PKI: The Security Solution for the Internet of Things

digicert®

Table of Contents

Executive Summary

In 1982, a compromised software that controlled pump speeds and valve settings deployed, making pressures in the Trans-Siberian Pipeline skyrocket. This resulted in a huge three-kiloton, non-nuclear explosion so big that it was seen from space.

Today, companies are deploying billions of Internet-connected devices into mission-critical systems. Mass deployment results in security risks with implications that grow with the number of deployed devices. Bad actors can easily compromise and misuse unsecured devices for nefarious purposes.

Public Key Infrastructure (PKI) is the foundation of securing Internet of Things (IoT) devices. As an accepted and well-established standard, PKI is a core component of data confidentiality, information integrity, authentication, and data access control. PKI is the foundation required to secure the communication between IoT devices and platforms.

Securing the IoT is dependent on ensuring the proper security development and deployment that incorporates the three key elements of trust: core device security, data and personal privacy, and adherence to standards and critical maintenance.

Ensuring that IoT solutions and projects meet these key trust elements is not only important for today's threat landscape, but also for the future product and service lifecycle challenges, which would otherwise inhibit the future success of these solutions.

PKI is uniquely positioned to deliver on the necessary and critical security needs of the IoT. The Institute of Electrical and Electronics Engineers points out, "When you're looking at authenticating devices, the only real standards at the moment that offer any real interoperability tend to be Public Key Infrastructure (PKI)."

Gartner touts PKI as a leading choice for information and communication security because of the inherent flexibility and wide range of applications. PKI delivers the essential authentication and encryption components needed by the IoT for data security, making it a proven solution and market-ready platform for IoT device security today.

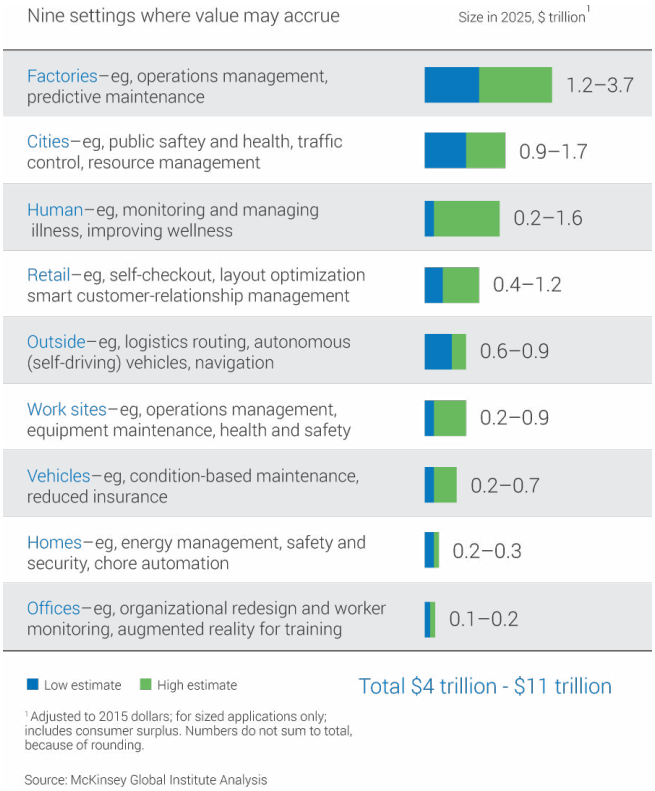
This white paper will discuss security challenges IoT providers face, the crucial need to secure communication in IoT ecosystems, and that PKI is the tried-and-true technology solution for authenticating and encrypting device communication.

The Emergence of the Internet of Things

The IoT is transforming the world we live in. IoT is often defined as a network of physical objects that can interact with other Internet-enabled systems and devices to share information and perform actions based on manual user input or an automated controlling system. IoT promises interconnected systems, data, and devices between the physical world and the online world for increased efficiency and business growth, as well as improved quality of life. IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine communications (M2M) and covers a variety of protocols, domains, and applications.

Recent reports by Gartner estimate that there are more than 2.9 billion networked IoT devices available to consumers in smart environments today. Factor in smart devices in use for corporate, medical, or non-traditional smart industries and the number of Internet-connected devices in use today is much bigger.

IOT OFFERS A POTENTIAL ECONOMIC IMPACT OF $4 TRILLION TO $11 TRILLION A YEAR IN 2025



A number of vertical markets are already integrating connected devices into processes, infrastructures, and workflows contributing to what we call the "Internet of Everything."

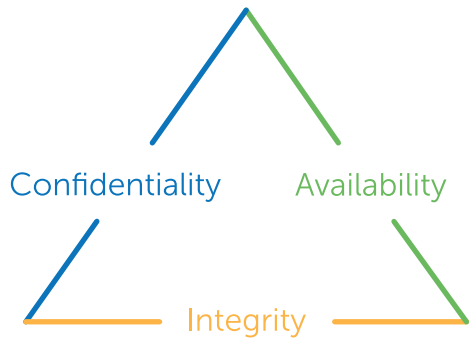
Connected devices range from smart heart-monitoring devices, wireless insulin pumps, biochip implants for plants and animals, built-in sensors for automobiles, to smart appliances. The connection between these embedded devices (including smart objects) will usher in automation for nearly all fields while also enabling advanced applications like a smart grid, and expanding into areas, and expanding into areas, e.g., smart cities, etc. McKinsey estimates that IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion per year by 2025.

As the number of networked devices continues to grow, the capabilities of IoT systems will diversify the type of networked devices, requiring better security as we bring connectivity, transportation systems, energy infrastructure grids, and healthcare monitors to communities everywhere. However, despite the various specifications and capabilities of these systems and devices, the underlying need for critical security and authentication is shared.

Security Risks in Networked Devices

While delivering on the promise of streamlined efficiencies and operational insights, smart devices in the IoT also present a new and more widespread threat to users and personal data. Current threats to IoT devices have moved beyond simple proof-of-concepts, and it is expected attackers will continue to explore the developments in technology and accelerate ways potential threats can be realistically exploited.

IoT solutions and implementations must account for the necessary and fundamental needs of secure systems and data, including the three core goals of information security: confidentiality, availability and integrity.



Confidentiality ensures privacy. Access to information must be restricted to those authorized to view the data and the storage, and transmission of the information must be encrypted to prevent unauthorized access to data being communicated between systems and devices.

Access controls are also part of availability. Availability ensures that hardware, applications, and systems are properly accessible to authorized entities and are performing intended functions.

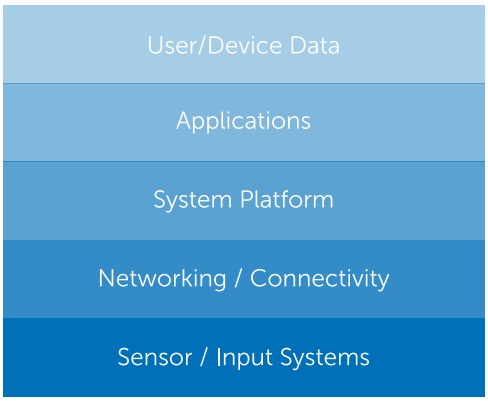
Integrity ensures data remains consistent and accurate during transit or as it is accumulated. Any solution that meets these three goals needs to be able to scale beyond current Internet levels of service. Large-scale IoT deployments often mean more complex requirements or a larger burden on a service provider's infrastructure, which makes scalable systems a challenge to ongoing data security.

Each IoT device is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Securing these Internet-connected devices and platforms requires a thorough understanding of the makeup of the IoT information stack, its various elements, and the specific security requirements of those layers.

For example, an IoT application that collects data from multiple connected devices may have entirely different security requirements than the actual device itself. Security must be considered and addressed throughout each part of a device's information architecture in the IoT. The Open Web Application Security Project's (OWASP) list of top IoT vulnerabilities demonstrates the critical concern that proper data security, identity, and trust play in developing solutions for the IoT. The list includes the following as the most critical existing attack vectors for IoT and networked devices:

- Unsecure Web Interface
- Data Privacy Concerns
- Unsecure Device Software/Firmware
- Insufficient System/Identity
- Authentication
- Unsecure Cloud Backend Systems
- Poor Transport Encryption
- Implementation
- Unsecure Network Services
- Unsecure Mobile Connections
- Poor Physical Device Security

IOT INFORMATION STACK



Security implementations are not simply about encrypting data, they also ensure the proper deployment and configuration of security across the various layers of communication within individual devices and across integrated systems.

Security in IoT implementations must be a critical component either during the device design and manufacturing phase or during the initialization phase or a product update. Correctly implemented, secure IoT deployments should ensure that the basic security requirements needed for data confidentiality, data integrity, and data accessibility are properly configured as part of the solution. For some, IoT deployments security has been an afterthought, causing some connected device manufacturers to retrofit devices with solutions that insulate them from malicious entities. Security built into design is a superior approach—something the Internet industry already knows too well.

PKI's Foundation of Strong Security

PKI has been the backbone of Internet security since its inception through the use of digital certificates. PKI inherently delivers the basic and essential elements of privacy in communications using encryption and authentication. PKI's unique role in the history of data and identity security and its ability to facilitate the secure transfer of information across networks makes it the clear solution for IoT service providers to ensure proper data security, authentication, and mutual trust.

Digital certificates have been used to secure networked devices, such as servers, routers, printers, and fax machines for decades. Because of the proliferation of new smart devices, the emergence of IoT adds complexity into an organization's security and trust ecosystem. One of the differentiators of IoT from traditional networked systems is the diversity of the networked devices, however, the common layers of the connected ecosystem found in traditional networked devices makes PKI a strong solution for securing the IoT.

PKI enables safe authentication of users, systems, and devices without the need for tokens, password policies, or other cumbersome user-initiated factors. With PKI, IoT solutions can enable direct authentication across systems in a decentralized handling of authentication. While not vulnerable to common brute-force or user-deception attacks, PKI facilitates the secure storage and transmission of sensitive information. This protects it from malicious actors even if a data stream or data source were captured or compromised. Modern-day PKI is secure and cannot be replicated when using modern-day cryptography.

PKI has the capability to address the security needs of at-rest and in-transit data. Additionally, PKI ensures the integrity of data acquired from sensors or other intelligence systems. PKI also facilitates the verification of proper availability and access for protocol and application configuration, or interaction with data stored in the device, thus ensuring the complete coverage of data and system confidentiality, integrity, and availability.

PKI solution providers are uniquely positioned to address the security needs of the growing IoT community. Commercial PKI vendors can deliver the specific security components, trust anchors, flexible and scalable platforms, and the expertise needed to properly secure IoT devices. A comprehensive PKI solution includes the hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates, as well as manages the encryption process used to secure information in communication between systems and devices.

PKI & DATA SECURITY

PKI is an open standard, free to be adopted, implemented, customized, and extended. This makes PKI the clear choice for organizations that are adding connectivity to systems, services, and smart devices. With the greater emphasis today in smart devices, smart grids, networked health data systems and devices, as well as networked infrastructure, data security is of the utmost concern.

The most effective mechanism to mitigate the risk associated with information stored and exchanged between networked devices is to ensure that strong identity assurance and authentication is required for any access to sensitive data assets. Identity assurance is the measure of confidence that the entity at either end of a data transaction or authentication event is who it claims to be. Identity verification is a fundamental element for effective security and networked device trust. It is also a pre-requisite for proper identity management, which is a requirement for robust security implementations.

PKI's existing infrastructure of identity vetting completed by publicly trusted and audited Certificate Authorities provides the necessary foundation for IoT organization authentication. PKI certificates are evidence that the identity of organizations, domains, and devices was properly established because certificates cryptographically bind public keys to such identities. Pre-vetting capabilities and on-demand issuance, like DigiCert's Managed PKI for IoT performs, enable one-time pre-verification or real-time verification to perform the identity assurance needed by IoT projects and systems.

PKI provides the core competency and unique value to enable trusted connections between networked devices, cloud services, smart infrastructure, and "things." This is the authentication component IoT needs for its security. In these areas of security, PKI excels as a proven solution. Gartner, IEEE, and other industry groups tout the flexibility and wide range of applications of PKI as a leading choice for information and communication security.

PKI & FLEXIBLE DEPLOYMENT

While every IoT device varies in its utilization and implementation, PKI offers flexible deployment options in order to cater to the critical authentication and encryption capabilities of unique devices.

The availability of network connectivity, a device's internal memory or computational power, or regular maintenance or updates are all important factors that impact the security deployment of an IoT device.

Performance, capability, and availability of platform flexibility or project customization will vary greatly between Certificate Authorities. Some of these differences include the following:

- Custom profiles, key usage fields, and OIDs
- Shorter and longer validity periods for certificates
- Custom certificate subject fields
- Stronger cryptographic hashes and algorithms
- Direct-to-root-chained certificates hashes and algorithms
- High availability of systems and distribution of services worldwide
- Revocation checking performance
- Flexible trusted roots and revocation options
- Scalable from thousands to millions to billions of certificates

Additionally, numerous certificate management protocols exist as part of a security certificate enrollment and device deployment process:

- Simple Certificate Enrollment Protocol (SCEP)
- Certificate Management over CMS (CMC)
- Enrollment over Secure Transport (EST)
- Enterprise API

PKI security allows for a variety of deployment approaches, which makes PKI the most flexible solution for securing IoT devices. This level of flexibility enables PKI to be implemented during device manufacturing process by a hardware manufacturer or deployed remotely during a customer's initial device setup or configuration.

PKI & SYSTEM SCALABILITY

There are needs for specialized IoT PKI platforms in order to provide the scalability and dependability required from possible implementations of networked devices and to mitigate the risks associated with networked devices. Addressing the growing demands from IoT projects requires a more comprehensive PKI solution from an IoT-focused Certificate Authority. Selecting the right Certificate Authority with specialized systems, industry knowledge, and technical expertise must be a key consideration during the IoT security development and vendor selection process.

In addition to the sheer number of devices that require security implementations, IoT providers should consider how their IoT needs will impact their CA. Device manufacturers need to consider critical implications for IoT devices, such as computational power and device memory, in order to meet the performance and capacity needs of the chosen security solutions.

Even with low computational power and memory, cryptographic algorithms can often still be computed within reasonable time. If cryptography can't be added to the individual device, then the first step is to secure the hub or controller at the next level in the ecosystem. Devise a plan to provide a truly secure infrastructure in the short future.

IoT implementations can either be open systems, where users decide to join on-demand, or closed systems, where IoT solution providers control the deployment. Some key considerations for IoT PKI implementations include the

massive size, scale, and scope of IoT solutions. Most PKI certificate implementations deal with significantly smaller implementations than new IoT PKI requirements. IoT providers will need to find a Certificate Authority with a scalable infrastructure to meet their needs.

IoT device management, as well as key and certificate lifecycle management, requires the combined analysis of device capabilities and supporting Certificate Authority cloud infrastructure. Ongoing maintenance for device and security components required to secure data will drive how you manage the provisioning and management process of device certificates and keys throughout a device's lifecycle.

PKI & STANDARDS

Legislative and industry bodies have addressed the unique nature of data security within different IoT verticals. Data security requirements such as HIPAA, PCI, FERPA, CALEA, and others, are evaluated to ensure the standards are sufficient to secure IoT devices and make sure providers deliver proper security.

While some data and device security standards may not be in place or government mandated yet, we know that encryption and authentication will be part of whatever finalized standards are developed for IoT security.

Knowing this, IoT providers must consider the damage or safety implications that a security lapse or data compromise could have on their—or their clients'—organization. Data loss or injuries to users who depend on smart devices could prove detrimental to an organization and to the mass adoption of these new IoT technologies. PKI provides the highest level of authentication and encryption to ensure data integrity for IoT devices.

Example PKI IoT Deployments

DigiCert recently partnered with media streaming solution provider Plex to deploy one of the largest public IoT implementations using publicly trusted certificates.

With the increasing use of streaming personal media online, along with Plex's own commitment to software security, the Plex team selected DigiCert's IoT PKI platform to secure its media streaming platform and user devices. Enabling PKI certificates for its software and user devices ensures Plex users the highest security and privacy assurance. Because Plex is used on computers, TVs, and mobile devices, the situation demanded a ubiquitous solution, which DigiCert provided.

The Plex streaming server's automatic update process enabled Plex to deploy fully vetted x.509v3 DigiCert certificates automatically to customer devices already in production—a seamless security implementation. IoT APIs enabled automatic and on-demand certificate request, issuance, and deployment in real time, without the need for expensive device maintenance or user input.

In addition to data security, this IoT PKI implementation delivered publicly trusted certificates that now allows users to see the trusted padlock, indicating secure access to their personal media dashboard. The added assurance of privacy and public trust delivered a solution that private certificates or self-signed certificates could not provide.

This IoT PKI deployment process is accomplished by leveraging DigiCert's IoT management platform and APIs to provision trusted certificates during manufacturing, on-demand, and update stages to renew and update public certificates.

PKI is the Security Solution for IoT Security

PKI has a history as the de-facto standard for Internet security and has the developing specifications to accommodate the requirements of diverse IoT deployments. Therefore, PKI is the best option for solution providers to secure data and connected devices.

When correctly implemented, PKI can build and support security and trust in IoT ecosystems. PKI's role in IoT provides strong identity authentication and creates the foundation of trust that systems, devices, applications, and users need to safely interact and exchange sensitive data.

PKI and the spawned trust communities cover the critical security requirements IoT projects need, providing the encryption, authentication, and data integrity that create the foundation of trust. IoT PKI platforms also deliver the scalability and flexibility that providers need as they move through testing, production, and deployment requirements. PKI is poised to accommodate and leverage its existing technologies for the specific and increasingly diverse needs of the IoT.

Anderson, M. "Looking for the Key to Security in the Internet of Things," IEEE Spectrum, 2014.

Evans, D. (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). Cisco. Retrieved 9 September 2015.

Höller, J., Tsiatsis, V., Mulligan, C., Karnouskos, S., Avesand, S., Boyle, D.: From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Elsevier, 2014, ISBN 978-0-12-407684-6.

Miessler, D. (2015, August). IoT Attack Surface Mapping DEFCON 23. Retrieved April 6, 2016, from https://www.owasp.org/images/3/36/IoTTestingMethodology.pdf.

Monnier, O. : A smarter grid with the Internet of Things. Texas Instruments, 2013.

"What is PKI? - A Complete overview , January –23, 2015". Retrieved 2015-02-24.