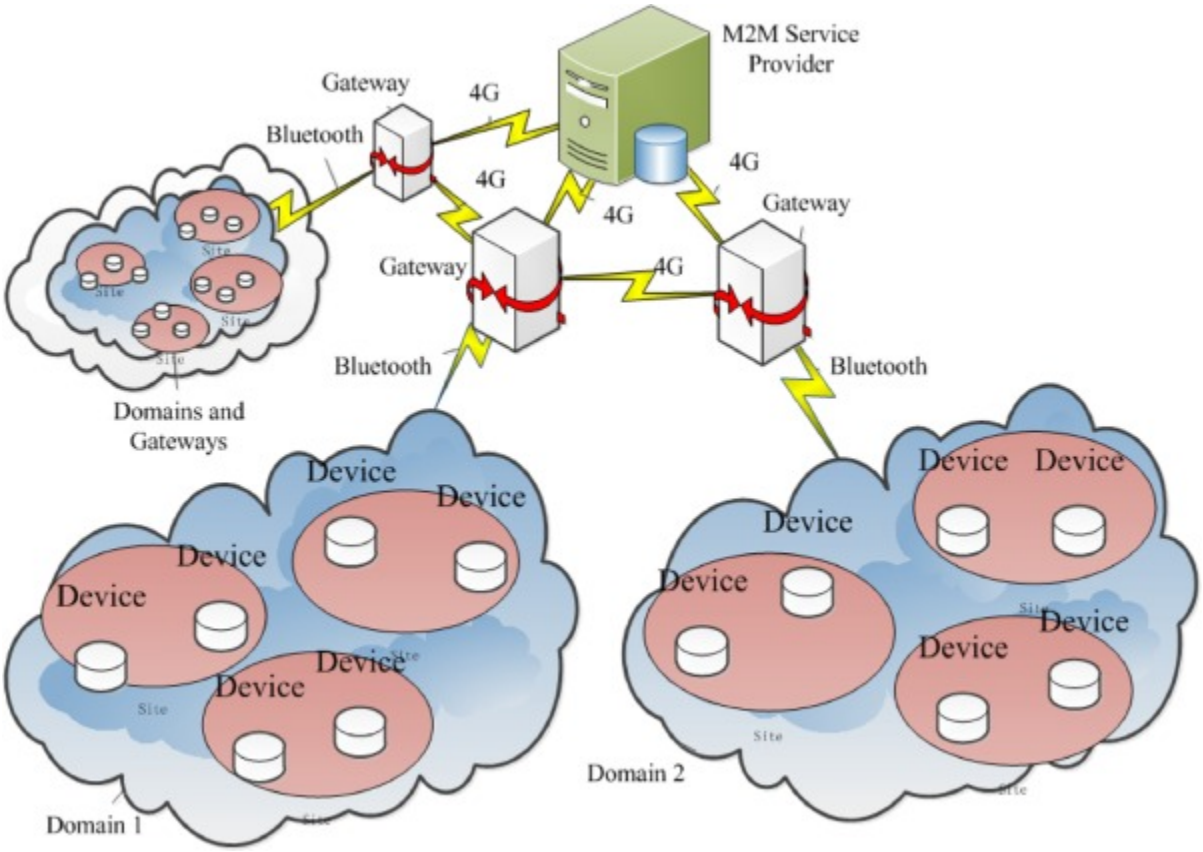

Figure 11. Proposed inter-domain M2M authentication [22]

As shown in aboveFigure 11, a M2M Service Provider (MSP) acts as a central component to the authentication architecture. In this case, the MSP also acts as the KGC. Each domain additionally has its own Gateway at the edge of the domain for which inter-domain authentication must pass through. A detailed description of the authentication process is available in [22]. Put simply, authentication occurs from a Source Device through a Source Gateway and is managed by the MSP, which forwards necessary information to a Target Gateway and finally to the Target Device.

One noteworthy advantage of this architecture is its usage of certificateless cryptography, which provides security without requiring any authority to generate or hold private keys other than the

subject of authentication. This also could remove the necessity of a Certificate Authority or trusted third party to distribute certificates for the devices public keys because the MSP takes on that role during the initialization phase. Although, inclusion of digital certificates within an authentication schema can provide devices and processes with useful and verified information, such as device manufacturer or expiration/maintenance dates.

Additionally, the implementation of an authentication scheme for device verification across site boundaries could be particularly beneficial to emerging use cases for AR and SMR technology. SMR designs are well poised for distributed applications where interactions between SMRs or centrally to a monitoring platform will be an important aspect for cybersecurity. Other use cases for NPPs such as hydrogen electrolysis could benefit from this cross-boundary communications, for example, receiving information from the electrolysis process to better inform processes within the plant. In short, this would allow devices in distinct applications to authenticate one another, leading to improved efficiency and facilitating adaptable processes in response to quickly changing demands of industrial processes or the grid.

While inter-domain authentication is a useful aspect of this architecture, it does not solve the need for intra-domain authentication. The authentication mechanism relies on the MSP to perform device authentication. While this may still be used for authentication within the network, it would require the information to leave the boundary, which could cause unnecessary delays when authenticating devices that are in close proximity from a network perspective. In the current description, it can be assumed that the communication between devices within a domain maintains a posture of implicit trust, which still must be mitigated.

The MSP in this architecture may also prove to introduce concerns when looked at for a nuclear application. Because the MSP fulfills a critical role, there must be sufficient redundancy measures in place for its possible failure. If the MSP (or the source or target gateway) were to fail or become unavailable, devices would be unable to authenticate each other's identities. A potential solution would be to allow for a second MSP that can be used as a fallback, which would require significant work to ensure that both MSPs are securely communicating to maintain synchronized databases for authentication.

Because the MSP provides the authentication service to multiple domains, there must be some defined policy by which those domains agree for the management of the MSP. Managing the MSP or determining an acceptable steward requires consensus and cooperation among multiple entities (including relevant regulatory bodies). This challenge is not unique, and would be a required process when establishing a Certificate Authority (CA) or list of trusted CAs for a shared public key infrastructure (PKI).

3.2.4. A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment

Esfahani et al propose a lightweight mechanism for authentication in Industrial Internet of Things environments [24]. The protocol use case described within the report is between a smart sensor and a router, where an AS acts as an oracle for the smart sensor to "register" into the environment and receive necessary cryptographic functions for mutual authentication with the router. The registration procedure is shown in Figure 12.

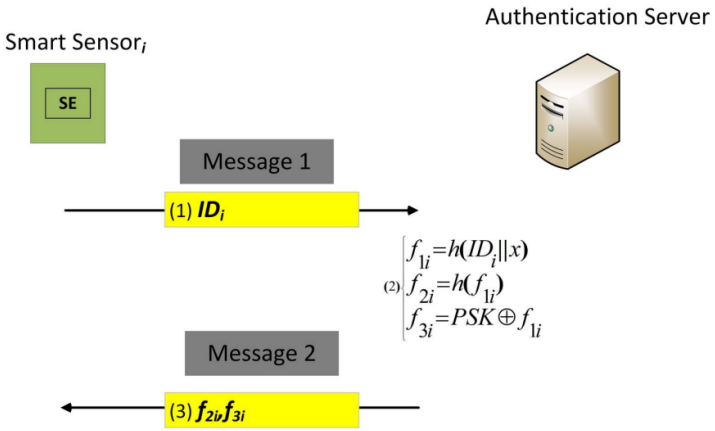

Figure 12. Esfahani et al registration procedure [24]

In Figure 12, "h" denotes a one-way hash function, ID denotes the identity of the smart sensor, x denotes the private key of the AS, and Predefined Pre-Shared Key (PSK) denotes a predefined pre shared key between the AS and the destination device, in this case a router. An in-depth description of the protocol for registration and authentication processes is available in [24]. These procedures were designed to make use of common and low computational overhead functions to achieve an authentication mechanism that is lightweight enough to be suitable for real time environments.

While the mechanism described is lightweight, and a marked improvement over the current practice of implicit trust, there are many aspects that are undefined, which could leave room for errors causing large security gaps in a final implementation. For example, the protocol defines that during the registration procedure, the smart sensor should communicate with the AS over a secure channel. This secure channel, its underlying cryptographic mechanisms, or requirements are left undefined, however. Additionally, the security of the registration procedure relies heavily on the confidentiality of the smart sensor ID. The AS does not explicitly authenticate the smart sensor during the enrollment process, so there is undefined behavior for an unknown device requesting to authenticate. It is possible that the AS is loaded with an allowed list of IDs, and only responds to allowed devices, though. If an attacker is able to learn the ID of a device on the network, the AS could be probed for the same response, or if the communication channel is not sufficiently confidential, both the ID and response could be recovered. Because the AS's secret key, x, is concatenated with the ID and then hashed twice, an attacker may be able to perform an offline attack to recover the AS's secret key, meaning the identity of all devices authenticated through the AS is no longer trustworthy. This could be mitigated by a TTL constraint on the key x or an appropriately long key, but these parameters are not explicitly stated. Additionally, the procedure relies on PSK, for which the protocol assumes that the AS has previously established with the router.

This page left blank

4. ANALYSIS FOR ADVANCED REACTORS

Authentication can be thought of as the process by which trust is established in the identity of an entity, which may be human, digital, or a combination of both. In digital systems, there are three factors by which authentication can be established: something you are, something you have, and something you know [25]. While authentication and trust between or involving humans can adapt to changing contexts, digital devices require a prescribed and procedural method to establish this trust automatically.

The earliest form of authentication in digital systems came in the form of "something you know." In this case, a PSK (i.e., a password) was established between users and multi-user computers in the 1960s [26]. Although many advances have been made since, the principle of the PSK is still alive in many commonly used authentication mechanisms, like Kerberos and LTE. At scale, maintaining this mapping on each device would require a very high storage footprint for devices to directly authenticate each other. Additionally, although there are some generally cryptographic protections on the PSK while in storage (e.g., cryptographic salt and hashes, which ensure that PSKs are stored in a fashion that allows for the authenticator to verify that the attested PSK matches but is never stored in plaintext, creating a higher workload for an attacker to recover the PSK), an attacker who gains access to these could perform offline attacks to recover the secret. Therefore, there is generally an established central authority to maintain a database of identities and their associated secret. This creates a "crown-jewel" for attackers to target within the network, giving near complete autonomy once it is compromised. Enterprise environments are able to maintain a lower risk factor because of regular security updates to services like Kerberos. But, in an NPP, strict configuration management controls, maintaining regular updates in this fashion is likely infeasible due to Verification and Validation (VnV) procedures that delay changes to digital assets (especially those considered Important to Safety (ItS)) for possibly weeks or months.

ARs must be designed both in terms of physics and digital systems to limit risk. Risk is defined as probability x consequence. Reviews of protocols and methodologies relying on PSK find that a key aspect is the inclusion of a central authentication service, which maintains (at least in some fashion) critical information about authorized devices and their permissions. An adversary who is able to gain total compromise of the authentication server may gain full control over all authorization and authentication processes within the plant, and possibly extract critical information about digital assets allowing for ongoing attacks and subversion of authentication for one or many digital assets. Because successful attack in a PSK-based authentication scheme pose devastating potential consequence for ARs, it is not recommended that this approach be used, unless risk analyses find that the probability of successful attack is significantly low due to other cybersecurity controls within the operational environment.

In contrast to a PSK-based approach, many modern authentication mechanisms are moving toward principles that rely on asymmetric cryptography. These generally involve a PKI and X.509 [27] certificates. Certificates are used to prove an identity's origin (like a chain of custody) stemming from a route CA and potentially through intermediate CAs. A digital signature can then be used by a subject of authentication to prove its correlation with the digital certificate. A notable benefit in comparison to an architecture relying on PSKs, is that each digital asset is able to mutually authenticate another without the need of a central authentication server (like the internet). However, there is still a requirement for a highly trusted party within this schema, in the form of the CAs. CAs are a highly valuable target to attackers, and successful attacks have occurred in the past [28] [29]. Careful consideration must be made by integrators and operators when deciding the trustworthiness of certificates within the infrastructure.PKI offers many benefits over PSK-based authentication, the

key being that secret keys may be stored on individual digital assets, and other assets may authenticate its identity without the need for sharing information that can be used to recover keys over the network. Authentication schemes relying on a PKI also have the flexibility to decide whether to transfer risk of CA compromise to a third-party with expertise in the area or maintain the system in-house. This gives AR vendors the opportunity to conduct a personalized evaluation and select a solution, while still maintaining a cohesive authentication structure across AR sites.

One alternative to PKI is Web of Trust [30], which grants entities the responsibility of managing their own network of trust. Within this paradigm, entities decide to trust others based on behavioral attributes or mutual connections, effectively eliminating the need for a centralized authority. However, the adoption of this model in an OT/highly automated environment would require well-defined procedures, backed by verified behavioral information, which is currently lacking in the OT realm. Therefore, Web of Trust authentication schemes are not recommended for AR networks.

Blockchain-based mechanisms, like proposed in IEEE's 4th International Conference [31] blockchain-based PKI solutions for IoT present another avenue for authentication tailored to OT. In this schema, organizations allow digital assets to generate their own public/private key pairs during device commissioning. The organization then creates a digital certificate for this keypair and adds it to a distributed ledger. Each digital asset in the network queries the ledger (stored locally or in remote nodes) during authentication. A core benefit to the distributed ledger paradigm for NPPs lies in the inherent distributed nature, providing redundancy and resilience. Remote nodes and all digital assets maintain the same ledger, removing potential downtime or failures due to a central authentication server's failure. Additionally, because the ledger still leverages digital certificates, these can be used to store useful associated data about digital assets such as their manufacturer, date of commission, firmware versions, etc. Although, the device provisioning process, digital assets used during provisioning, and remote nodes storing the ledger must maintain a mature security profile and be trusted by digital assets within the network.

Because of the unique needs and requirements of AR systems, it is recommended that block-chain based approaches be incorporated into the authentication schema. Because CDAs must not be connected to the internet, this gives AR operators the ability to provision new digital assets into the environment while maintaining a strong PKI-based authentication schema. Additionally, important information about the PKI (like revocation lists) can be introduced into the AR network via "sneaker-net" removing the need for digital assets to connect to the internet in order to access the revocation lists. Blockchain provides strong cryptographic protections on the integrity of the ledger, ensuring that digital assets all have access to the same information.

4.1. Cryptography in Real-Time Environments

Real-time environments have specific constraints in timing and resources. Devices must achieve certain functionality in a critical window of time to prevent system failure. Video conferencing an application widely used today is a real-time environment where information must be transmitted and received within a precise range of time for communication to occur properly. Control systems must also deliver sensor reading and processing in a timely manner, or SCADA systems will be useless and inaccurate. These devices often also have restraints on their memory and processing power. Because of the environments where these systems operate, these devices are often required to be compact. Any operations running on these systems must not be too central processing unit or memory intensive. These processes must also not consume too much energy and power.

In ICSs, PLCs are responsible for data retrieval and processing from sensors. As mentioned before these systems are typically small and under strict requirements. In 2017, an assessment of cryptographic protocols for real time embedded systems was released that show the data, energy, and time costs of various asymmetric and symmetric cryptographic algorithms [32]. In this report the authors find that data size of the cryptographic function has a large impact on the power consumption and energy of the device. They also prove that the energy consumption of an operation is near-linear to its execution time.

In a real-time system, the main cryptographic threats to consider are often snooping, alteration, and spoofing. In advanced reactors mitigating these threats are crucial to the safety and performance of critical operations. Snooping refers to an unauthorized accessing of information and data. Snooping is typically blocked by symmetric encryption, which provides confidentiality to one's messages. In the previously mentioned report the following symmetric algorithms were under analysis [32]: DES, 3DES, IDEA, AES, CAST, RC2, RC4, RC5, BLOWFISH, SKIPJACK. These algorithms were assessed in various categories, one of them being data processing speed. The algorithm RC4 was shown to process the most kilobytes per second. However, RC4 is known to be vulnerable to bit-flipping attacks. An advanced reactor developer must take these categories into consideration during their implementation process, while also understanding the potential security tradeoffs. An example of a more acceptable encryption primitive could be AES, which has relatively low performance and memory requirements while providing strong levels of protection against information disclosure.

Alteration refers to a changing of sensitive data. The standard method of maintaining the integrity of some data is by running it through a hashing algorithm. These algorithms are one-way functions that can transform any piece of data into a set length digest. A change to a single bit in the input data leads to a drastically different output in the digest. The most common hashing functions are MD2, MD4, MD5, SHA-1, and SHA-2. MD5 has the lowest unit energy consumption however, similar to the lowest energy consumption encryption (RC4), tradeoffs must be considered as MD5 is now considered deprecated. A recommended course of action would be to select an algorithm with higher security but acceptable energy consumption specific to a given AR design. Spoofing denotes an impersonation of some party in the system. Authentication services typically prevent spoofing by verifying the identity of the desired party. This is typically accomplished through asymmetric cryptography algorithms such as the Elliptic Curve Digital Signature Algorithm and Rivest-Shamir-Adleman. Various tables and figures showing the energy and time costs of these algorithms are presented in this cited report [32].

There have been many efforts to create lightweight cryptography protocols. Two notable algorithms are the SIMON and SPECK ciphers. These algorithms were made by the National Security Agency in response to U.S. Government requirements. The SIMON and SPECK cipher both have simple, easily implemented round functions and key schedules that minimize computational power, but in return impact cryptographic security. There have been a few papers regarding reduced round attacks on these algorithms [33].

In 2019, applicants submitted algorithms to a NIST competition for Authenticated Encryption with Associated Data. These algorithms were to be lightweight cryptographic procedures combining the properties of confidentiality and authentication. The environments under which these algorithms were to operate would be under various constraints. The ten finalists listed here: ASCON, Elephant, GIFT-COFB, Grain-128AEAD, ISAP, PHOTON-Beetle, Romulus, SPARKLE, TinyJAMBU, and Xoodyak were accepted to the final selection round [34]. In 2023, NIST announced their winner for this competition. They announced that the best "defender of data" created by small devices is the algorithm ASCON. This algorithm had won prior competitions,

which highlights the numerous rounds of scrutiny it has faced by cryptography experts. ASCON is a family of algorithms and one of its variants also offers some resistance to quantum computing attacks. Due to NIST's assessment of this algorithm it may be worthwhile investigating the functional use of ASCON in ICS environments.

Real-time environments can benefit by the introduction of hardware cryptography measures. These measures come in the form of Trusted Platform Modules (TPMs) and Physically Unclonable Functions (PUFs). TPMs are a microchip that allows storage of any type of cryptographic and/or configuration information including keys, passwords, digital signatures and more. A user must be able to correctly authenticate to the chip to access these resources. PUFs are created through the manufacturing process of an integrated circuit. The random physical aberrations that are created inside the device can be used as a fingerprint when generating some cryptographic key. A PLC could use these measures in the generation and storage of their keys and critical data.

These real-time systems must have a key management system in place. A key management system could keep track of which users and services are currently able to securely communicate with each other, how long to the session has been ongoing, and how much longer the session should be allowed to continue. This system should manage distribution of certain keys and aggregation of log information pertaining to key use throughout the environment.

5. CONCLUSION

In the realm of OT and digital networks in NPPs, where sensitive physical processes are controlled and operated by digital assets, authentication becomes a key component to maintaining a strong cybersecurity posture. As use cases change and AR technology becomes more prominent, network structures may require an evolution from the current "air-gap" and trusted boundary approach, necessitating strong and reliable authentication methodologies for digital instrumentation and control components. The unique aspects of NPP environments also require a nuanced approach to developing new M2M authentication procedures that blend modern advances in authentication from traditional IT environments with domain-specific considerations for the nuclear industry.

A core principle for authentication in networks moving toward ZTA, remote access, and strong cybersecurity controls in general is mutual authentication. Mutual authentication ensures that trust is reciprocated between all communicating digital assets. Without this, there must be an implicit trust in one party, leaving room for attackers to leverage trusted assets for attack. This aligns with the principles of Zero Trust and ensuring security on both sides of any digital communication.

Recommendations based on reviews and analyses presented within this report are as follows:

- Use ticket-based authentication to ensure timely reauthentication within the AR network.
- Use of asymmetric cryptography to ensure unique digital identities and critical information is not redundant on the network.
- Incorporation of digital certificates to aid in contextual information and advanced decision-making during authentication.
- Incorporation of block-chain technologies to allow for secure redundancy of non-critical information such as public keys, and ensure synchronization.

Approaches to authentication that use a ticketing system are found in common IT authentication protocols such as Kerberos. Tickets are used to ensure that the authentication process used by a person or digital asset to access another digital asset or service is given strict parameters regarding its allowed level of access and the timing related to this access. This approach is particularly useful for OT environments, because conversations between devices may span extended durations, making timely re-authentication unintuitive without a similar construct. These tickets should be based on either a time to live, amount of data transmitted, or a combination of both. This ensures that trust remains relevant and up to date for communications between digital assets.

As computation speeds increase and power draw decreases in digital devices, many authentication protocols are moving toward asymmetric cryptography (for example, the inclusion of the EAP-TLS authentication in 5G). Asymmetric cryptography within an encryption scheme offers many benefits over symmetric or PSK-based authentication approaches, particularly that a private key can reside exclusively in the device whose identity is associated with it. Generally, the benefit of using symmetric cryptography is the large gap in performance/computation time for asymmetric operations. But, because authentication does not need to occur with each individual message, it is a prudent choice, especially in an environment like an NPP, where communications between digital assets are more formulaic than an unpredictable Enterprise or telecommunication network.

Asymmetric cryptography also opens the possibility of leveraging digital certificates. Digital certificates can be used to enrich the authentication landscape and amount of useful data. Digital certificates are not only used to establish identity, but also can house contextual information that can

be useful for real-time automated decision making. This information can include important aspects of a device like manufacturer, commissioning date, firmware versions, etc. Additionally, these certificates, when tied back to a manufacturer can assist in mitigation of supply chain attacks by providing a chain of custody from a particular device back to its manufacturer.

Blockchain integration into the authentication approaches emerges as a compelling approach to authentication procedures in NPPs. The distributed ledger inherently assists in ensuring redundancy, assisting in requirements for removing Common Cause Failure. Because the ledger can be distributed among multiple remote nodes, it allows for devices and authentication servers to maintain up to date and redundant copies of digital certificates and digital asset IDs. Additionally, this approach would allow for revocations for decommissioned or otherwise untrusted devices or certificates to be added to the ledger. Querying of a certificate revocation list could pose as a particular challenge for traditional PKI in NPPs because this requires an internet connection unless an on-site list is updated regularly via "sneaker-net."

Although an approach using a blockchain distributed ledger allows for the removal of a CA, it does not necessitate its exclusion from the paradigm. CAs allow for traceability and relatively trustworthy reporting of interactions that occur outside of the NPP environment. This could allow for cryptographic verification of a device's manufacturer, integration information, and operational details, assuming correct configuration of trusted root CAs and each parties' alignment with the infrastructure. The blockchain could allow for multiple certificates per digital asset, enabling operators to tailor authentication requirements to unique demands of their particular environments.

Given these insights, the path forward to a standardized and accepted authentication schema for NPPs and OT in general remains complex. Industry stakeholders must analyze associated risk and make common decisions regarding acceptable CA parties, preferences for in house or third-party management of related software and hardware, options for adopting complete technologies/proposals, and what acceptable costs or development and operation are worthy of the benefits. While the future of NPP authentication requires a multifaceted approach, and further input from industry partners, this research finds that any given decisions can be supported by an amalgamation of existing approaches and technologies.

REFERENCES

[1] Cybersecurity & Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure," Cybersecurity & Infrastructure Security Agency, 20 July 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. [Accessed 22 August 2023].

[2] P. Grassi, M. Garcia and J. Fenton, "NIST Special Publication 800-63-3 Digital Identity Guidelines," June 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf. [Accessed 23 August 2023].

[3] International Atomic Energy Agency, "Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Revision 5)," International Atomic Energy Agency, 2018. [Online]. Available: https://www.iaea.org/publications/11092/physical-protection-of-nuclear-material-and-nuclear-facilities-implementation-of-infcirc225revision-5. [Accessed 22 August 2023].

[4] Administration Cybersecurity Priorities for the FY 2025 Budget, 2023.

[5] MITKerberos, "Kerberos: The Network Authentication Protocol," 11 July 2023. [Online]. Available: https://web.mit.edu/kerberos/.

[6] T. Y. C. Neuman, "The Kerberos Network Authentication Service," July 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4120.

[7] MIT, "MIT Kerberos Documentation," 2015. [Online]. Available: MIT Kerberos Documentation. [Accessed 24 8 2024].

[8] J. Gerend, "Kerberos Authentication Overview," 29 July 2021. [Online]. Available: https://learn.microsoft.com/en-us/windows-server/security/kerberos/kerberos-authentication-overview.

[9] V. Shastri, "Kerberoasting Attacks," 1 March 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/kerberoasting/.

[10] MITRE , "Steal or Forge Kerberos Tickets: Kerberoasting," 30 March 2023. [Online]. Available: https://attack.mitre.org/techniques/T1558/003/.

[11] E. Biham, "K7: A Protected Protocol for Industrial Control Systems," April, 12, 2021.

[12] Amazon, "What is Amazon Cognito?," 2023. [Online]. Available: https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html#what-is-amazon-cognito-user-pools.

[13] "What Is Data Mining?," 2023. [Online]. Available: https://aws.amazon.com/what-is/data-mining/. [Accessed 01 May 2023].

[14] 3GPP, "3GPP Privacy Policy," 3GPP, 2019. [Online]. Available: https://www.3gpp.org/. [Accessed 22 August 2023].

[15] K. Mayes and T. Evans, "Smart Cards for Mobile Applications," 2008. [Online]. Available: https://link.springer.com/chapter/10.1007/978-0-387-72198-9_4. [Accessed 23 August 2023].

[16] 3GPP, "LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Radio Transmission and Reception," 2017. [Online]. Available: https://www.etsi.org/deliver/etsi_ts/136100_136199/136101/14.05.00_60/ts_136101v140500p.pdf. [Accessed 23 August 2023].

[17] R. M. Dhanasekaran and S. Nair, "A Comparison of 4G and 5G Authentication Methods," Nokia, 2023. [Online]. Available: https://onestore.nokia.com/asset/210846. [Accessed 23 August 2023].

[18] ETSI, 5G; Security Architecture and Procedures for 5G System, ETSI, 2018.

[19] U.S. Nuclear Regulatory Commission, *Regulatory Guide 5.71 Cyber Security Programs for Nuclear Facilities,* https://www.nrc.gov/docs/ML0903/ML090340159.pdf, 2010.

[20] S. Peyrott, "Using Machine to Machine (M2M) Authorization," 07 October 2021. [Online]. Available: https://auth0.com/blog/using-m2m-authorization/. [Accessed 01 May 2023].

[21] W.-L. Chin, Y.-H. Lin and H.-H. Chen, "A Framework of Machine-to-Machine Authentication in Smart Grid: A Two-Layer Approach," IEEE, 16 December 2016. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/7786117. [Accessed 01 May 2023].

[22] Y. Qiu, M. Ma and S. Chen, "An Anonymous Authenticaiton Scheme for Multi-Domain Machine-to-Machine Communication in Cyber-Physical Systems," Elsevier B.V., 24 December 2017. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S138912861730381X. [Accessed 22 August 2023].

[23] H. Abelson, R. Anderson, S. M. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. G. Neumann, R. L. Rivest, J. I. Schiller and B. Schneier, "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption," 1988. [Online]. Available: https://www.schneier.com/academic/archives/1997/04/the_risks_of_key_rec.html. [Accessed 22 August 2023].

[24] A. Esfahani, G. Mantas, R. Matischek, F. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. G. Tauber, C. Schmittner and J. Bastos, "A Lightweight Authentication Mechanism for M2M Communciations in Industrial IoT Environement," February 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8006209. [Accessed 22 August 2023].

[25] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, September 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf. [Accessed 23 August 2023].

[26] L. Volonino and P. Dalal, "Network Middleware," 23 November 2007. [Online]. Available: https://doi.org/10.1002/9781118256107.ch3. [Accessed 23 August 2023].

[27] ITU, "ITU-T Recommendations," October 2019. [Online]. Available: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509. [Accessed 23 August 2023].

[28] P.-M. Bureau, "Win32/Stuxnet Signed Binaries," ESET, 19 July 2010. [Online]. Available: https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/. [Accessed 23 August 2023].

[29] J. Nightingale, "Revoking Trust in DigiCert Sdn. Bhd Intermediate Certificate Authority," Mozilla, 3 November 2011. [Online]. Available: https://blog.mozilla.org/security/2011/11/03/revoking-trust-in-digicert-sdn-bhd-intermediate-certificate-authority/. [Accessed 23 August 2023].

[30] A. Ulrich, R. Holz, P. Hauck and G. Carle, "Investigating the OpenPGP Web of Trust," 2011. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-642-23822-2_27. [Accessed 23 August 2023].

[31] A. Singla and E. Bertino, "Blockchain-Based PKI Solutions for IoT," 20 October 2018. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/8537812. [Accessed 23 August 2023].

[32] G. Z. Jiang Wei, "Measurement-based research on cryptographic algorithms for embedded real-time systems," *Science Direct ,* vol. 59, no. 10, p. 11, 2017.

[33] R. Beaulieau and S. Treatman-Clark, "The SIMON and SPECK lightweight block cipher," in *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC)*, San Fransisco, 2015.

[34] M. Turan and K. McKay, "Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process," *NISTIR 8369,* 2021.

[35] A. Hall and L. Drakopoulos, "Building Fine-Grained Authorization Using Amazon Cognito User Pools Groups," 01 August 2017. [Online]. Available: https://aws.amazon.com/blogs/mobile/building-fine-grained-authorization-using-amazon-cognito-user-pools-groups/. [Accessed 01 May 2023].

[36] "AWS IoT TwinMaker," 2023. [Online]. Available: https://aws.amazon.com/iot-twinmaker/. [Accessed 01 May 2023].

[37] Y. Yan, Y. Qian, H. Sharif and D. Tipper, "A Survey on Smart Grid Communication Ingrastructures: Motivations, Requirements and Challenges," 24 February 2012. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6157575. [Accessed 01 May 2023].

DISTRIBUTION

Email—Internal

Name	Org.	Sandia Email Address
Lon Dawson	8851	ladawso@sandia.gov
Ben Cipiti	8845	bbcipit@sandia.gov
Christopher Lamb	8851	cclamb@sandia.gov
Benjamin Karch	8851	brkarch@sandia.gov
Romuald Valme	8851	rvalme@sandia.gov
Minami Tanaka	8851	matanak@sandia.gov
Technical Library	1911	sanddocs@sandia.gov

Email—External

Name	Company Email Address	Company Name
Katya LeBlanc	katya.leblanc@inl.gov	Idaho National Lab
Cheyenne Odenthal	cheyenne.odenthal@inl.gov	Idaho National Lab

This page left blank

Sandia National Laboratories

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.