A Standardized Trust Model for Enabling Data Security and Interoperability within Smart Distributed Systems

David P. Maher
Technology Initiatives
Intertrust Corporation
Milpitas, USA
dpm@intertrust.com

Hebberly E. Ahatlan
Technology Initiatives
Intertrust Corporation
Milpitas, USA
heb@intertrust.com

Anahita D. Poonegar
Technology Initiatives
Intertrust Corporation
Milpitas, USA
apoonegar@intertrust.com

***Abstract*— Smart distributed systems (SDS) are the foundation of smart cities, utilities, supply chains and hospitals. They support digital marketplaces where data is exchanged to generate value in the form of social services, business functionality or money. They are the engine of modern economies. They communicate data and real-time action requests from multiple parties, with diverse owners, enable better insights from AI, and deliver safer, more efficient and sustainable environments. But what is the impact if the data used by these systems is compromised?**

Without data security and interoperability, these systems would be wasteful and inefficient, and could even become lethal weapons. In this paper, we propose a solution to allow secure collaboration of data within SDSes. We propose establishing an achievable global standard that lays the framework for interoperability, security, and authentication across the totality of the smart distributed system.

Keywords—data security, data interoperability, zero-trust architecture, authentication, data integrity, distributed energy systems

I. Introduction

Smart distributed systems (SDS) are complex data and IoT networks that encompass billions of sensors, AI and machine learning ecosystems. They connect private and public information across all verticals in a social and economic fabric from online social services for citizens to neighborhood rooftop solar panels.

Smart distributed systems have three key characteristics:

- **Cyber-physical integrations:** Computational and communication components are combined with physical elements to collect information via IoT sensors, transfer it through networks, and analyze data with AI to make decisions that control physical processes. An example is a system for delivering electricity for a city.
- **Heterogeneous entities:** Diverse elements that make up a digital economy, including people, IoT networks, wind farms, local and national governments, smart transportation infrastructure, businesses, emergency response systems, hospitals, agricultural farms, and smart factories.
- **Hyperconnectivity:** The accelerated pace at which heterogeneous entities are interconnecting dynamically with each other, creating complex layers of cyber physical integrations.

Smart distributed systems are expected to propel modern data-driven economies [1], but if their data is compromised, or they cannot enable secure collaboration around their data, then they would be at best, wasteful and inefficient - at worst - they could become lethal weapons. In this paper we propose how to bring greater security and interoperability to smart distributed systems. We propose establishing a standard that lays the framework for interoperability, security and authentication across the totality of the Smart Distributed System. We use a subset of SDS—distributed energy ecosystems (DEE)—as the centerpiece of our discussion.

II. Distributed Energy Ecosystems

Distributed Energy Ecosystems encompass energy generation, storage, distribution, consumption, monitoring, and control elements. A DEE is distinctly dynamic, and its automated control subsystems support demand modulation, time shifting, storage diversion, and bi-directional power flows. This allows DEEs to bring new elements online or offline with precision, driven by sophisticated, automated multi-faceted optimizations, often using artificial intelligence.

DEEs need a signaling system for commands, transactions, status information, and data distribution with a control subsystem that executes policies to support a hierarchy of objectives that begin with safety and reliability and cover numerous technical, environmental, economic, social, and political objectives. DEEs can provide safe and reliable power with lower atmospheric carbon impact, and greater operational efficiency and support power packetization, where smart infrastructure balances power grids to increase capacity [2].

Robust growth for these kinds of ecosystems requires interoperability and risk management, specifically targeting burgeoning threats to system integrity. Commands, action requests, and their responses must be authoritative with provenance that is verifiable in real-time. Standards provide interoperability for these assurances, maintain trustworthiness and accommodate OT, IT, and hybrid IT/OT capabilities. Privacy, confidentiality, and transparency must be supported as appropriate for each type of message and circumstance.

A Trust Model for a secure, open, interoperable, dynamic, control system overlaying the Internet and private networks is most challenging, especially when the communicating elements are used or owned by various independent entities, managed and deployed by a different set of entities, and manufactured and supplied by yet another set of entities, whereby the functions of

979-8-3503-9775-8/23/$31.00 ©2023 IEEE

the system have multiple, conflicting objectives among those entities, and the system is subject to attack by an array of nefarious actors ranging from pranksters to fraudsters to political and state-funded terrorists.

III. A PROPOSED SOLUTION FOR GREATER SECURITY & INTEROPERABILITY

Effective operational and secure interoperability requires some novel and specific approaches. We address these challenges by implementing a trust model to minimize the burdens of interoperability, organized into four layers:

TABLE 1. TRUST LAYERS & CONCERNS

Layer	Trust Concerns
3	Robustness, Renewal, Compliance
2	Trusted key management
1	Assurances for the signaling framework
0	Protected resources in the ecosystem

In Layer 0 the trust model accounts for all resources and classifies them according to function and vulnerability. It also defines what entities need to interact with those resources. This allows a *zero-trust model* [3] to be deployed throughout the ecosystem. Layer 1 unambiguously defines the ecosystems encryption, authentication, authorization, and validation schemes for messaging and persistent data protection. Layer 2 supports Layer 1 with advanced, but flexible, cryptographic key management policies and mechanisms, making system administration easy and efficient, and which allows for control by different parties who are accountable for different entities in the ecosystem.

Layer 3 includes robustness measures reinforcing assurances and protections described at the lower layers. They describe measures designed to limit the scope of external interactions with the resources at level 0, assuring the systemic effectiveness of layer 1. Another layer 3 security construct is renewability of the lower layer security mechanisms. DEEs are a rich target for sophisticated cybercrime, and need to adapt to fight new threats, expanding and improving risk management procedures.

To promote interoperability, recognizing the various use cases and approaches being proposed for DEEs, we focus on strict and minimal implementations of Trust Layer 1, but allow for rapid, vigorous, and innovative evolution of Trust Layers 0, 2, and 3. This approach is essential for making the entire scheme achievable, and organic.

IV. LAYER 0: DEE RESOURCES AND ZERO TRUST

Zero trust. In simple terms, zero trust means no reliance on network security to provide the security properties of the signaling system and the applications that run on it. This is based on the assumption that the entities in a DEE are often hyperconnected, sometimes only intermittently connected, and connectivity is difficult to discern and control. The model must identify the protected resources, and account for how each entity interacts with them.

In a DEE, resources include:

- Data stored in some component of the ecosystem.
- Controls that can actuate functions of an element of the system. These can include energy resources as well as computing and communication resources.

Resources are organized into devices (machines), applications, including virtual and composite devices consisting of several devices that appear to provide single points of control or sources of data. Resources can be provided by web or cloud services that are more usefully characterized by their APIs and other service descriptors.

Several other entity types are part of a DEE, including:

- Device-based apps with resources that include authorization mechanisms and controls for other resources.
- Cloud-based apps and services with resources accessed through APIs, including:
  - event data
  - collections of sensor data
  - signals that used for energy pricing, discounts, and real-time availability.
  - up-to-date system status information
- Composite devices such as sensor arrays, or composites of digital twins for physical devices.

The system provides provenance and authenticity for data and commands, and a trusted way to verify those claims for all parties involved in any data exchange. The internet has no built-in capability for supporting verifiable claims about data authenticity, provenance, authority, or trustworthiness.

V. LAYER 1 SECURE MESSAGING

Commands, requests, and responses are encapsulated in secure messages that can originate at the DEE *application level*, consistent with a zero-trust model. When a message is sent, it includes sufficient information for the receiver to:

- Verify the provenance (originator) of the message.
- Verify that the message has not been illicitly modified.
- Assure that an illicit actor did not reply to a message.
- Verify that the sender has the explicit authority to send the specific command or action request.

Means of assuring these properties depend on the use of cryptographic keys associated with the legitimate originators of the messages. The DEE therefore relies on (trusts) the means of distributing or establishing the requisite cryptographic keys, and the means of using them to provide the assurances for the integrity of these messages. Key management for a distributed, heterogeneous system is provided by a subsystem that has its own trust model described below for layer 2.

Security associations. Each entity in a DEE maintains a list of security associations, which is a list indexed by the identities of all the entities that the device might be expected to interact with. Each entry of the list minimally includes a unique principal identifier and a shared symmetric key. Message integrity is

assured by robust message authentication codes using keys derived from the shared key.

Persistent data integrity. Message integrity and provenance mechanisms validate the content and the sender, which be a specific device or instance of a software application and not merely a network address. However, the data may have originated earlier from yet another device. Therefore, the trust model provides assurances for persistent data integrity and provenance by using a persistent digital signature using a public key, or in the future using a keyless signature using a trusted blockchain [4].

Rich identity. Underpinning mechanisms for ensuring authenticity, provenance, and authority for commands and data, we need trustworthy mechanisms to identify devices, applications, and human and AI actors, for every identity in a DEE that anyone relies on. Rich identity entails identifiers uniquely associated with an entity, but also attributes, such as properties, qualities, and features of an entity. These attributes need to be authoritatively assigned and verifiable.

Policies. Automated decisions in a globally decentralized and distributed energy system are determined by sets of rules that we refer to as Policies. Policies can be very simple and implicit, or they can have several layers, requirements, options, conditions, exceptions, and references, and they can include internal data references, including time, or system status. Critical decisions can be submitted to AI evaluation – with access to additional data – to determine if a referenced action is safe under current conditions. In a DEE, policy rules support rapid, low latency actions while flagging rarer anomalies that may require deeper evaluation. Policies can be centralized and common among all elements of a DEE or decentralized and specialized for different applications and subsystems. Heterogeneous policies require transparency so that visibility, traceability, and accountability can be enforced.

Trusted assertions: Given that commands, action requests, identity and authority need to be validated, the Trust Management Infrastructure needs to provide means for users to validate statements like

- Entity X belongs to domain D and has IPv6 address (FE80:CD00:0000:0CDE:1257:0000:211E:729C)
- Entity E is permitted to use Interface A with resource R
- Entity X controls resource R
- Entity X has property P

Assertion types that will become increasingly sophisticated and detailed. Properties can include:

- Alternate names and identifiers
- capabilities
- credentials
- compliance assertions
- group memberships
- authority metadata
- permissions
- rights
- additional metadata that can affect decision making in an automated IoT system (see Policy, below)

We implement simple assertions as bindings where an identity value and one or more attribute values are hashed together, and the resulting value signed by a certificate authority or entered into a database such as a blockchain.

Trusted assertions are used in security associations, a Layer 1 Trust mechanism. The integrity of those assertions is provided by assurances in level 2 and higher.

Layer 1 messages use an encapsulation protocol whereby commands, responses, data, etc., are encapsulated in a security wrapper whose elements provide the means for assuring the provenance, privacy, confidentiality, authenticity, and authority of the message.

The formats and optional content for Security Associations will NOT be interoperable. However, an Abstract Data Type specification is provided. Compliance with the abstract data type is required and close compliance with recommendations is encouraged to simplify deployment administration.

VI. Trust Layer 2 mechanisms

DEE devices behave and operate differently than typical WWW entities. It is common for previously unidentified, even anonymous devices to legitimately show up in WWW use cases. These kinds of events generally should not appear in DEE deployments. As a new device is added to a deployment, it usually happens intentionally in ways that can help its trustworthy introduction into the environment.

Consider a home IoT deployment including a solar array with a controller/inverter, water heater, HVAC systems, auto charger etc. and trusted controllers and interfaces to various cloud services such as a smartphone app. The app can have various administrative privileges. Privileges include updating Security Association tables for various the devices in the existing deployment. The event of adding a new device can use the app to pair (using Bluetooth, or preferably NFC) the app instance with the battery device.

Layer 2 trust mechanisms for maintenance of SAs need not directly interoperate in our model, and for different parts of a DEE deployment they can include:

- Supervisory entities with privileges allowing them to remotely update the SA tables of devices.
- PKI based authenticated key establishment (AKE) using Cert chains.
- AKE using keyless signatures and trusted assertion and attestation ledgers (trusted blockchains).

The blockchain approach is more scalable with simpler mechanisms for revocation and update. PKI can be used to provide credentials for authorities who update ledgers. FIDO (https://fidoalliance.org/passkeys/) and Apple passkeys can be used for identifying and authenticating authorities who may update credential ledgers. The keyless signature approach can

also provide for a systemic means to resist future quantum computing attacks.

VII. TRUST LAYER 3

A. Security Policies

Automated decisions in a globally decentralized and distributed energy system can be determined by sets of rules that we refer to as Policies. Policies can be simple and implicit, or can have several layers, requirements, options, conditions, and exceptions. They can include internal data references, including time, system status, etc. Critical decisions can be submitted to AI evaluation to determine if a referenced action is safe under current conditions.

Over time, policies will be increasingly sophisticated and designed to enable better security, performance, and optimization, supporting rapid, low latency actions while flagging rarer anomalies that may require deeper evaluation.

Policy can be centralized and common among all elements of a DEE, or it can be decentralized and specialized for different applications and subsystems. Policy can determine:

- What an entity does operationally regarding maintenance of trust, including taking part in both local and systemic recovery from compromise
- How robustly the entity performs trusted actions and avoids bypass of assurance mechanisms.
- How robustly the entity resists nefarious actions.
- How the entity can be updated to repair flaws in implementations or to provide new implementations required to address new threats.

B. Compliance and robustness rules (CRRs)

CRRs name policies grouping them for different types of devices and entities, providing a means of rating the overall security and trustworthiness of the entity. They also describe:

- Required, specific, interoperable rules and actions such as the layer 1 message integrity actions.
- Required rules and actions chosen from an option list such as approved means for establishing SAs.
- Optional rules and actions for optional capabilities that an entity may support.

Device robustness classification. As the number of device and other entity types in a DEE can varies widely with different vulnerabilities and scope of operation, we categorize robustness in several dimensions including by trust layer, function, scope, and ability to affect other entities.

Event and action logging and monitoring, and administrative interoperability. Part of the overall trust model needs to include systemic accumulation of data that can be used to monitor security performance and evaluate anomalies that indicate illicit activity and detect acute attacks. This area is crucial to what we call administrative interoperability allowing a DEE to benefit from broad participation, while preserving confidentiality.

C. Renewability

A DEE is generally highly dynamic with new entities appearing, and properties, status, and attributes of participating entities changing often. This requires adaptability across signaling, security associations, and policies – in addition to effective and instantaneous revocation of credentials, security bindings, and certain system capabilities. As we discover how illicit activities affect a DES, we will upgrade, and make it easy for entities to adopt more secure and appropriate options without undue disruption.

D. The TEIA alliance

TEIA (https://www.trusted-energy.org) is an alliance devoted to establishing an adaptable, interoperability standard applicable to DEE and SDS in general.

Based on TEIA, companies deploying distributed energy systems can determine the best path to deliver energy, provide for multi-party transactions, recover from hacks, and diversify intelligent network interactions, database lookups, and ultimately support complex software-defined networks.

Such a standard can permit energy capacity to expand even without an expensive infrastructure revamp of physical plants. TEIA can promote a vibrant, responsive energy market based on reliable, real-time and historical data, and allow for investment in new physical plants for generation, storage, transmission, and distribution.

Specifically, using TEIA standards, DEEs can:

- Immediately find and safely engage other components that complement a service, technical or business function, making any one component more valuable (e.g., storage for variable production).
- Get immediate credit for stakeholders sharing components: a buyer for energy, credit for using renewable energy, or remuneration for data.
- Using readily available data, optimizing the design and introduction of specific components
- Ensure compliance with evolving mandates for cooperation in the ecosystem including data regulations and compliance.
- Accomplish the above while assuring preservation of privacy, confidentiality, safety, and reliability.

A high-integrity energy signaling system in TEIA records conservation, carbon capture, and carbon offset events and provide the basis for tokenization and compensation for these efforts. Ultimately an active and dynamic energy market can emerge, connecting large and small participants [5].

VIII. REFERENCES

[1] https://www.energy.gov/oe/articles/smart-grid-introduction-0
[2] https://spectrum.ieee.org/packetized-power-grid
[3] https://digitalprivacy.ieee.org/publications/topics/what-is-zero-trust-architecture
[4] https://internetinitiative.ieee.org/newsletter/july-2017/persistent-protection-of-data
[5] https://www.wri.org/insights/6-ways-remove-carbon-pollution-sky