intertrust®

White Paper

Intertrust XPN

Solving for data trust in IoT networks

End-to-end persistent protection with Intertrust XPN™

Contents

The problem with IoT networks

IoT networks are optimized for cheap devices—not trust or safety.

As the number of sensor and actuator based "things" connected to the internet explode, so do the challenges associated with them. This has led to dozens of protocols for wide, neighborhood, local, and personal area networks, most primarily designed and implemented to address these challenges.

Small size, low power consumption, and inexpensive hardware drive the optimization of these devices. And, in turn, these factors determine the network parameters. Because of this, the devices tend to have low compute requirements and almost always have low data throughput requirements. Accordingly, they usually are intermittently connected rather than fully connected. They are also intended to be secure, but security often takes a backseat to minimizing cost, reducing power consumption, and extending battery life.

Security challenges are further exacerbated because IoT devices tend to be highly distributed, decentralized, and physically available to attackers—creating a large attack surface. Particularly for consumer IoT devices, another issue is that many manufacturers may not have the incentive or capabilities to build in effective device security. This low threshold leads to increased opportunities for attackers, and a higher probability of successful attacks.

Many IoT devices and systems manage mission critical real-time systems such as oil and gas pipelines, electricity grids, semi-autonomous vehicles, and building systems. Because of the efficiencies they introduce, these "professional" IoT systems are spreading at an ever increasing rate, making them an ever increasing target for cyberattacks. As of the time of writing, the US Federal government lists 16 critical sectors of concern on its Cybersecurity and Infrastructure Security (CISA) web site: https://www.cisa.gov/critical-infrastructure-sectors.

Because of the high probability of cyber attacks and dangerous impacts, the risk needs to be actively managed. Mitigations outlined in security frameworks such as PSACertified.org, the NIST Cybersecurity Framework[1] and ISO27001[2], offer best practices, control catalogs, and processes to manage and minimize the residual risk of fielding IoT systems.

Inadequate network protocol security

While security frameworks are very helpful, we need to understand that many of the protocols used in the IoT today simply were not designed to help mitigate today's threat model. This model now includes nation state attackers waging cyberwar and well funded and technically adept criminal gangs operating under the protection of aggressor nation states. The Dark Net was also not accounted for, and how to mitigate against this powerful marketplace for buying and selling everything from exploit kits, to passwords, to entire botnets, all to the highest bidder.

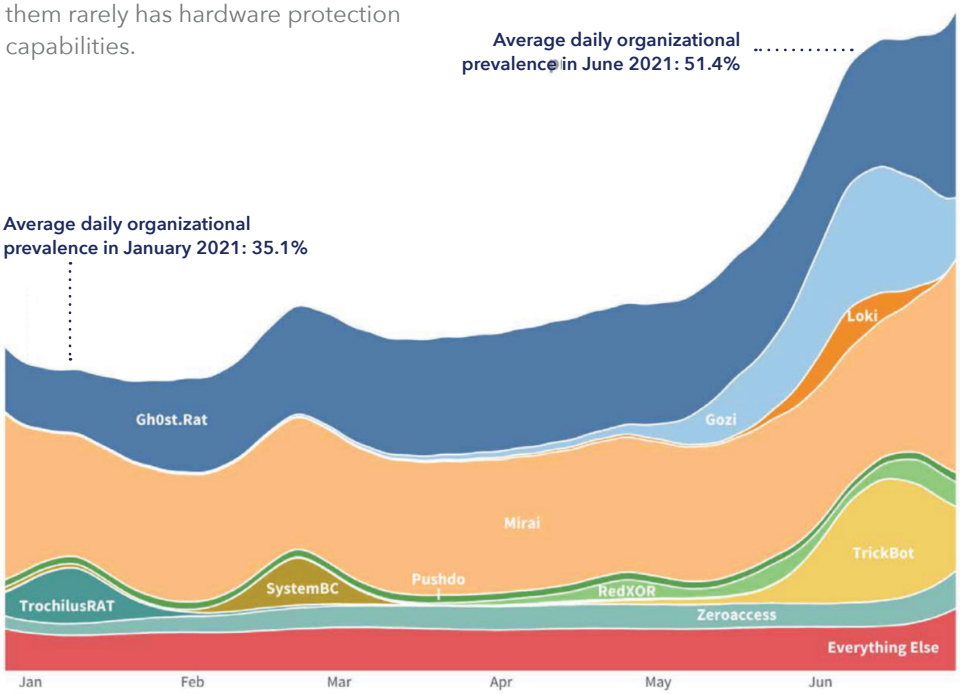
We also did not envisage the widespread use of Bluetooth in hospital systems, 802.15.4g based mesh protocols in utility Advanced Metering Infrastructure (AMI), or home security systems based on Zigbee. All these communication protocols have serious security vulnerabilities [3].

While security protocols such as IPSec and TLS have been deployed as part of these protocols' IP networking stacks, they have proven inadequate to address the threat model—as demonstrated by the almost daily examples of deeper and more widespread breaches and compromises.

Many network protocols don't even bother with the mutual authentication features of IPSec and TLS or even implement public key cryptography essentials. Rather, they seek to secure the network link layer with four basic security services: access control, message integrity, message confidentiality, and replay protection using nothing more than shared secrets via the AES cipher.

This approach underpins many Advanced Metering Infrastructure (AMI) systems. There are also networked protocols in widespread use that have no intrinsic security and the hardware running them rarely has hardware protection capabilities.

For example, the CAN bus in a vehicle does not have any notion of identity for component communication, never mind authentication. Modbus is widely used in industrial settings for manufacturing and Supervisory Control And Data Acquisition (SCADA) systems that form the mission critical backbone of most utilities. Yet, the current Modbus protocol does not have authentication, only an IP address and function code are needed to establish sessions.



Source:
Fortinet Global Threat Landscape Report, August 2021

Intermediaries: hubs, routers, headends: good hunting grounds for middle men

The spectacular growth of Mozi and other botnets targeting the IoT brings us a cautionary tale. These botnets not only operate at hyper scale, but they have automated reconnaissance, vulnerability scanning, exploitation, and ultimately ownership of these intermediate (and cheap) IoT machines. As such, they continue to grow at an incredible rate: 46% between January and June 2021, according to Fortinet. [4] Botnets have also developed cloaking capabilities,meaning that the true growth of compromised hosts is far larger. Once a machine is compromised, all the traffic flowing through it can be viewed, and modified. Botnets use traffic analysis to develop a pipeline of new victims to continue their automated worming growth. The attackers' lateral movement is facilitated in IoT networks because of the many-to-many relationships between machines.

Many heterogeneous networks

The challenge of network security in the IoT is very different from that of e-commerce over the consumer internet. In the relatively simple use case of a shopper using an application (typically a browser) to connect to a server over a flat, consistently connected point to point network with pre-provisioned certificates for those servers, this has largely been solved with TLS.

Because it works so seamlessly and easily, this solution has been blindly implemented in the IoT. The trouble though, unlike e-commerce over the consumer internet, the IoT is multidimensional with many more challenges and constraints:

- The hardware is very inexpensive compared to smartphones and laptops
- Devices are intermittently connected with no persistence
- Devices are highly distributed with even less physical security than a smartphone / laptop, creating a much larger attack surface
- Many multiple topologies and networks are used
- Often the edge network used is a mesh-based network and device data is collected at a headend. The data from that headend will then traverse through a communication provider network before the data lands at the actual cloud-based IoT management system being used.
- This network fragmentation requires technical and administrative bridging between operational technology (OT) and information technology (IT) divides

The overly simplistic paradigm of e-commerce when applied to IoT misses a fundamental truth: e-commerce is a 1:1 relationship between the shopper and the vendor. It simplifies the governance model, which is well known and covered by a web of national laws, societal norms, risk assessment, and coverage by credit card firms. It is ultimately a model where a single device connects to a single (instance) of a server.

In the IoT where the paradigm is many to many, how could this possibly work? Typically, IoT use cases combine data from many sensors that, when collated together, provide a detailed time series based view of the ground truth in the physical world that is then used by many applications. For example, a typical energy company started with implementing Advanced Meter Reading (AMR) systems for their smart grids.

However, it became evident that while monthly meter reading was important, the data flows that AMR could provide were insufficient for applications such as proactive and real time balancing of the grid with dynamic Time-of-Use pricing, time shifting of peak loads and even load shedding applications. Accordingly, most energy companies have moved to AMI which provides a more timely and granular data stream.

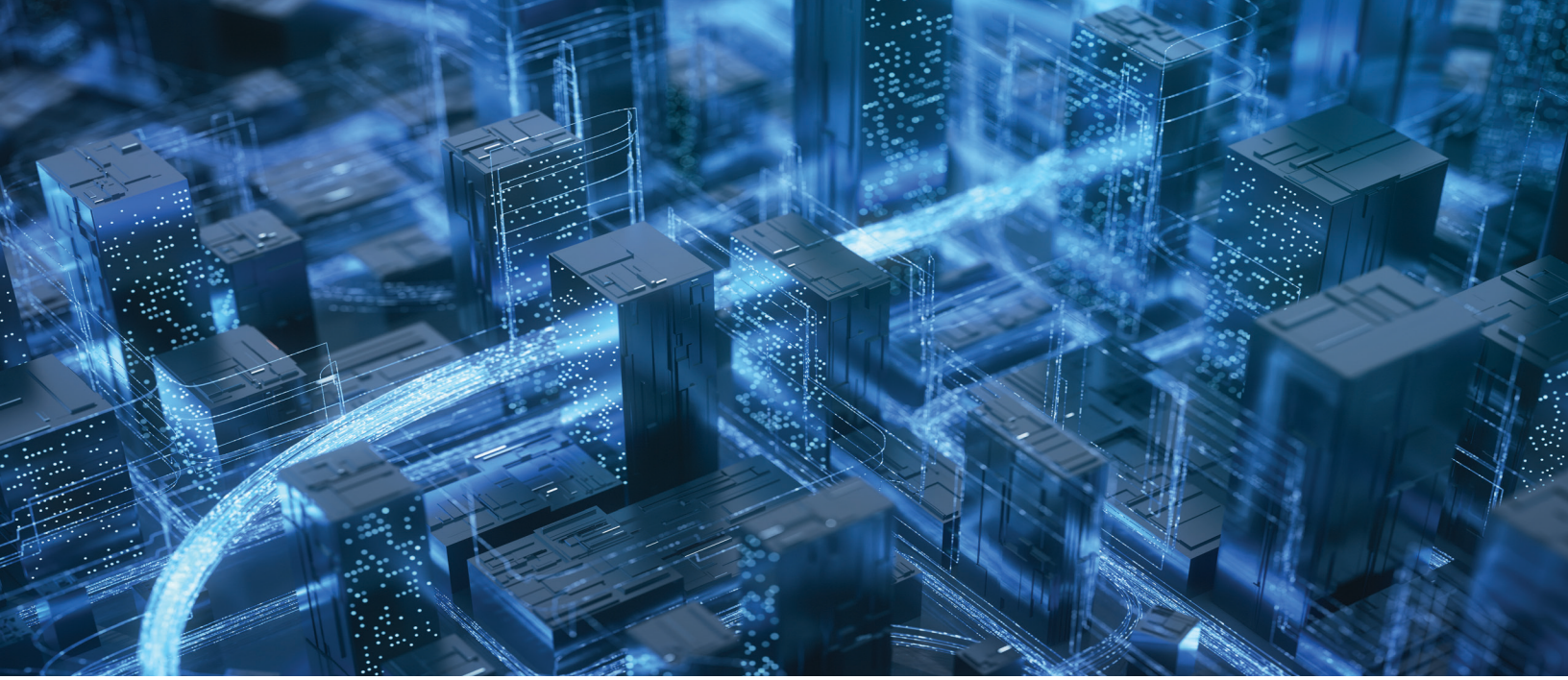
What's more, e-commerce has no real concept of a forward link where authorized commands are sent to actuators. How can this be managed in a fully authenticated, authorized framework? Furthermore, how can such a framework be achieved in a world of (semi) autonomous machines that make decisions much faster than humans can intervene?

IPSec generally, and VPNs (virtual private network) in particular, suffer all these problems and then some. Unlike the application level protocol at which XPN operates, IPSec runs at the network level. It breaks when it crosses network topologies, and in many mesh systems, it is not a viable option at all. Worse, it requires detailed and meticulous configuration and doesn't behave well when new machines are introduced, moved, or modified. Maintenance becomes a major headache.

IPSec suffers from further complications in a heterogeneous network environment– TCP meltdown. TCP meltdown occurs when you stack one transmission protocol on top of another, such as a TCP tunnel transporting TCP traffic inside it. The underlying layer may detect a problem and attempt to compensate, and the layer above it then overcompensates.

This overcompensation causes delays and problems with the transfer of data. This is a common occurrence, difficult to predictively guard against and often a challenge to troubleshoot. Simply turning off the VPN will make data flow smoothly and appear to fix the problem, but of course, all that's been achieved is removing the basic protection of the network, making it even more vulnerable

For more, visit: https://openvpn.net/faq/what-is-tcp-meltdown/



Key spaces are fragmented and siloed

IoT networks are deployed today with different trust and threat models. These networks are fragmented and work in isolation. The resulting separate and fragmented key spaces are designed (ostensibly) to be more resilient to attack, but in fact they only offer a splintered view of all the data needed for true resiliency.

An example is in the home. The U.S. Energy Information Administration says that the U.S. residential sector accounts for 21 percent of all energy consumption and is responsible for 20 percent of the country's carbon emissions[5]

The fragmented nature of the different key spaces in the disparate networks used means that the home network is kept hermetically sealed from the industrial AMI network used by the electrical utility. That network is also separate from the network used by the electric vehicle being charged in the garage.

The industrial technology consumer chasm

To enable energy utilities to effectively incorporate homes into virtual power plants (VPPs), we need consumers to trust that their data will be reasonably protected. Currently, we segment our networks to offer better trust and security. Because of the simplistic link layer security design inherited from e-commerce, we don't have an effective risk-adjusted network design to bridge the chasm between our bulkheads of industrial technology, enterprise IT, and the consumer-oriented home. We need a new approach to bridge these environments and further meet consumers' trust needs.

Explicit Private Networking and data trust for IoT

Intertrust XPN™ solves the many-to-many challenge of IoT networks.

Intertrust Explicit Private Networking (XPN) makes use of the fundamental elements of modern cryptography that are known to be resilient in the face of even the most advanced attacks. We use, for instance, the Diffie-Hellman Station-to-Station protocol for XPN-PDP-key establishment, adapting it to meet the challenges of the IoT's many-to-many relationships and optimizing it for use as a messaging protocol.

XPN does more than protect streaming sessions of data in a simple client-server topology. Not only does it protect data in transit, it also protects data at rest and in use in hostile environments. Data remains protected because XPN data is only encoded and decoded in a protected processing environment.

Leveraging trust in endpoints—at the edge and in the cloud

Connected devices are the source of essential sensor data flows. They also act as actuators that make machines do things, for example turning off large electricity loads such as air conditioning at peak times for the electricity grid. Therefore maintaining security and trust is of utmost importance.

The intersection between operational technology (OT) and information technology (IT) systems and IoT gateways in field area networks (FANs) are critical exposure points for abuse by attackers. As noted, many networks have inadequate security and cannot be trusted. Accordingly, zero trust has become the preferred network security model.

The solution used by Intertrust XPN is to leverage trust in endpoints, both at the edge and in the cloud. Similar to IPSec / Virtual Private Network (VPN) technologies in its aspirations, XPN protects data as it passes through untrusted gateways and networks because the end points are trusted. This trust is leveraged to protect the data as it travels over data networks to the cloud.

XPN scales particularly well in complex VPP and distributed energy resource (DER) applications because these applications require distributed trust and that is a strength of XPN. Prior to XPN, enabling distributed trust has been difficult because all the participating energy devices, the networks they operate in, and their managing entities exist in different Public Key Infrastructure (PKI) key spaces. This increases the complexity of security coordination between the different partners.

With XPN, trust is no longer dependent on only protecting data in the "pipe" of the original network segment. Trust is extended from when a sensor actually generates the data through to the ultimate consumption of that data. XPN offers the true end-to-end distributed trust essential for VPP applications.

XPN incorporates these essential services:

- A True end-to-end overlay of trusted data
- Persistent data protection
- Commands and authorization
- Edge-trusted audit logs
- Communications with uncompromised entities: The Entity Attestation Token (XPN-EAT)
- Digital twin and firewall for brownfield devices and systems

A true end-to-end overlay of trusted data

Persistent data protection

The IoT has a wide attack surface that includes devices likely to reside outside of the typical defensive perimeter of firewalls, intrusion detection/prevention systems and the like. Worse, the field area networks where many reside are often implemented using weak network protocols. When there is decent communication protection, the protection often terminates at a VPN or TLS gateway, leaving the data exposed as it travels onward. As a result, attackers can access IoT and other internal systems with seeming impunity. The Mirai botnet's rapid growth has been enabled by such weak links in the security chain.

XPN's Persistent Data Protection (PDP) solves this problem by assuring data integrity, authenticity, and optionally secrecy protection, both at rest as well as in transit, even as it travels across trustless gateways and networks. XPN signs, and, optionally, encrypts data when it is generated on a device. The same protection is provided for data sent to a device, for example, when commands are sent to an actuator. This unique PDP protection layer can co-exist with network security measures such as VPN. Unlike VPN protection, the XPN PDP layer continues after the data exits the VPN pipe and will even persistently protect data at rest.

XPN PDP requires an XPN client installed on each end point. The XPN client is configured to ensure that sensitive processing is only done in a Protected Processing Environment (PPE) on the end point and sensitive cryptographic key material is stored only in secure storage. The device software should be digitally signed so only known good software will be running on the end point. All of this is verified by the Trusted Boot process at startup.

The XPN client relies on the secure foundations of TEE (Trusted Execution Environment), Trusted Storage, and Boot to ensure the resilient protection of data. These foundations are enabled through a combination of PKI toolsets and integration with the chip's hardware security, particularly those that are PSA Certified.

As soon as the digital data is generated by a chip, the XPN client accesses the buffer with the data and signs it using the XPN keys associated with a particular trusted key space. Signing ensures the authenticity of the data originating from the specific end point and, through the use of a SHA-3 hash, ensures the data's integrity throughout its journey. Optionally, the XPN client can also encrypt the data to maintain data secrecy. Since many IoT devices are performance and resource constrained, XPN leverages AES symmetric key ciphers. These ciphers are agreed upon between the client and server using the Diffie-Hellman Station-to-Station protocol, so secrets need never be distributed.

XPN packages contain the routing data for the consuming server. The consuming server is an XPN end point included in Intertrust Platform (more at https://www.intertrust.com/platform/). Once the server receives an XPN package, the server performs a HMAC verification to validate the authenticity and data integrity of every data packet in the package. If encryption was applied, it will decrypt the data. Further distribution, collaboration and sharing of the data is managed using other Intertrust Platform features.

Commands and authorization

Perhaps even more important than safeguarding the transmission of sensor-generated data to data services in the cloud is protecting the commands sent to actuators that drive and control machines at the edge. These messages send near real time signals to command machines used in critical infrastructure to, for example, turn a machine off if load needs to be shaved or to a smart thermostat to reduce the temperature in a home as agreed to by the homeowner and their energy provider.

Implemented correctly, commands can securely bridge the divide between industrial energy systems and consumer devices in a home. VPPs can finally bring homes, which consume 20% of energy and contribute even more to emissions, within the energy management fold in a trusted and secure manner.

Done poorly, VPPs represent yet another vector of attack into the home and ultimately on our energy distribution systems.

Intertrust has developed highly resilient trusted distributed data and device systems for decades. Applying lessons learned over these years, we developed XPN technology and the PDP messaging format to be highly secure. By leveraging rich authorization descriptions combined with protected processing in endpoints, XPN acts as the foundation for a command infrastructure that is extensible, flexible and Turing Complete.

Edge-trusted audit logs

Audit logs have a dual purpose, baseline establishment and forensic analysis. Together, they are a vital part of the trust equation, ensuring that disputes among parties can be resolved, and historical analysis can be done with accuracy and integrity.

Accordingly audit logs can't be left exposed and vulnerable to modification by unauthenticated and/or unauthorized parties. XPN assures trust in audit logs by recording them at the edge in a ledger that hashes log entries at a polling interval configured by the system owner. Crypto hashes make such data immutable and fraud or modification is easily detected by comparing the appropriate hashes. Tables of hashes are protected with digital signatures and availability is assured by distributing ledgers and ensuring they sync in a timely manner.

Communications with uncompromised entities

The Entity Attestation Token (XPN-EAT)

Owners of IoT applications such as VPPs and their cloud service and IoT platform partners are expected to provision and onboard devices in the field at massive scale. The problem is, when onboarding, can they determine if these devices are trustworthy or compromised bots?

VPP and other application implementers need assurance the devices they work with are in a known good state. To do so, the device must attest to their state in a trustworthy manner to properly "introduce" itself to a service. This is done through entity attestation. Entity attestation claims include data such as the device's ID, software version, and hardware version. The Trusted Execution Environment generates an entity attestation as a "trust signal" and the attestation is signed to ensure data integrity and authentication.

The XPN client software installed on a device creates an Entity Attestation Token (EAT) conformant to IETF Entity Attestation Token (EAT) specification [6]. Intertrust Platform acts as a relying party to process the attestation result which is then used to make policy decisions, such as whether to grant a device access to certain resources. EAT is a critical element of the NIST IoT Cybersecurity Capability Core Baseline (NIST 8259A,)[7] and is endorsed by PSA Certified.[8]

Because of the wide adoption of the IETF EAT standard, XPN works with the vast majority of modern IoT devices, allowing providers to rapidly onboard IoT devices in a highly trusted fashion. Device attestation is a critical element of NIST 8259A, and one that device makers and service providers find difficult to implement. Through the combination of EAT support and other trust features, XPN Intertrust is uniquely positioned to execute on the promise of highly distributed trust in IoT systems.

Digital twin and firewall for brownfield devices & systems

Not all connected devices have the necessary hardware and software capabilities to protect themselves. Legacy brownfield systems, such as many SCADA systems used in industrial systems, have limited or no security capabilities. Exposing these critical infrastructure systems to the internet without proper protection capabilities is very problematic since they can be easily exploited. The best practice today is for these systems to be deployed in protected network segments with limited or no access to the internet. However, the utility of these connected devices is diminished when a large proportion of systems are kept effectively offline.

XPN offers a solution. First, legacy systems need to be tightly segmented into safe zones, with a firewall configured to only permit traffic to / from a singular trusted end point in the cloud. In XPN, this firewall is a digital twin. An insecure brownfield device only has permissions to connect to its digital twin in the cloud. By creating an explicit private network connection between a legacy system and this single digital twin run in Intertrust Platform, the benefits of connected systems can be realized while greatly reducing the security risk. The digital twin itself is strongly protected with robust perimeter defenses, a proper Root of Trust, software partitioning/ protection, and, using the attestation services mentioned above, running known good software and all connected devices properly verified.

The digital twin will be an exact digital replica of the device holding all the data the original device has generated. It can fully participate in an IoT network and provide all the benefits of the IoT: real time dashboards, data analytics, predictive/ prescriptive and prognostic analytics, and the generation of data for use by machine learning models and AI algorithms.

Using Intertrust Platform's secure execution environment along with the Platform's strong identity authentication and data virtualization features, sensitive data can be handled with a greatly reduced risk of it being copied or otherwise exfiltrated. Governed collaboration among multiple parties that may only have limited trust between them is also possible.

To further reliability and cybersecurity resilience, the digital twin also runs a reference monitor to initially develop a baseline of a device's known good activities. It then continually monitors the device to detect any anomalous indicators which may mean a device has been compromised. It can quickly and easily inspect, quarantine and, if necessary, remediate a device.

The XPN digital twin for brownfield devices feature provides utilities with the ability to securely incorporate a wide range of legacy systems into real-time smart grid systems.

A new level of data trust

XPN ensures data from IoT devices can be trusted, and this trust can be maintained throughout its journey, including when commands and other data are sent to actuators. XPN provides the missing element in securing machine data and can be extended further to peer-to-peer communications and value exchanges. Through these measures, XPN creates a significant layer of distributed trust for VPPs and other IoT applications.

Endnotes

1 NIST Cybersecurity Framework https://www.nist.gov/cyberframework

2 ISO/IEC 27001 and related standards

3 The 5 Worst Examples of IoT Hacking and Vulnerabilities in Recorded History

4 Fortinet Global Threat Landscape Report, August 2021

5 Home Energy Use, Center for Climate and Energy Solutions

6 ETF RATS EAT https://datatracker.ietf.org/doc/draft-ietf-rats-eat/ (see example table below)

7 NIST 8259A: IoT Cybersecurity Capability Core Baseline https://csrc.nist.gov/publications/detail/nistir/8259a/final

8 PSA Certified White Paper on Device Attestation https://www.psacertified.org/app/uploads/2020/02/PSA_Certified_Entity_Attestation_Overview_Whitepaper.pdf

Example of some common claims used by Entity Attestation Tokens (EAT).

Claim Name	Claim Description
Unique identifier	Similar to a serial number. Universally and globally identifies each individual device.
Manufacturer and model	Identifies the manufacturer of the chip and/or the finished device.
Installed software	Lists the software present on the device including versions.
Device boot and debug state	Indicates if the device booted securely, whether debug mode is enabled, and debug ports disabled.
Geographic position location	For example, based on GPS, WiFi, cell tower or some combination. Only available if the device has location features.
Versions, measurements and/or integrity checks of running software	Measurements of running software, usually hashes of the code, are provided for comparison against known-good-value to help detect tampering.
Nonce	Cryptographic quality random number generated, sent by the server and returned as a claim to prevent replay and reuse.

intertrust®

Building trust for the connected world

Learn more at: intertrust.com/platform
Contact us at: +1 408 616 1600 | dataplatform@intertrust.com