IDC Technology Spotlight

Sponsored by: Trustify

Author:

Martin Whitworth

Research Director,
European Data Security and Privacy

June 2018

The Time Has Come for Automated Cryptographic Services to Support Identity and Trust

Introduction

Digital business is driving a wide variety of applications, business services, and data sources deployed on diverse platforms including on-premise, private cloud, hybrid, public cloud, multicloud, IoT, and operational technology (OT) environments. Now more than ever we see that the provision of competitive responsiveness without slowdowns, interruptions, or crashes is a critical success factor for organizations striving to deliver digital business imperatives.

Flexibility and agility are must-haves in this environment, and legacy systems and approaches simply can't move fast enough to keep up with the changes currently facing the modern business world.

On-demand service offerings provide a rapidly growing point of interest for organizations as they consider the level of overheads they are willing to support and the efficient delivery of system and service capabilities that as-a-service offers.

Security generally, and cryptography in particular, are examples of specialized subject areas where this kind of flexibility and agility is much in demand — and offer great opportunities for on-demand service solutions.

Enterprise Requirement for Cryptographic Services — On-Demand

An Ever- Evolving World

Your corporate data is out there — constantly changing, moving, and being accessed by people inside and outside your organization. The growing use of mobile, cloud, social media, and IoT exacerbates this constant state of flux. For this reason, the traditional data security perimeter as we have known it is disappearing.

IDC sees three overarching global trends that are dictating today's challenges in the worldwide security market. Organizations may have little control over these factors, but they are having to take full account of them in their strategy development:

- A dynamic and evolving threat landscape
- Regulatory changes (privacy, security)
- Digital transformation

Convergence

One key area of evolution is the convergence of traditional information technology (IT) with the world of OT. Traditionally, these disciplines have been kept apart, as

have the teams and systems used to manage and operate them. Valuable skills and experience, such as those relating to security and cryptography, have not been shared between the disparate teams.

Risk Management

Complexity is the enemy of security and introduces unnecessary risk to the enterprise. This, unfortunately, is the situation we find ourselves in when attempting to design, implement, and manage cryptographic systems, products, and processes, often across disparate technology realms (IT, OT, connected devices, IoT). Traditional approaches are costly, complex, and require resources that are scarce — i.e., risky!

Cryptographic products and services (including encryption/decryption and authentication) can prove to be valuable solutions and controls in our deperimeterized world.

Why Cryptography?

Cryptographic products and services (including encryption/decryption and authentication) can prove to be valuable solutions and controls in this deperimeterized world — but they are not, necessarily, well understood in many enterprises.

Data needs to be protected, wherever it is — in transit, during processing, or at rest — and it is the endpoint that becomes the focal point in the world without perimeters. The expansion of connected devices and IoT device adoption escalates, exponentially, the potential number of these endpoints that need securing and managing.

It is not only the protection of corporate or personal data that is important. In the world of IoT and connected devices, the secure distribution of firmware upgrades, and other over-the-air (OTA) updates, is increasingly challenging.

Cryptographic Management

Managing cryptographic products, systems, and processes is non-trivial. Typically, there is a struggle to find or build the right skills around the topics of key management generally, and managing public key infrastructure (PKI) in particular. Traditional systems are costly to manage manually and there have been, until now, limited opportunities to introduce automation and orchestration.

Cryptographic Skills

The design, implementation, and management of cryptographic products, systems, and processes are specialized functions. For them to be effective, they require in-depth knowledge of processes, procedures, and audit requirements that are specific to cryptography. These are not, typically, core competencies for most organizations, and acquiring and retaining these skills can be difficult and expensive — and as a result, enterprises need help.

Where is Help Needed?

As we have said, cryptography is not a core competence for most organizations and this lack of capability typically becomes very noticeable, and potentially critical, in the following key areas:

Regulatory Compliance

Concerns about data protection and privacy are unescapable. Citizens, regulators, and legislators are becoming increasingly vocal on these topics, and businesses are having to listen. The digital economy is truly global, and different geographies and industry verticals are developing and implementing their individual legal and regulatory requirements at different rates. The sheer complexity of laws and regulations — local and international — that impact data, challenges organizations to select and implement appropriate controls.

Key Management

The burden of key management and generally managing PKI is complicated and not well understood. It should be taken away from the user of the system and be incorporated into a consistent delivery layer that allows for automation and orchestration. This could also include the selection of appropriate cryptographic algorithms and key management models.

Key management should also provide support for the management of encrypted data by allowing data to be recovered even if one or more key updates have been performed. The same is true for the change in the length of cryptographic keys or even the cryptographic algorithms used in the encryption process.

User Management

Providing a consistent and scalable approach to user administration is a challenging and often complex task. Managing the credential life cycle, which typically involves cryptographic keys and digital certificates, from issuance and distribution through modification and rotation, and eventually retirement or deletion, is a non-trivial series of processes requiring sophisticated audit facilities.

Device Management

The number and types of connected devices that are components of digital business networks are growing exponentially — and they all have to be managed. As with users, an effective solution must be able to cope with the entire life cycle of the device, from implementation and enrolment all the way through to retirement and deletion.

We have already established that, in the world of digital business, the traditional network perimeter is no more. This makes the security of our network-connected devices even more important — they effectively become the new perimeter and must be appropriately secured and protected. Furthermore, as we are not operating totally within a secure perimeter, the data that flows between and resides on our connected devices must be protected. This requires the implementation and management of end-to-end encryption (E2EE).

Many connected devices provide additional challenges as they have limited storage and processing, bespoke operating systems, and are often not designed with update (or patching) capabilities as a primary capability. This is also a very dynamic environment, with new entrants constantly appearing, a demand for rapid implementation and retirement, and a shortage of skills — all putting pressure on organizations if they have to resource internally.

Integration

Cryptographic systems and processes must be capable of being efficiently and effectively integrated into the operational enterprise systems — and able to evolve as the business evolves. This requires a consistent and implementable approach, but should not require complicated rework of existing systems.

Taking a wider view, very few organizations stand alone as an island. Secure connections to suppliers, partners, and customers are key components in today's world — and these must all be implemented, managed, and monitored in a consistent and demonstrably compliant manner.

Centralized Management and Monitoring

Enabling the capability to centrally manage and monitor cryptographic services — whether for IT or OT systems — allows for an efficient, consistent, and effective solution. It is possible to devolve some controls and capabilities, but as a minimum it should be possible to centrally manage the following functions:

- Dynamically adding or reconfiguring resources to meet any increase in demand or operational issues (e.g., device failure) such that the available capacity of the system is not impacted.
- Performing BAU operational tasks such as addition of new functions or users and to interface with key management systems for the management of key material.
- Accessing audit logs for problem resolution at the application level and to check for anomalous behavior by applications.

Skills and Resources

Cryptographic and key management skills and experience are very specialized and in short supply. Most organizations are not able to build and retain a specialized cryptographic function, and nor should they — it is not their core competence. This resource and skills shortage situation is further exacerbated when we consider the need to understand cryptographic implementations in an ever-growing number of network-connected devices.

One key mitigation for the shortage of available skills and resources is to introduce the capability to automate (and orchestrate) many of the tasks associated with the management and operation of cryptographic solutions.

The Trustify Approach

The Company

Trustify is a U.K.-based company that has built its expertise in managing specialized PKI projects for several international clients over many years. Through these efforts it has accumulated a depth of knowledge and expertise in cybersecurity and has used this to help define and develop its own cyber-risk management tools.

With its cybersecurity and embedded systems expertise, Trustify has expanded its view and engaged heavily in many different verticals and, working with key

partners, has focused on the problems of securing data and devices in the connected but perimeterless environment. This has led to the development of an Enterprise Crypto Service offering.

Trustify is looking to take the pain away from its customers — not only reducing demands on skilled staff, but also mitigating existing risks.

Trustify Crypto Service Offering

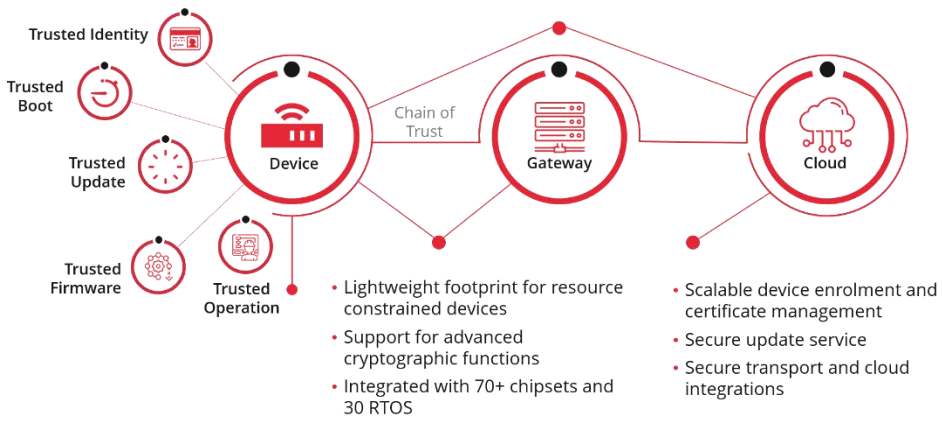
Trustify provides a chain-of-trust offering to implement a data protection on demand service. The protected chain-of-trust extends from the connected devices, users, and data through to the hardware security module (HSM) providing fundamental cryptographic services and trust points.

The Crypto Service platform recognizes certificates and devices from disparate sources, authenticating and tracking them throughout their entire life cycle. At the same time, devices or applications that are not already chain-of-trust–ready can be protected via the high-volume, high-velocity certificate issuance capability.

Trustify is approaching this from a perspective of taking the pain away from its customers. Through flexible service level agreements (SLAs), it is offering a range of service options — including facilitating automation of cryptographic management functions — aimed at both IT and OT systems. This approach not only reduces demand on skilled staff, but also helps to mitigate risks by providing a consistent end-to-end approach and centrally manageable solution.

Trustify Root of Trust

Figure 1
Trustify IoT Security



Source: Trustify

A key factor in Trustify's approach is that it looks at the end-to-end nature of the problem space and has designed the solution to address this.

Connected devices, IoT, and OT are a particular focus for Trustify, where it is a recognized expert, and the company delivers a solution that provides protection and end-to-end-encryption through:

- Lightweight footprint for resource-constrained devices
- Support for advanced cryptographic functions
- Integration with many chipsets and real-time operating systems (RTOS)
- Scalable device auto-enrolment and certificate management

- Secure update service
- Secure transport and cloud integrations

A key factor in Trustify's approach is that it looks at the end-to-end nature of the problem space and has designed the solution to address this. Notable examples of this line of attack can be found in its end-to-end discovery, update, and analytics capabilities and the attention paid to the distribution of crypto to IoT devices.

Reinvigorating PKI

PKI implementations have historically suffered from confusion about what issues they can address and how PKI can help. Usage has also been restricted by the belief that PKI can only be implemented by utilizing very scarce technical resources and that complex processes need to be put in place to manage it. Trustify is changing the approach to PKI — enabling PKI implementation by making it easier, for example, to:

- Provide automation capabilities to ease the burden of having to implement onerous manual processes
- Offer multiple, centrally managed, implementation options — on-premise, cloud based, or hybrid
- Offer the option of a fully managed, outsourced solution

By taking the pain away from the customer, effective PKI solutions can be implemented across IT, OT, and IoT.

The Challenges Ahead

Through its partnerships, Trustify is already having an impact in many sectors (including retail, financial services, healthcare, and industrials). It is also very focused on IoT and connected devices in sectors such as oil and gas, power generation, smart cities, healthcare, and utilities.

An additional challenge for Trustify, however, comes from those that propose blockchain as the answer to all problems — ignoring the fact that PKI is fundamental to blockchain success. The key for Trustify will be translating its message to address the needs of the various, often non-traditional, audiences and roles involved in digital transformation programs.

Trustify has an attractive proposition to assist those seeking to make their digital business initiatives a success — across diverse platforms (especially encompassing OT and IoT).

IDC UK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.