

Identity, Security, and the Internet of Things

Knowing Your Device is Securing Your Device

CSS Solution Brief | Q2 2017

For PTC ThingWorx IoT Platform Users

IoT Has Awesome Potential, But Do You Trust It?

Remember the 1990s? The internet was going mainstream, promising to spark new business models and transform everything from culture to customer experience.

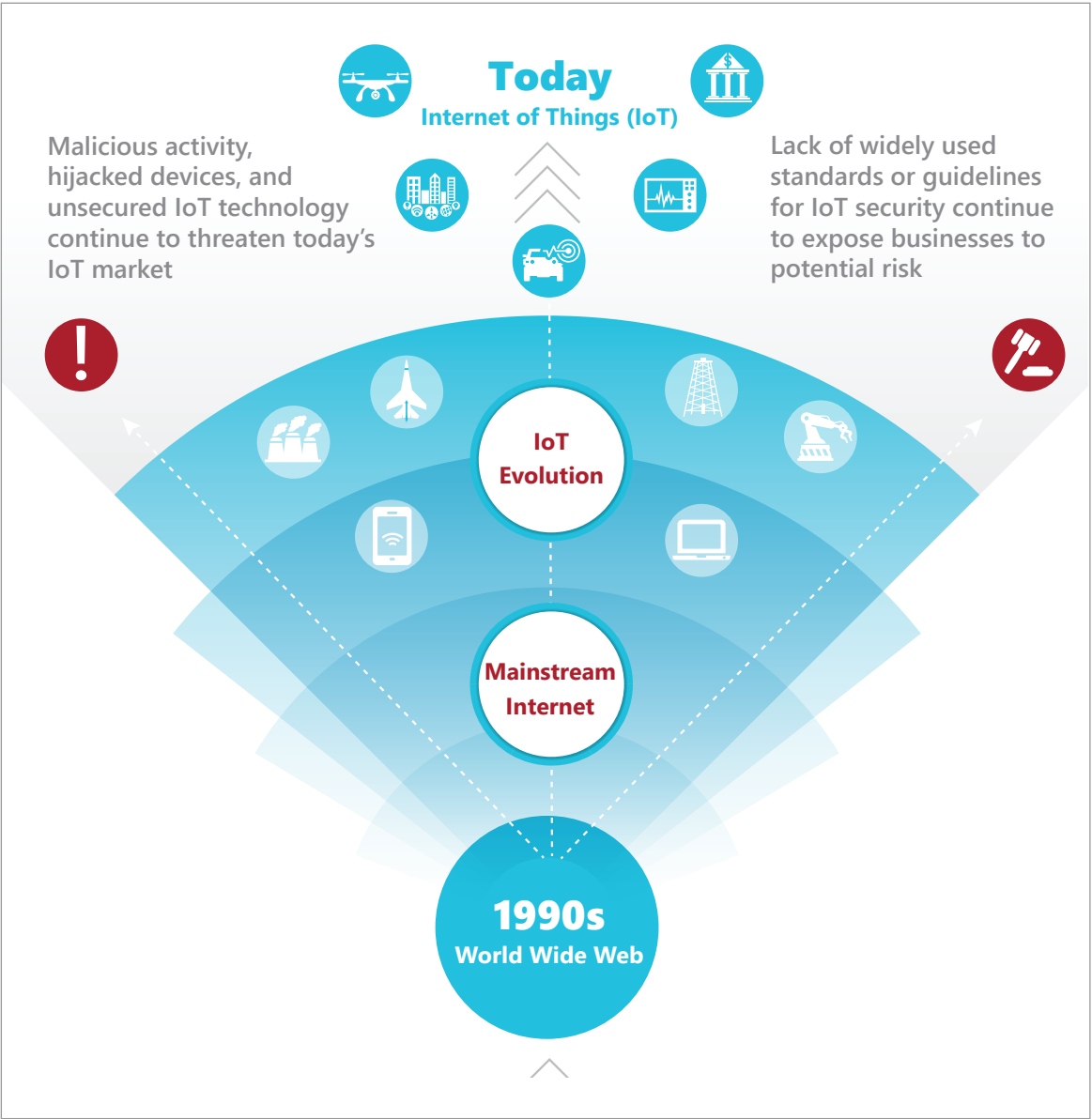
With the growth of the physical manifestation of the Internet of Things (IoT), it's like it's the 1990s all over again. IoT offers big business promises, but its application possibilities are even greater, spanning everything from the industrial realm to drones, self-driving cars and beyond.

But reflecting on the naiveté of the early internet should also serve as a warning. In the 1990s, not many people thought clearly about the nuances of online businesses or the potential of malicious actors to hijack the web.

Now, the internet is awash with reports of hacked IoT devices, breached banks, and cyber-interference of elections. It doesn't help that there are no widely used standards or guidelines for IoT security—just as there weren't with the internet decades ago. While industry groups such as the Industrial Internet Consortium and the IoT Security Foundation have developed security frameworks to address this problem, their efforts are still in their early stages.

As the IoT market expands, it's all too common for vendors to push unsecured IoT technology to the market. Many IoT devices consist of parts from various hardware vendors, each created according to different security principles. The result is an environment where the lowest common denominator of security measures rules, inviting malicious activity that can wreak havoc on businesses, institutions, and critical infrastructure.

Figure 1. The Potential of Today's IoT is Awesome, Yet Security Risks Continue Decades Later



Why the Internet of Things is A Different Animal than Enterprise IT

In theory, the Internet of Things has promised to be more secure than traditional enterprise IT applications. Humans are generally the weakest link in a secure environment. But once an unauthorized person breaks into a machine-controlled network, they can launch exceptionally powerful attacks.

A central challenge of securing IoT is its sheer size. Many IT organizations would consider 100,000 user identities to be overwhelming. With an IoT project, however, even one million devices would be modest. Indeed, an IoT directory should be as ready for 100 million devices as it is for a single device.

Hackers can also leverage the massive scale of IoT to launch crippling attacks. For example, in October 2016, cybercriminals orchestrated a distributed denial of service attack with speed of 1.2 Tbps that took down popular websites Amazon, Twitter, Spotify, and Reddit. The botnet pulled off this stunt by using about 100,000 connected devices—mostly standard routers, DVRs, and video cameras. The attack weaponized the scalability of IoT and exploited the widespread use of default passwords.

The diversity of IoT hardware, software and protocols is another problem. The fact that most IoT devices are headless and rely on automated processes is another challenge.

All of these traits make managing an IoT deployment vastly different than administering a traditional enterprise IT application, with its clearly defined set of users and limited number of devices.

Security Challenges of IoT

Sheer Size and Massive Scale	• An IoT directory should be as ready for 100 million devices as it is for a single device. • Hackers can leverage the massive scale of IoT to launch crippling attacks.
Diversity and Automation	• IoT hardware, software and protocols are diverse, and most IoT devices are headless and rely on automated processes.

"Nearly 47% of businesses have suffered breaches for each function where they are planning to deploy, or have deployed, IoT solutions."

— Forrester

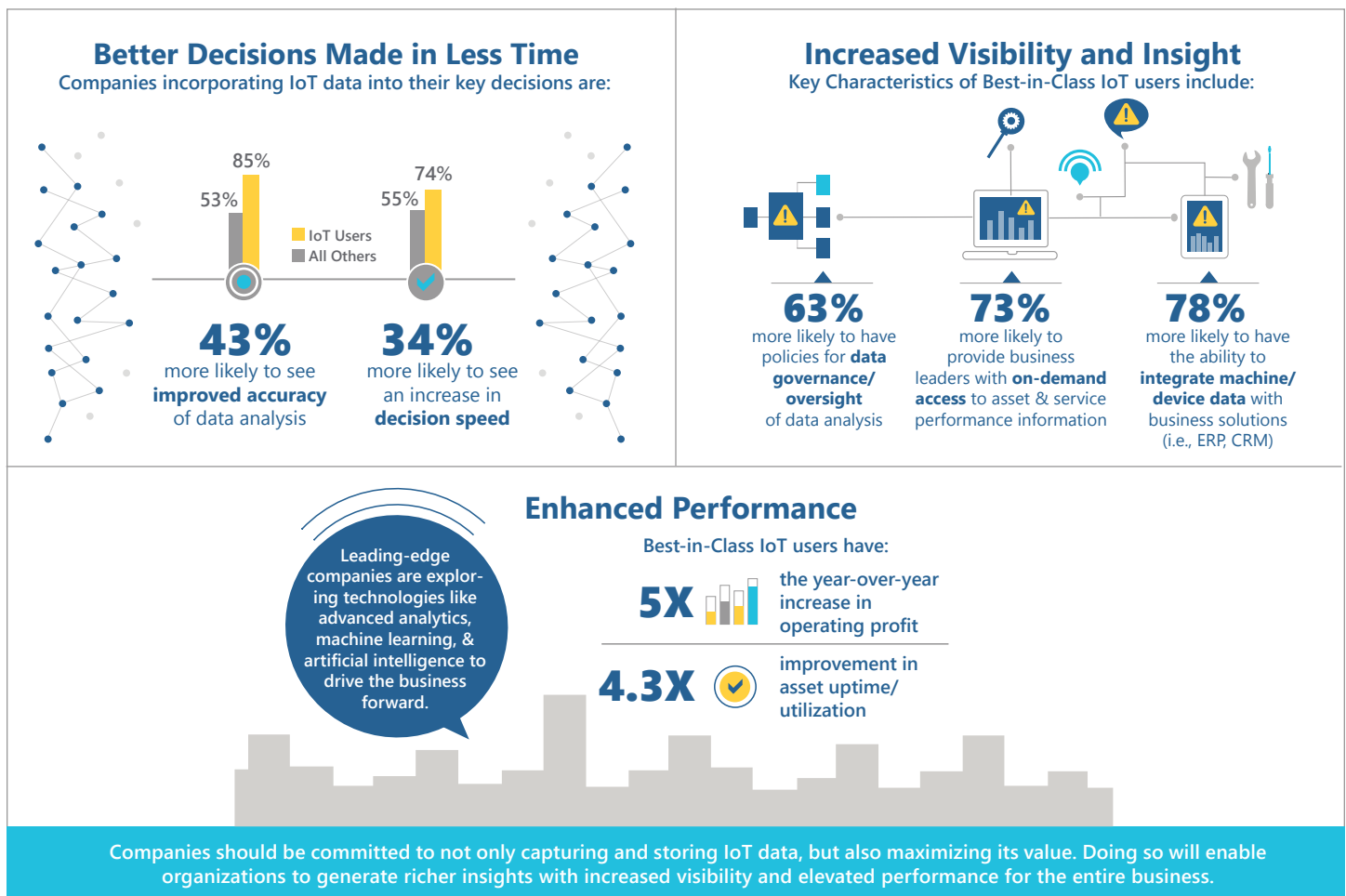
If Data is King, the Crown Jewels are at Risk

Not only can IoT devices be misused, but hackers can also compromise or sabotage data. If data integrity from IoT devices cannot be validated, its value is diminished or negated.

On the upside, data analytics can lead to operational insight and trigger immediate automated actions within connected systems. But if someone tampers with the data or intentionally feeds false data into the system, the triggered actions will be erroneous and potentially destructive.

The security risks in the industrial IoT realm are not merely theoretical. Nearly 47% of businesses have suffered breaches for each function where they are planning to deploy, or have deployed, IoT solutions, according to Forrester.¹

Figure 2. The Benefits of Leveraging IoT Data



Source: Research by Aberdeen Group. Brought to you by PTC/ThingWorx.

The Industrial IoT Increases the Risks

At present, the most enthusiastic sector to embrace the Internet of Things is the industrial realm. The so-called Industrial IoT (IIoT) offers immense potential for an array of niches including automotive, healthcare, energy, and the aerospace industries.

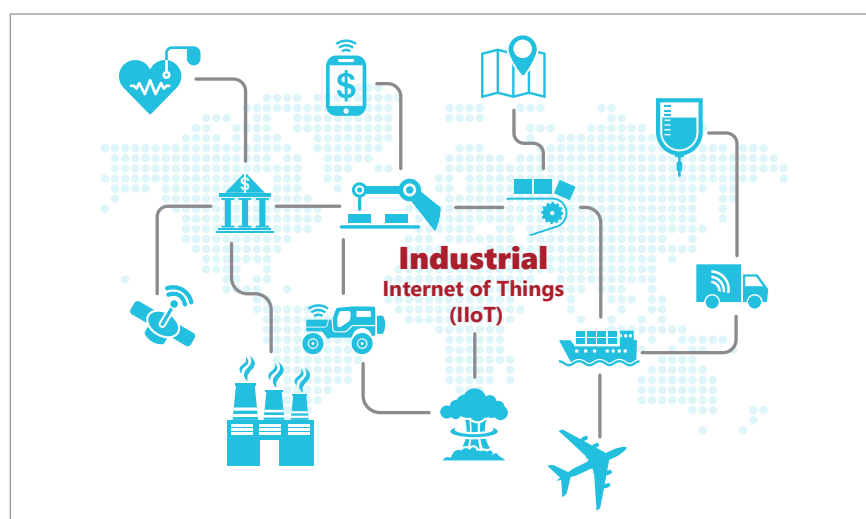
The cost of a breach in these industries is irrevocably high. It's one thing to have hackers crash your laptop; it's another to have them crash your medical device, your car, or a plane.

It's not hard to find evidence that the security risks with IoT are more real than theoretical. White hat hackers have already found vulnerabilities in devices like pacemakers and infusion pumps. In the past couple of years, Ukraine has blamed Russian hackers for targeting its power grid and infrastructure with malware and shutting down power on multiple occasions. And in 2015, the cyber security researchers Charlie Miller and Chris Valasek remotely hijacked a Jeep Cherokee while it was driving and turned off the transmission while the vehicle was on the freeway. Last year, the duo stated they expanded their bag of tricks, and could cause unintended acceleration or play with the car's steering wheel or brakes when the car is traveling at any speed.

Other notable security horror stories include a hacker who claimed to take control of a plane while in flight by breaking into its in-flight entertainment system. There have also been security experts who have remotely controlled medical devices such as insulin pumps and pacemakers.

Likely the most famous malware to target the industrial environment is the Stuxnet virus, which caused physical damage to Iranian nuclear centrifuges by targeting their supervisory control and data acquisition (SCADA) systems. First discovered in 2010, the virus is said to have ruined nearly one-fifth of Iran's nuclear centrifuges. The same types of attacks, at least in theory, could cripple many industrial facilities across the globe.

Figure 3. Industrial Internet of Things (IIoT)



"The foundation of IoT security lies in establishing an *identity framework* with a Root of Trust (RoT) and unique identity for each device. This framework is the basis for authentication of IoT systems, encryption of data, and execution of secure code."

A Strong Security Foundation is Indispensable

One of the most fundamental lessons we can take from the history of the internet is that security should be built in. Attempts to retrofit security into a project are complex, inefficient, and ultimately ineffective.

That's long been the case with the internet itself. A quick look at the history of the internet and the missed opportunities to integrate security will show how important it is. The precursor to the World Wide Web, ARPANET, debuted back in 1969 as a network to link trusted endpoints in the military and academia. In 1973, the electrical engineer Robert Metcalfe warned that ARPANET was vulnerable to security breaches. In 1978, Vinton G. Cerf and Robert E. Kahn worked to build encryption into TCP/IP but later gave up in doing so. By 1988, the insecurity of the internet became evident when a Cornell University grad student infected about 10% of the 60,000 computers then on the internet. Fast-forward to today and malware is rampant across all types of internet-connected devices, and many IoT vendors, especially in the consumer realm, continue to downplay the security risks.

With IoT, we have the potential to learn from the mistakes of the past and ultimately build secure internet-based or IoT-based directories. To do that, you must be able to uniquely identify entities within it. The foundation of IoT security lies in establishing an identity framework with a Root of Trust (RoT) and unique identity for each device. This framework is the basis for authentication of IoT systems, encryption of data, and execution of secure code.



CMS VerdeTTo: Security Begins with Trusted Identity

A central cyber security challenge is identifying the internet's unique users. CMS VerdeTTo is a secure service that lets you establish your own dedicated IoT Directory with a dedicated RoT that includes unique certificates for each device. Your IoT Directory allows for the execution of certificate-based authentication, granular authorization, data encryption, and assurance of secure code execution. CMS VerdeTTo establishes unique identities consisting of device certificate, trust chain, and customizable extended attributes for each of your IoT devices, whether numbering in the thousands or millions. Building a trusted identity framework into your ThingWorx IoT project is best done at its onset, with full integration of your IoT Directory and ThingWorx, and an identity framework that leverages your own RoT. The result is assurance that all IoT devices and gateways connecting to your ThingWorx system are uniquely identifiable.

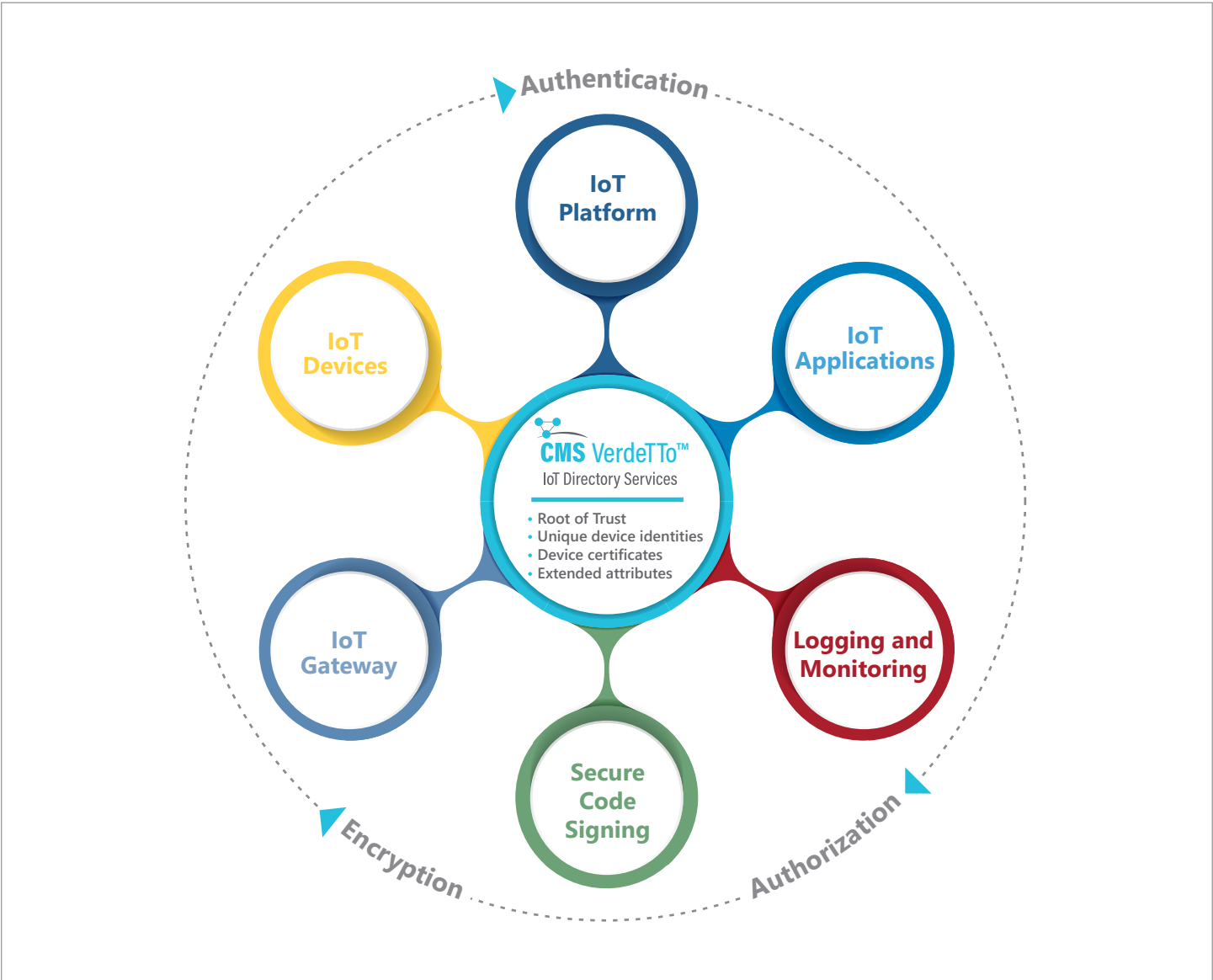


CMS VerdeTTo™

IoT Directory Services

- Root of Trust
- Unique device identities
- Device certificates
- Extended attributes

Figure 4. CMS VerdeTTo IoT Directory Services



"CMS VerdeTTo ensures that all IoT devices, gateways, platforms, and applications are uniquely identifiable and their identity used to secure them. Security begins with identity."

The Effectiveness and Scalability of Public Key Infrastructure

The CMS VerdeTTo solution leverages Public Key Infrastructure (PKI) to establish unique device identities in the form of digital certificates and extended identity attributes. PKI offers an effective and secure identity layer that is scalable and capable of accommodating millions of devices. PKI is a trust framework composed of hardware, software, policies and procedures needed to manage trusted digital certificates and public key encryption. CMS VerdeTTo brings together these elements into a service offering that establishes an IoT Directory based on dedicated RoT for your IoT ecosystem. The private PKI service CMS VerdeTTo provides produces the IoT Directory, RoT, and digital certificates for all elements of the ecosystem, including your ThingWorx IoT Platform, devices, gateways, and data analytics systems. Each element uses these digital identities, their certificates, and keys for encryption, authentication, authorization, and digital signing to ensure secure code execution. When compared to identification alternatives native to the ThingWorx IoT Platform, PKI provides the richest capabilities and highest security assurance level. Shared passwords and tokens can be compromised. Unauthorized devices can use those compromised passwords to attempt to access IoT systems. These passwords and tokens are difficult to update, and having a shared key limits the ability to control the identity and access of particular devices within the overall fleet. PKI offers non-exportable digital identities, individually controlled at a per-device level, enforced within all authentication and encryption functions.

PKI Management and Avoiding Erosion

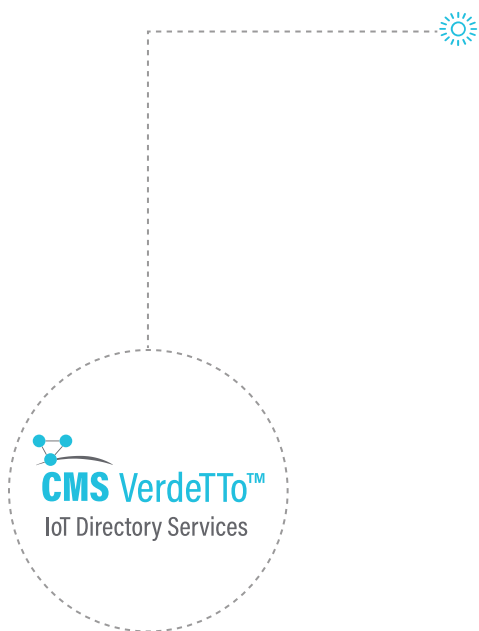
While PKI can secure an IoT system, the cost, time, and expertise needed to manage a robust PKI can be staggering. From services to resource salaries and hardware, annual in-house PKI maintenance can cost from \$300,000 to more than \$1 million.

"The cost, time, and expertise needed to manage a robust PKI can be staggering. From services to resource salaries and hardware, annual in-house PKI maintenance can cost from \$300,000 to more than \$1 million."

Strong PKI operations also tend to deteriorate over time, requiring further maintenance. As projects expand and new initiatives arise, organizations find themselves enabling PKI in new workloads without factoring those demands into their original PKI design or operations model. This results in widening security gaps and increased stress on management teams. Continued operational oversight and built-in scalability are mandatory for a PKI to continue supporting original requirements while taking on new initiatives, all the while maintaining its security assurance level. CMS VerdeTTo ensures the ongoing efficiency and security assurance of a PKI by offering a managed service model or PKI as a Service (PKIaaS). It also eliminates the direct responsibility of maintaining the system per required functionality, performance, and security assurance level. As an operator of PKI services for the Fortune 500, Certified Security Solutions (CSS) has longstanding PKI expertise, along with the operations management platform and models needed to ensure that the PKI is operational, scalable, and secured.

Overview: CMS VerdeTTo

CMS VerdeTTo excels at establishing an IoT Directory and digital identity management foundation for use within device authentication and authorization, data encryption, and signing of secure code. The Root of Trust (RoT) established by CMS VerdeTTo is a private root, with no chaining to other organizations or certificate vendors, and no shared trust with unrelated parties or certificates. You have full ownership and control of all identities issued from it and trusted by it. Unlike a shared Root of Trust, or one that chains to a shared root, there is no action required if and when another organization is breached or their private keys compromised. The fate of your IoT security is disconnected from outside organizations. CMS VerdeTTo does allow, however, publicly-rooted certificates to be used and managed. You can issue as many certificates as needed without the cost of purchasing certificates from public certificate vendors or resellers. Each identity in your IoT Directory is comprised of a digital certificate, a trust chain, and special extended attributes bound to each identity. They are stored within your single-tenant directory. These attributes are fully customizable and can be configured for different relationships and statuses. Furthermore, the attributes can be modified at any time, either through the CMS VerdeTTo administrative console or directly by your device and applications via Web API. These extended attributes open the door for adaptive authentication and granular authorization into your ThingWorx IoT Platform.



CMS VerdeTTo provides RoT management using device agents and web APIs. This strategy ensures device keystores and truststores are optimally configured. This includes the identity of a device and the connected systems it should trust, as well as the issuer identity of updates to accept and code to execute.

This RoT management allows you to limit who your devices and applications can communicate with, rather than relying on default trusted root lists that typically include every public certificate vendor that common web browsers trust. In the IoT realm, there is usually no need for a device or system to speak to anyone outside of your private ecosystem, and keeping default trusts in place causes unnecessary exposure.

Authentication and Authorization

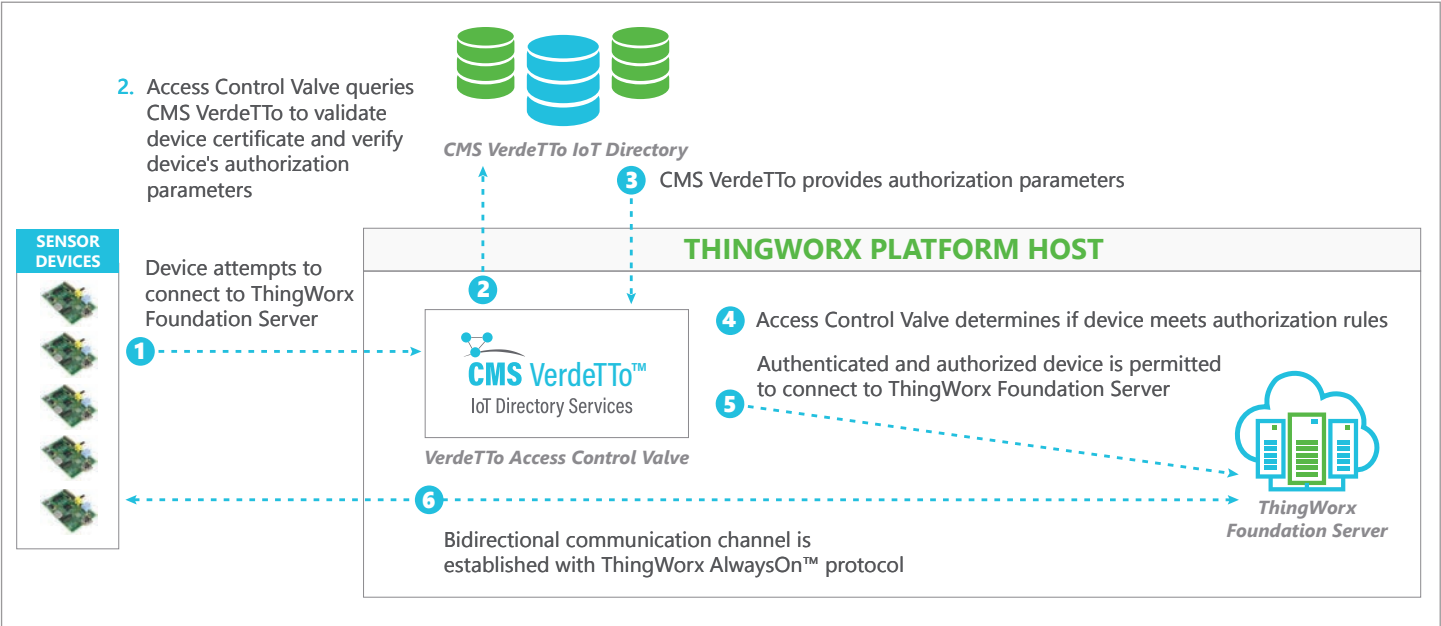
CMS VerdeTTo includes an Access Valve for ThingWorx that enables real-time authentication and authorization with your IoT Directory. CMS VerdeTTo verifies the validity of a device's certificate and applies rules to its extended identity attributes to perform authentication and authorization. This allows for time- and geo-fencing. This technique can also instantly restrict device access based on custom criteria reflected in a device's extended attributes within the IoT directory.

The CMS VerdeTTo Access Valve for ThingWorx embeds this authentication and authorization functionality directly into the ThingWorx IoT Platform, without requiring modification or addition of any application code.

Revocation

With CMS VerdeTTo, device identities can be revoked individually, or their status defined to determine how they can be authenticated. Within vast IoT landscapes, Certificate Revocation Lists (CRLs) can lose relevance and suffer accessibility problems because of CRL caching, update frequency, and enforcement of CRL checks. The same limitations apply to Online Certificate Status Protocol (OCSP), a traditional method of verifying if a certificate has been revoked. CMS VerdeTTo leverages its extended identity attributes to provide an agile and precise method for turning off, or temporarily pausing, individual device access.

Figure 5. What is CMS VerdeTTo?

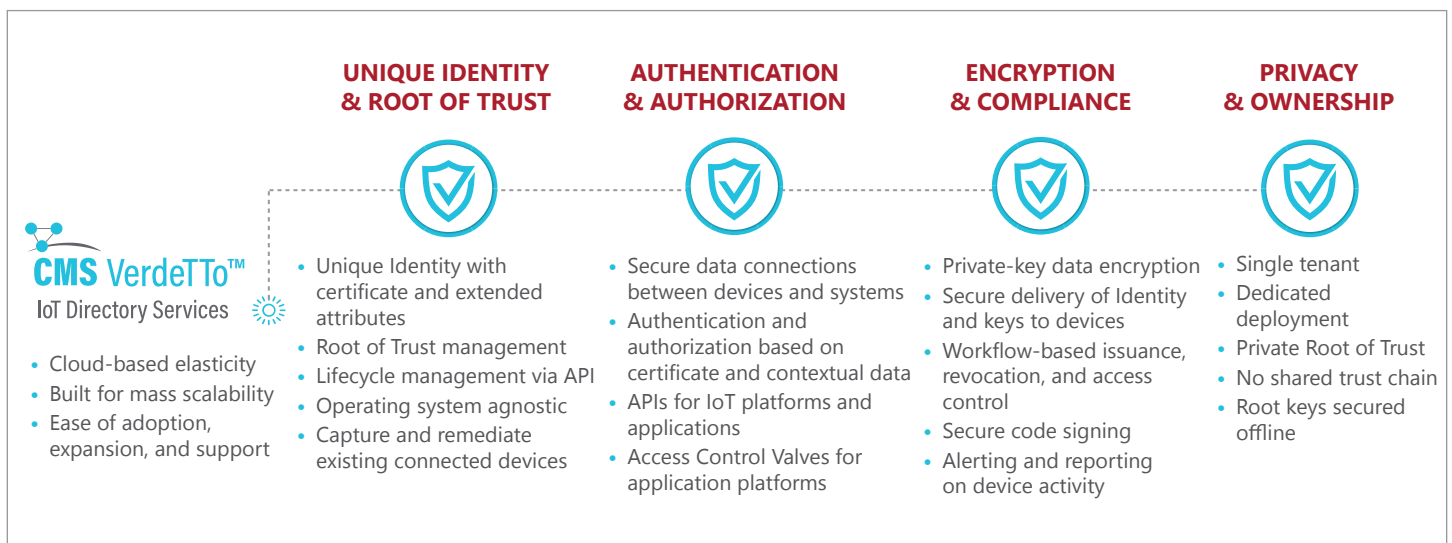


Conclusion

As the IoT landscape evolves and its security requirements shift, an IoT system built upon the ThingWorx IoT Platform must be equipped with a solid identity framework from its inception. PKI and an RoT can provide a secure foundation for IoT devices, platforms, applications, and data analytics.

CMS VerdeTTo, and the CMS VerdeTTo Access Valve for ThingWorx, provides a robust identity framework (an IoT Directory) featuring trusted digital identity. It also can help you own and manage your RoT, and provides tools for easily enabling authentication and authorization. Ultimately, this results in secured IoT devices and validated IoT data. A user friendly and scalable service, CMS VerdeTTo eliminates the need for extensive PKI management demands for your IoT operations. CSS has a rich history of partnering with businesses to secure IoT systems using software and managed services. Our PKI experts become an extension of your organization's security team. CSS can assist in addressing IoT security challenges with the knowledge, experience, and operational efficiency needed to fit the needs of any business. As your organization delves into the IoT security world, we invite you to contact us with questions. We can help identify security best practices that are needed to plan, implement, and manage a trusted and efficient IoT security solution.

Figure 6. CMS VerdeTTo Sets in Motion Comprehensive Device and Data





About Certified Security Solutions (CSS)

As the market leader in enterprise and IoT digital identity security, CSS is a cyber security specialist that helps enable secure commerce internationally. Headquartered in Cleveland, Ohio and with operations throughout North America, CSS delivers innovative software products and SaaS solutions that are scalable, economical, and easy to integrate. Visit www.css-security.com for more information.

About CSS Research

CSS Research monitors threat intelligence for more than 3.7 billion IP addresses. We offer oversight and threat intelligence for digital certificates used in SSL/TLS connections across the Internet. CSS Research also provides threat intelligence and can assist with early detection of certificate vulnerabilities.

Contact Us
css-security.com
877.715.5448

References

1. [White Paper]: Security: The Vital Element Of the Internet Of Things. Sponsored by: Forrester and Cisco. 2015.