

The Observatory

Europe

March 2021



Insight

Blu5

A Viable Replacement to the Existing
CA-based PKI for IoT Devices



A Viable Replacement to the Existing CA-based PKI for IoT Devices

Author: [Giorgia Somma](#), Business Development Manager & [Antonio Varriale](#), Group CTO at [Blu5](#)

At a glance

- 5 minute read 🕒
- IoT rapid expansion and complexity
- IoT security: the present
- Future suitability of current IoT security technologies
- The next steps to a CA-PKI alternative



IoT rapid expansion and complexity

The internet of things (IoT) is proliferating across consumer products, industrial operations, and supply chains. Gartner's IoT forecast is showing that, by 2029, more than 15 billion IoT devices will attach to the enterprise infrastructure [1]. Previously, devices were "air gapped" meaning they had no connectivity at all or, in some other cases, they had a dedicated, isolated custom-designed network using proprietary protocols.

Nowadays IoT is more often about connecting smart devices to standard IT types of networks, including the Internet and, in some cases, to Cloud computing platforms, for analytics and data processing.

What's more, IoT deployments spread these connected devices around the world in locations that traditionally would not be populated by smart devices, such as a patient's home, a remote utility grid site, or on a transportation network. The IoT ecosystem is extremely complicated, fragmented, and evolving. The need for security has never been greater in such ecosystems.

Scaling to massive deployments naturally introduces a number of complexities: more complex devices, more complex connectivity, more complex deployments, and more complex management at scale.



"The IoT ecosystem is extremely complicated, fragmented, and evolving. The need for security has never been greater in such ecosystems."

As the Security Expert Bruce Schneier says, “Complexity is the enemy of security”. Security becomes critical since the attack surface expands in intricate and profound ways when connecting billions of new and previously unconnected devices. Let’s briefly analyse how this complexity is being addressed from a security perspective.

IoT security: The Present

Every device needs to connect securely to another to verify its own identity as well as the identities of others upon connection. This is to ensure that information is not sent to an unauthorised recipient or received from an untrusted sender and is needed by devices on the Internet of Things (IoT) as much as any other device connected to a network.

The traditional way to protect data from unauthorised access is through a Public Key Infrastructure (PKI) and

Transport Layer Security (TLS). PKI (Public Key Infrastructure) offers a one-size-fits-all solution for all IoT devices, however unique they are.

It employs X.509 digital certificates to identify devices. This certificate is then signed by a Certificate Authority (CA) that confirms that the information in the certificate is legitimate. The CA, in turn, has its self-signed certificate attesting its identity.

PKI is a core component of TLS since TLS relies on Public Key Infrastructure for authentication. Transport Layer Security is becoming the de facto standard to provide end-to-end security on the current Internet. IoT scenarios are not an exception since TLS is also being adopted there. Considering the expansion of IoT deployments and their peculiarities, it is necessary to evaluate the potential challenges of using TLS and PKI in these scenarios.



“Considering the expansion of IoT deployments and their peculiarities, it is necessary to evaluate the potential challenges of using TLS and PKI in these scenarios.”

Future suitability of current IoT security technologies

IoT platforms consist of heterogeneous, often constrained, devices with complex network stacks. The design of security services that provide fine-grained access control, authentication and confidentiality are a challenge for most devices in the IoT. Traditional solutions are often ill-suited for IoT architectures as they have a large computational overhead and require ubiquitous connectivity of the smart devices.

PKI/CA offers a one-size-fits-all solution for all IoT devices, however unique they are and so, is very often unsuitable for each and every IoT architecture. Some of the main concerns about PKI/CA are:

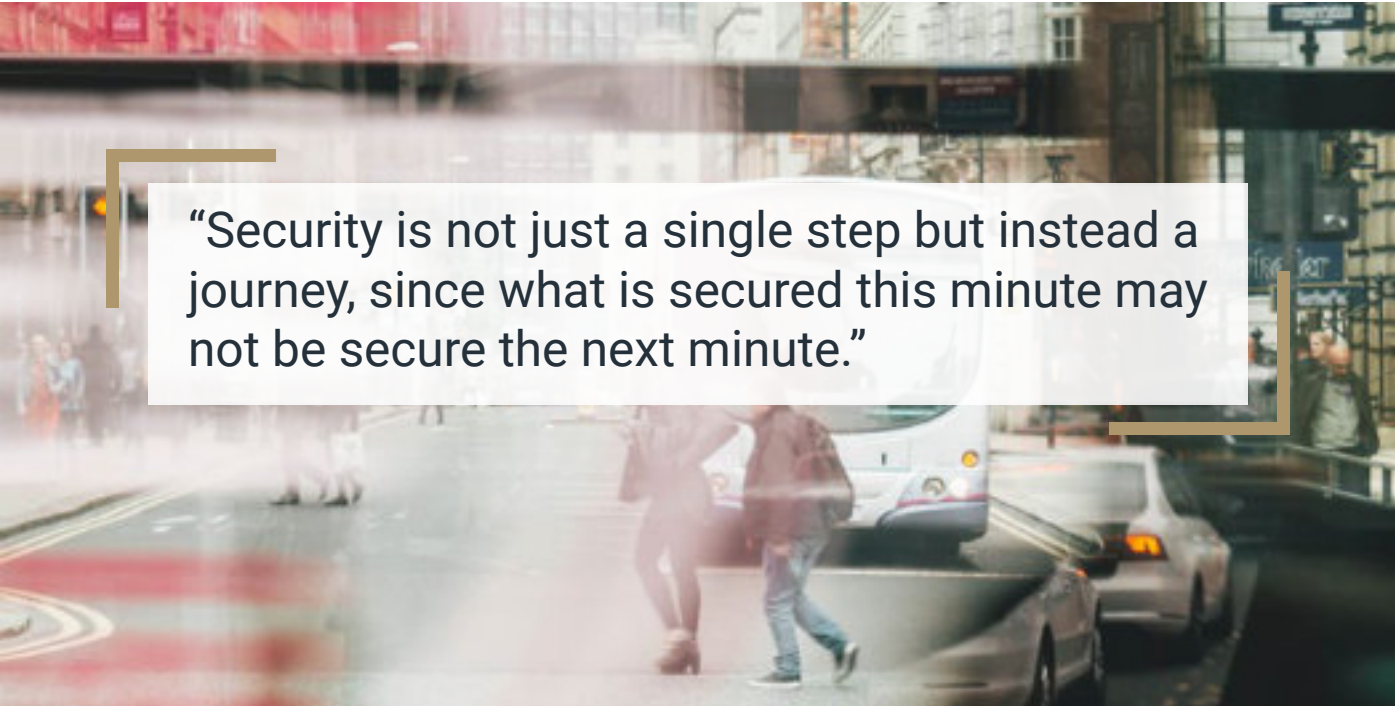
1. PKI relies on the fundamental principle that the certificates of the CA need to be trusted. The idea of trust on the Internet has been increasingly abandoned in the past years. Quoting Gartner's analysts, the Internet is a cesspool of attacks [2].
2. Certificate life-cycle management is still the age-old challenge. The large number of devices, connectivity, device life time as well as time of manufacturing cause a problem in maintaining an updated list of trusted CA in each device.
3. Many customers may need to rely on external vendors for their certificates.
4. Certificate management can be costly and adds to total solution

cost since PKI/CA requires a large infrastructure to manage certificates and requires each IoT device to have at least one certificate for client authentication.

5. Distribution of certificates for many devices is impractical and nearly impossible.
6. They have a large computational overhead and require constant connectivity of the smart devices.
7. Existing security solutions may not be applicable to all IoT domains, in particular those designed with resource constrained devices.
8. The significant threat of Quantum-computing behind current PKI design.

Companies in the IoT industry have noticed important limitations to the past and current state of the technology and want to gain more knowledge on the subject, especially where it affects their current and future products and solutions.





“Security is not just a single step but instead a journey, since what is secured this minute may not be secure the next minute.”

The next steps to a CA-PKI alternative for IoT

There are three primary considerations organisations should make when choosing a solution to protect information especially when dealing with constrained, typically embedded IoT devices: Security Level, Performance and Cost.

Security Level

IoT introduces new challenges in terms of energy and power consumption. It is therefore desired that device cryptographic capabilities designed for IoT should be based on lightweight protocols and frameworks. Besides, security is not just a single step but instead a journey, since what is secured this minute may not be secure the next minute. Quantum computers present new threats to existing cryptographic solutions as demonstrated by Peter Shor’s quantum algorithm that breaks RSA, ECC.

This means that in this model all commonly used public-key systems are no longer secure [3].

However, Quantum computing will not affect all types of cryptography in the same way. Organisations that have very little use for PKI, but are rather using symmetric cryptography, may have little risk and could afford to wait.

In other cases, like the IoT, where quantum risk is not tolerated, system owners should act now by implementing quantum-safe technologies.

To minimise the risk, organisations should consider the following:

- Making an inventory of public key systems in use
- Assessing future and retroactive risk from quantum computers
- Taking action to urge the adoption of quantum-safe solutions
- Building cyber-resilience and cryptographic agility into the digital infrastructure to smooth cryptographic transitions

Performance

The dual challenges of ownership and CA agility faced by PKI administrators during deployment are worrying as they directly impact on efficiency as well as security. Some organisations may have several CAs deployed in their network or rely on several third-party CAs and thousands of SSL/TLS certificates spread throughout the infrastructure.

As organisations push for more rapid and efficient deployment of business applications, tracking certificate ownership in such scenarios is a difficult task and may become impossible, let alone the risks resulting from the lack of control of CAs, such as increased costs, trust issues, security risks because of CA compromise. Besides, performance of IoT devices is strongly affected by the additional overhead imposed by cryptography in terms of computation, memory, storage, network bandwidth, which makes it that protection used on traditional networks cannot be readily deployed on IoT networks.

IoT introduces new challenges in terms of energy storage and power consumption. It is therefore desired that

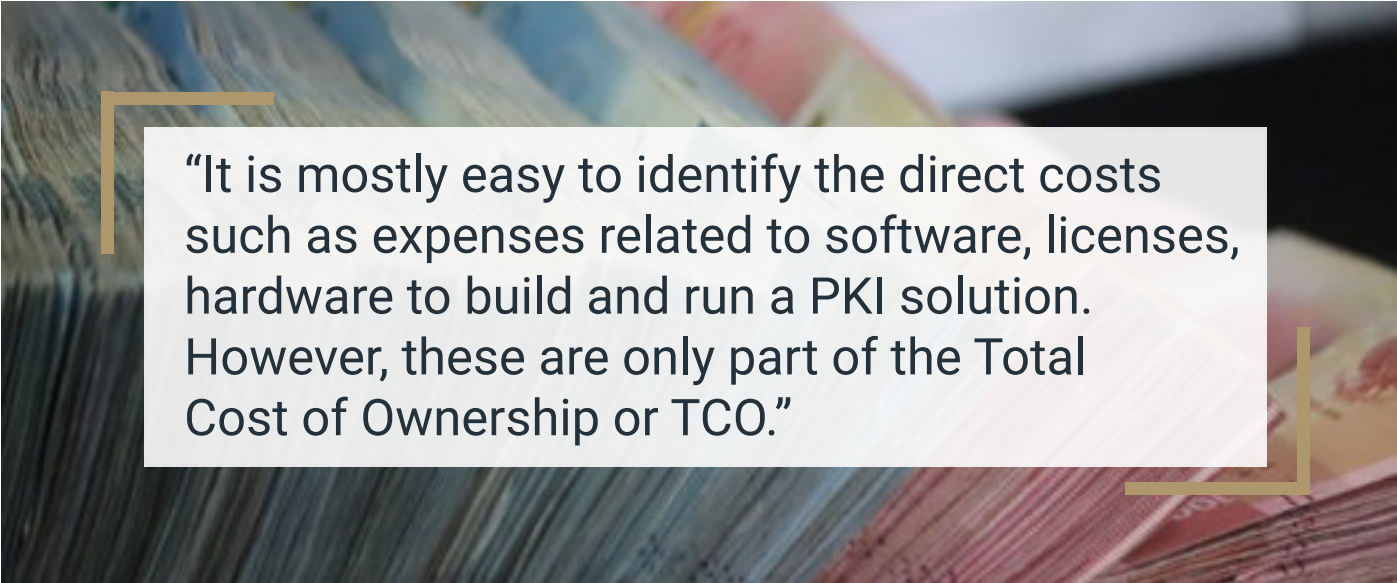
device cryptographic capabilities designed for IoT should be based on lightweight protocols and frameworks.

Cost

Implementing a cutting edge PKI infrastructure is costly and often complex to build and maintain. It requires for you not only to invest in the infrastructure and build expertise but also to permanently upgrade the changing technology and evolve with new security threats.

It is mostly easy to identify the direct costs such as expenses related to software, licenses, hardware to build and run a PKI solution. However, these are only part of the Total Cost of Ownership or TCO.

To build and maintain a PKI solution, there are many different cost components to consider. These include amongst others project management, the organisation of regular audits, monitor threats and technology evolution and migration to a new security infrastructure. Industries and organisations must compare the potential costs of using outdated cryptographic standards to the costs of transitioning to the new standard.



“It is mostly easy to identify the direct costs such as expenses related to software, licenses, hardware to build and run a PKI solution. However, these are only part of the Total Cost of Ownership or TCO.”

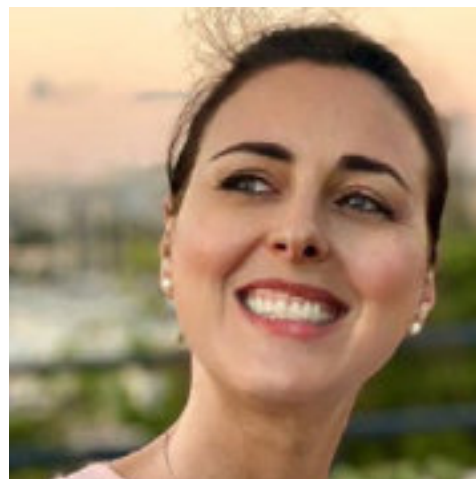
Such problems with cryptographic transitions are leading to growing calls for a focus on cryptographic agility and cyber resilience (i.e., resistance to failure due to cyberattacks). Cryptographic agility comes with the potential benefits of lower transition costs and greater security due to ease in transitioning away from newly discovered security flaws.

SElink™ is the evolution of traditional ways to protect data from unauthorised access like Public Key Infrastructure (PKI) and Transport Layer Security (TLS). Suited for your end-to-end security (authentication, confidentiality, and integrity) between endpoints, nodes and servers achieved with future-proof security, zero encryption overhead, low bandwidth consumption, minimum resources, Quantum-safe. SElink™ the most appropriate technology for resource-constrained devices and for high system availability.

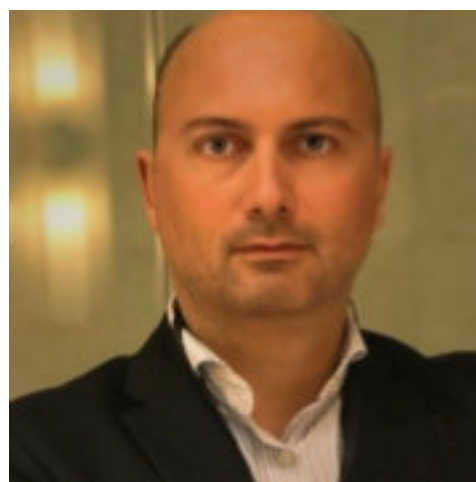
References: [1] Gartner: Predicts 2021/ Cloud and Edge Infrastructure Cloud Infrastructure Edge, February 2021.

[2] Gartner: It's Time to Isolate Your Services From the Internet Cesspool, November 2017

[3] Enisa: Post-quantum Cryptography. Current State and Quantum mitigation. February 2021



Giorgia Somma
Business Development
Manager, Blu5



Antonio Varriale
Group CTO, Blu5

“Cryptographic agility comes with the potential benefits of lower transition costs and greater security due to ease in transitioning away from newly discovered security flaws.”



The
Cyber Security
Observatory

Europe - Third Edition