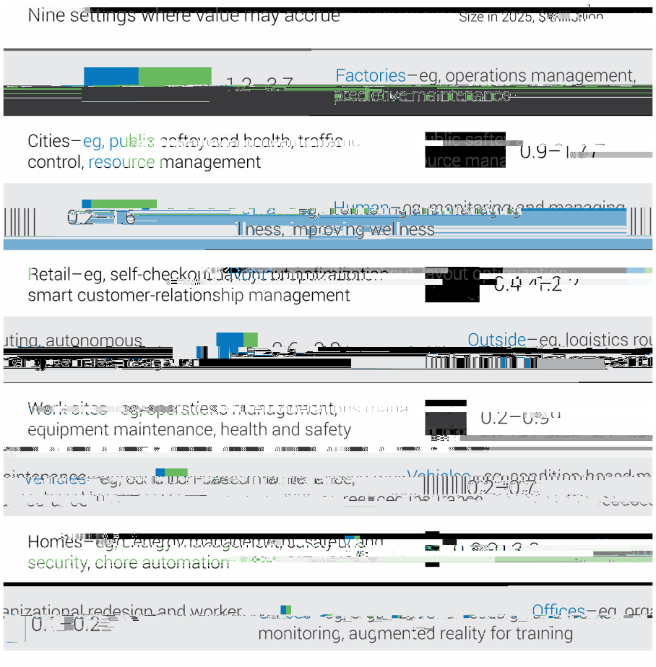
digicert®

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

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.



[1] Adjusted to 2015 dollars; for sized applications only; includes consumer surplus. Numbers do not sum to total, because of rounding.

Source: McKinsey Global Institute analysis

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

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:

Availability

I

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.

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

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
-
- Authentication
- Unsecure Cloud Backend Systems
- Poor Transport Encryption
- Implementation
- Unsecure Network Services
- Unsecure Mobile Connections
- Poor Physical Device Security

PKI has been the backbone of Internet security since its

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.

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 tr

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.

interaction with data stored in the device, thus ensuring

integrity, and availability.

PKI solution providers are uniquely positioned to address the security needs of the growing IoT community.

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,

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

or authentication event is who it claims to be. Identity

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

provides the necessary foundation for IoT organization

identity of organizations, domains, and devices was properly

public keys to such identities. Pre-vetting capabilities and on-demand issuance, like DigiCert's Managed PKI for 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

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

Authorities. Some of these differences include the following:

-
-
-
- Stronger cryptographic hashes and algorithms
-
  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

deployment process:

-
-
- 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 [illegible]

PKI has a history as the de-facto standard for Internet

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

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.