intertrust®

Creating secure IoT device identities

White Paper

Intertrust PKI

Contents

Executive summary

The Internet of Things (IoT) is radically transforming how we work and how we live. However, with this transformation comes increased risk.

IoT applications are extremely vulnerable to cybersecurity attacks as they control both data access (often personal or sensitive) and connected devices. Without proper security, IoT technology will not grow as projected nor live up to its true potential in the marketplace. This paper focuses on how to create secure IoT device and sensor identities, fostering data access and interaction across devices in a trusted ecosystem.

Device identities are data structures consisting of various cryptographic credentials and assertions that define what the device can and cannot do during its lifecycle. The process of assigning a device identity is called provisioning. Device identities can be provisioned on the factory floor at the time of manufacture, or in the field when they are installed for the first time. Certificate authorities, which operate managed public key infrastructure (PKI), are well suited to create and distribute device identities.

IoT opportunities and challenges

In the private sector, smart home IoT devices like thermostats, washing machines, baby monitors, and door locks bring new levels of control and convenience for the homeowner.

In the medical sector, devices increasingly connect doctors, patients, and caregivers in new, interactive ways and improve overall patient health, diagnosis and outcomes. In the industrial sector, IoT applications can minimize downtime in wind turbines, drive manufacturing efficiency in oil rigs, optimize supply chains in autonomous vehicles, and provide improvements for many other applications. The possibilities are endless. In 2018, the global market for the Internet of Things (IoT) reached $130bn. This is projected to reach $318bn by 2023 at a compound annual growth rate (CAGR) of 20%[1]. According to IHS, more than 75 billion IoT devices will be online by 2025[2].

The proliferation of connected devices gathering data and controlling things is disrupting today's market at an accelerated pace. For example, Nest Labs, which was founded in 2010 around its smart thermostat, was acquired by Google in 2014 for $3.2bn, and it has continued to grow and add new products.[3] In 2017, Nest generated $726mn in revenue capturing over 75% of the smart thermostat market[4]. This has caused conventional thermostat vendors such as Honeywell (now Resideo), to adapt their market strategy and business approach.

Research has shown that IoT can improve efficiencies in industrial operations by lowering costs and improving quality. According to Forrester research, 52% of manufacturers report that IoT helped them optimize their supply chain; 50% reported that IoT could mitigate losses, and another 50% reported that IoT would improve customer service[5].

Yet, for all its promise, IoT technology is not without its difficulties and challenges. Early adopters of IoT technologies encountered significant barriers to adoption[6]. Security tops the list of major concerns, holding back 59% of those professionals from proceeding[7]. According to a study by the Ponemon Institute, 63% of CISO's believe that participation in IoT will increase cybersecurity risks in the future[8], and that over 80% of professionals predict that their organization will experience a catastrophic data breach caused by an unsecured IoT device.

The industry is still grappling with how to secure IoT deployments. A comprehensive security approach takes into consideration different technologies, policies, and processes. Organizations interested in exploring security standards for IoT can refer to (NISTIR) 8222[9], Industrial Internet Consortium[10] and IoT Security Foundation[11]. These specify security frameworks for IoT and tell how to assess and improve their ability to prevent, detect, and respond to security incidents.

In this paper we address a complex fundamental component of securing IoT: how to give devices and services secure identities so they can interact securely.

Importance of trusted ecosystems and mutual authentication

Behind every popular IoT device – whether it's a home thermostat, continuous glucose monitor, connected car, or sensor for critical infrastructure – is a sophisticated backend service which enables IoT devices to interact and access other devices and services.

For most IoT deployments, a trusted ecosystem of authorized devices and authorized services is the recommended approach. In a trusted ecosystem unauthorized devices or services are not allowed to interact with authorized devices or services. This prevents unauthorized access to the critical services and data of an IoT device. If this protection was not present, the consequences could be dire, especially where services are responsible for issuing commands that prompt a device to act in a certain way. Compromised devices could also report false data to the service, with potentially disastrous results. For example, if a service collecting data from wind turbines in an offshore wind farm is fooled into getting data from a rogue device that pretends to be a wind turbine, the safety of the entire operation could be jeopardized, and power could be disrupted.

Besides the security ramifications, a trusted ecosystem lets vendors retain control over their markets by limiting the types of devices and services that can participate in these ecosystems. This, in turn, ensures that revenue streams are under control and enables a consistent level of quality and interoperability.

Establishing a trusted ecosystem is not possible without mutual authentication. This allows two entities to prove to each other that they are authorized members of a particular trusted ecosystem. The standard practice for mutual authentication is public key cryptography. Managing public keys properly is crucial and will be discussed in detail later in this paper.

How device identities function

Device identities are data structures that include information, which allows devices to participate in trusted ecosystems.

While mutual authentication is a baseline requirement, devices also need a unique identity. This allows it to perform many different types of cryptographic operations and describes what it is and what it is authorized to do. Figure 1 describes how a device identity is used throughout its lifecycle.

Although a single cryptographic key or public key certificate can suffice for simple applications, most applications require a more complex data structure that includes–metadata, authorization statements, and cryptographic credentials. A typical device identity is shown in Figure 2.

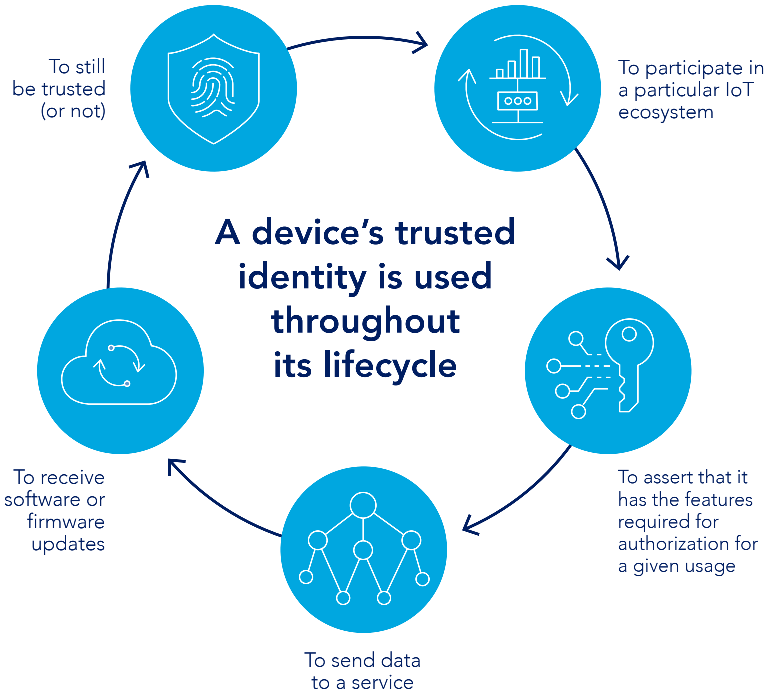

To still be trusted (or not)
To participate in a particular IoT ecosystem
A device's trusted identity is used throughout its lifecycle
To assert that it has the features required for authorization for a given usage
To send data to a service
To receive software or firmware updates

Figure 1.
Device identity lifecycle

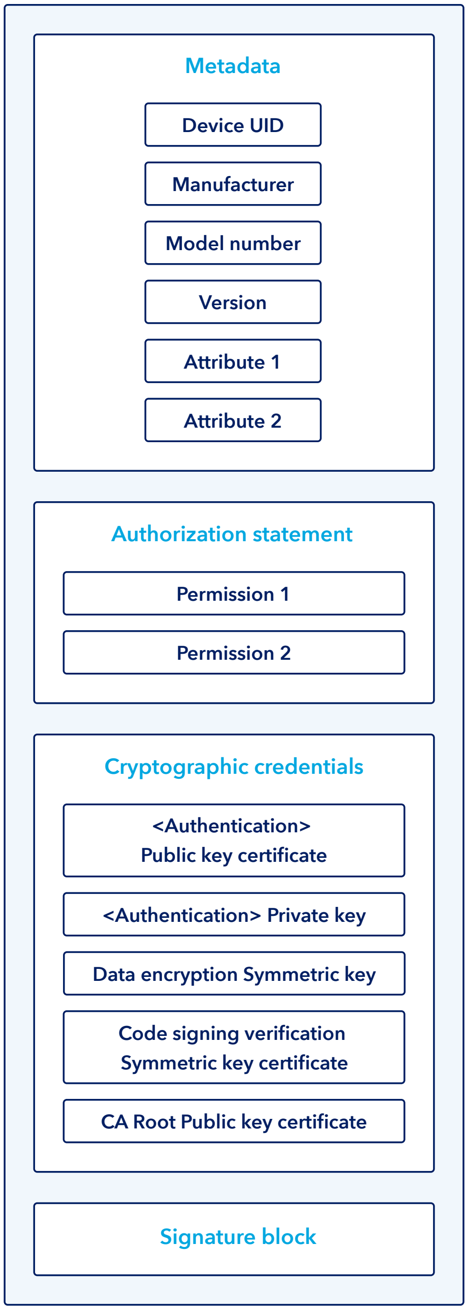

Metadata
Device UID
Manufacturer
Model number
Version
Attribute 1
Attribute 2
Authorization statement
Permission 1
Permission 2
Cryptographic credentials
<Authentication> Public key certificate
<Authentication> Private key
Data encryption Symmetric key
Code signing verification Symmetric key certificate
CA Root Public key certificate
Signature block

Figure 2.
A typical device identity

Metadata includes descriptive information on the device type, manufacturer, model and version number, and can also include attributes describing its functionality. For example, a camera's metadata might indicate whether it has the capability to shoot video, photos, or both.

Authorization statements are permissions that describe what the device is allowed to do. Some multi-functional devices might use only a subset of their capabilities for certain use cases. For example, a camera's video recording may be prohibited for legal reasons in some installations, but photography may be permitted.

Cryptographic keys: A device may need several types of cryptographic keys and certificates. For example, it might need keys to: authenticate to services, encrypt data, or verify code signatures. All certificates (cryptographic and authentication keys) will typically be tied to a unique root certificate issued by a certificate authority (CA). Some of the certificates in the associated certificate hierarchy might need to be included to verify the identity of the services the device interacts with.

Signature block: To prevent tampering, the entire device identity is protected with a digital signature.

Since the device identity can contain sensitive information such as private keys and CA root certificates, it needs robust protection. This is done by delivering the identity to the device over a secure, authenticated channel. Once on the device, the sensitive materials or the entire device identity will need to be stored securely; for example, in hardware backed storage.

PKI: A proven solution

Public key cryptography plays an important role in device identities. In any implementation of public key cryptography, it is important to have strict ways to create, manage, distribute, and revoke public keys.

For trusted ecosystems, it is important that device identities and specifically, the cryptographic keys they contain, are issued by a single source and tied to a unified domain. The standard way of doing this is through certificate authorities that manage a root key. This can be used to sign all the public keys that are part of that ecosystem.

A full-service certificate authority does the following:

- Generates and manages root keys
- Signs certificates- Revokes certificates
- Securely archives keys
- Offers disaster recovery services.

Running a certificate authority is complex. It requires specialized facilities, technology, processes and people.

Asymmetric cryptography

For asymmetric cryptography such as RSA, the private part of the key pair is extremely sensitive and must be protected carefully. Ideally, a private key would never appear in the clear in any system. For small scale deployments, having a simple password-protected private key is usually fine. But for enterprise applications, hardware security modules (HSMs) should be used to protect private keys at all times. HSMs are specialized appliances or peripheral cards and can do all of the necessary cryptographic operations in hardware without ever exposing the key in the clear.

Secure environment

Because of the sensitive nature of private keys, these HSMs should be located in a physically secured environment with limited access only to authorized personnel. Depending on the sensitivity of the keys, multiple layers of physical security might be needed in order to protect these systems. This might include security guards, biometric authentication mechanisms for authorized individuals and surveillance systems to monitor and record who enters and leaves the facility.

Protect against insider threats

Keys can be extremely valuable and steps must be taken to prevent theft from insider threats. This includes doing periodic background checks on employees and training them to understand operational processes and security awareness. For extremely sensitive operations, such as generating key pairs, it is necessary to establish multi-custody protocols that require two or more people to be involved in order to complete a sensitive operation. Think of it as a safety deposit box in a bank, where two people with keys (the bank manager and customer) are required to open a safety deposit box.

Protect against disaster scenarios

Private keys need to be protected against disasters as well. Questions to consider for any disaster plan include: Are private keys being backed up, off premise? How are those off premise sites secured? Sure, the keys can be encrypted and stored off site, but how can one protect the keys that protect the keys? And how quickly can service be restored?

Finally, what if a private key is compromised? New keys need to be reissued, but the existing keys need to be revoked. This can be accomplished using various key revocation mechanisms including Certificate Revocation Lists (CRLs) or protocols such as Online Certificate Status Protocol (OCSP).

Certificate authority partnership

These are just some of the things that need to be considered when designing and operating a public key infrastructure. It can be a complex, costly process to do all of this in-house. By outsourcing this function to a reputable certificate authority, you can save money, reduce risk, and get your projects up and running faster.

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) created a Public Key Infrastructure Assurance Task Force to establish the WebTrust Program for Certification Authorities. It is designed to ensure that a CA properly follows industry best practices.

Provisioning device identities

Key management is difficult enough when managing even a small number of keys. However, some deployments require a huge number of keys to be generated. Consider an IoT vendor that wants to give a unique cryptographic device identity to each of their IoT devices in the field. One can easily imagine deployments of millions of such devices.

Provisioning

The process of providing a device with an identity is referred to as provisioning. Once manufactured, the device identities need to get from the manufacturing source to the devices and services. There are generally two approaches to provisioning device identities: factory provisioning and cloud-based field provisioning.

Factory provisioning

With factory provisioning, the device identities are bound to the device in a factory during the manufacturing process. The primary reason to do factory provisioning is to take advantage of secure hardware. Many modern chipsets have specialized hardware features such as one-time programmable memory (electrical fuses) and other on-chip storage which can be used to store cryptographic keys securely. Getting keys into the hardware is a process commonly known as key injection. But, depending on the chipset, there might be limitations on the number or types of keys that can be injected into the chip.

Some chipsets have additional functionality such as secure boot to ensure only trusted firmware can run. Others have trusted execution environments, to protect sensitive computations at runtime. The features used largely depend on the type of application.

But, which factory? Generally, IoT service providers will work with OEM manufacturers, who in turn work with chipset manufacturers. This supply chain can complicate the provisioning process as device identity provisioning can happen at any point along this supply chain.

Security at factory environments

The factory environment can be both an advantage and a risk from a security perspective. On the one hand, such environments can often be tightly controlled.

For example, it is not uncommon for special facilities to be set up within the factory environment that are accessible to limited personnel to do the key injection. But increasingly, organizations are concerned about untrusted factory environments, especially by third parties in low cost geographies, where not all factory floor workers can be trusted to have access to sensitive keying material.

Cloud-based field provisioning

With cloud-based field provisioning, the device is given some minimal identity at manufacturing time, but it is not given a complete identity until it is first installed by the end user in the field. This is required if the identity of the device cannot be completely known until it is deployed. For example, the IoT service provider may have chosen an OEM or chipset provider long after those devices have been manufactured, and the device needs a more complex identity in order to participate in the trusted ecosystem provided by the service provider.

Minimum identity at manufacturing stage

Generally, the device must be given some kind of identity at manufacturing time using a factory provisioning process. At a minimum it needs to be given some kind of basic authentication key, known as a bootstrap key, in order to create a secure, authenticated channel with the cloud service. But this can be much simpler than provisioning the device with a more complex identity at manufacture time.

Once deployed in the field, and when the device is activated for the first time, it can connect to a cloud service (perhaps through a gateway device) to obtain its unique identity, using the bootstrap key to authenticate to the cloud. The device identity is then downloaded and stored in a secure location on the device.

Cloud-based field provisioning is a good approach for large scale deployments, as it enables cost effective and efficient scaling, even for millions of devices. By adopting a cloud-based field provisioning approach, the manufacturing process can be greatly simplified.

The Intertrust PKI advantage

Provisioning device identities requires an understanding of the supply chain, manufacturing environment, cryptography and cryptographic hardware. It can be particularly challenging to provision devices for large scale deployments.

Intertrust has provisioned over 1.5 billion devices, and counts the leading global service providers and device manufacturers among its customers. It is built to scale easily, and has a proven track record of provisioning over 10 million devices per day.

Our offering

Intertrust offers a complete, full-service managed PKI that specializes in delivering device identities at scale for trusted ecosystems, for companies that need security and control over all the players in their ecosystem.

In addition, it is important to provide the capability for devices to receive additional secure data. This ensures that they are capable of both endpoint and server mutual authentication, as well as delivering secured data, applications, firmware, etc.

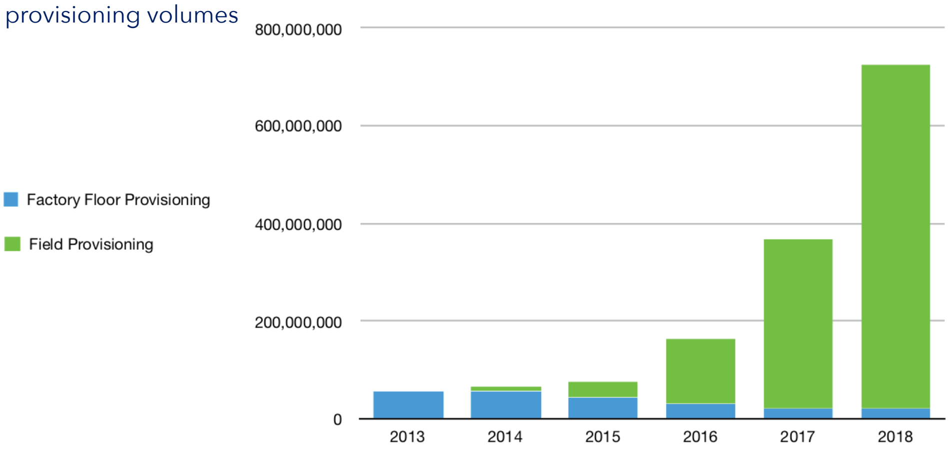
The solution has been designed to support both factory floor and cloud-based field provisioning, to meet all customer requirements.

Our differentiation

What differentiates Intertrust PKI is that it has been designed specifically for IoT and made-for services, unlike traditional PKI, that has been designed for millions of computers rather than devices.

Intertrust has designed technology to authenticate vast sensor networks via a certificate authority. We have generated billions of authenticated personalities for devices allowing any connected "thing" to be authenticated so it is clearly what it says it is. This, in turn, allows for interoperability across devices and platforms.

Figure 3.
Intertrust device identity provisioning volumes



Highly scalable device identity provisioning

Intertrust PKI is highly scalable. Our device IDs are already in 1.5bn devices worldwide, and its flexibility meets the needs of the evolving IoT market. Intertrust can provision up to 10 million device IDs per day through our scalable cloud provisioning service. In 2018 alone, we provisioned identities to more than 724 million devices using our cloud provisioning service.

Cost effective PKI

Using Intertrust PKI eliminates the need to run an in-house operation, or have PKI experts who know how to set up the appropriate facilities, technology, processes, and build a team. Further, due to economies of scale, Intertrust can provide these services at a cost savings of 50-85% over managing device identities in house.

Secure and trustworthy

Intertrust PKI is both WebTrust complaint and ISO 9001:2015 certified. The WebTrust certification covers all areas of the solution; from the people to the process, the infrastructure and solution itself. By using a Complete with a WebTrust compliant Certificate Authority, you can be assured that your PKI is being managed correctly. The ISO 9001:2015 certificate ensures that Intertrust PKI delivers the best-in-breed services at the highest possible quality.

Intertrust PKI has a perfect record of fulfilling orders that are 100% on-time and error-free.

Intertrust professional services

Intertrust's professional services team can design and implement customized schemes tailored to meet a specific business need. We understand the complexity of device identities and can work with you to design and implement a scheme tailored to your specific business needs. For other security, data governance and privacy management needs, our team can help define your security solution.

This includes creating:

- Credentials including certificates, keys, chip-secured trusted applications, key derivatives, hashing algorithms, XML files, SAML assertions, text and other data structures as per your security model.
- Cryptographic operations including digital certificates, digital signatures and encryption
- Collaboration with major chipset manufacturers, so you can take advantage of cryptographic hardware features in your device.
- Custom remediation if a standard CRL is insufficient
- Configurable and extensible systems that can accommodate a multitude of requirements.

Beyond device identity management and other PKI services, Intertrust has a team of world-leading experts to help design and implement the best-of-breed security solution for your business.

Conclusion

IoT is disruptive technology that is growing rapidly. However, without proper security, it will never reach its full potential.

Device identity management is a key consideration to secure IoT devices—where the process must be protected for both authenticating devices and authorizing access based on permissions. One of the best ways to provision secure device identities is through a PKI. Using the Intertrust PKI provides a comprehensive, cost-effective, and scalable solution to multiple problems that the IoT industry is facing.

Sources

1 GlobalData IoT Market Forecast and Growth Opportunities, September, 2018

2 IHS Technology, IoT Platforms: Enabling the Internet of Things February 2016

3 https://www.recode.net/2018/4/23/17272756/google-alphabet-nest-q1-earnings-2018-revenue-operating-loss

4 Alphabet Discloses Nest Financials for the First Time -- The Motley Fool, 24 Apr. 2018, Accessed 1 May, 2019

5 IoT in Manufacturing: Increase Operational Efficiency | Miles Data, May, 2017, Accessed May, 2019

6 https://www.helpnetsecurity.com/2017/12/05/implement-iot-projects

7 Ibid

8 2018 Study on Global Megatrends in Cybersecurity - Raytheon, Accessed May, 2019

9 https://www.nist.gov/topics/internet-things-iot

10 Industrial Internet Consortium- Security Working Group (for IIoT)

11 IoT Security Foundation

intertrust®

Building trust for
the connected world.

Learn more at: intertrust.com/pki-for-iot
Contact us at: +1 408 616 1600 | iPKI@intertrust.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035