EVIDEN

4G to 5G Migration

How PKI secures Telco use cases

an atos business

Introduction

The objective of this document is to describe security challenges for the telecommunication industry, and in particular those arising through the 4G (LTE) to 5G migration. By proposing Public Key Infrastructure (PKI) as a means to efficiently protect Telco ecosystem, the document targets mainly CISOs who wish to learn more about industry approaches of 5G security and how to implement PKI for telecommunications use cases.

When analyzing the evolution of cellular networks, we can clearly observe that 5G represents a new chapter in network technologies, as it opens the door to much more than communication and data exchange between entities. Indeed, this new technology focuses on the fact than Radio Access Networks (RAN) will be handling a very large number of devices, individuals, and applications alongside two major and fundamental trends, namely IOT deployments & Cloud based solutions.

Unsurprisingly, with the explosion of the number of network elements comes increased vulnerability as the attack surface increases consequently. Hence, two major concerns arise:

- How to trust that only legitimate entities are involved?
- How to protect data at rest and in transfer?

For both questions, this document aims to demonstrate that Public Key Infrastructure (PKI) technology is perfectly adapted to tackle existing and future security challenges for 5G

Background

Telecom operator infrastructures have been identified since some time already as mission critical systems. As a result, an EU Commission recommendation led to the “5G cybersecurity toolbox”, adopted in January 2020 and which had impacts also on national legal frameworks.

LTE (Long-Term Evolution) is a 4G wireless communication technology that offers high-speed mobile data and voice services. It significantly improved data transfer rates and reduced latency compared to earlier 3G networks.

Nowadays, the whole Telco industry switches to 5G, the fifth generation of wireless technology, representing a leap forward in connectivity with even higher data speeds, ultra-low latency, and massive device connectivity.

Enhanced speed introduces new possibilities for entertainment, productivity, & communication

Low Latency enables real-time communication and responsiveness crucial for applications like online gaming, telemedicine, and autonomous vehicles.

IoT Connectivity allows to handle a massive number of connected devices simultaneously. This is particularly essential for the IoT, where billions of devices, from smart home appliances to industrial sensors, will be interconnected.

Thus, 5G offers new possibilities for Industrial and Healthcare Applications, Autonomous Vehicles and Smart Cities.

On the other, one must bear in mind that migrating from LTE/4G to 5G presents several challenges and security concerns, such as:

Security Gaps: 5G networks introduce new attack vectors, such as increased surface areas for cyberattacks due to a larger number of connected devices & new protocols. Ensuring the security of these networks is crucial.

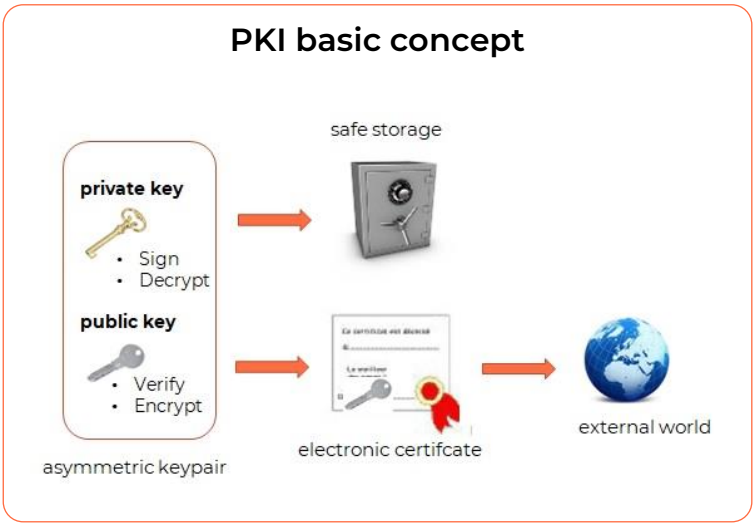
Privacy Concerns: With 5G's ability to process and transmit massive amounts of data in real-time, privacy concerns arise. Protecting sensitive user data and ensuring compliance with privacy regulations is paramount

Cyberattacks: As 5G becomes central to critical infrastructure, it becomes a prime target for cyberattacks. Ensuring the resilience of 5G networks against threats like DDoS attacks and ransomware is vital.

Authentication and Identity Management: Secure authentication mechanisms are needed to ensure that only authorized devices and users can access the network.

Regulatory Compliance: Compliance with various cybersecurity regulations and standards becomes a challenge, requiring rigorous adherence to guidelines

PKI at a glance



In a nutshell, Public Key Infrastructure is a technology based on asymmetric cryptography, which makes use of very long prime numbers, and which form a keypair, to manipulate data. Without going into details, a keypair consists of a private key and a public key and is used to perform actions like encryption/decryption and signature/verification to guarantee authentication, confidentiality, integrity, and non-repudiation. The private key is a crucial, sensitive information that must be kept in secure place, whereas the public key is shared with all entities.

In order to distribute public keys in a trustworthy manner, an electronic certificate is issued by a trusted authority, aka the Certification Authority, typically a company, an organization, a bank, a government people usually trust as reference.

PKI is governed by many international standards (X.509v3, PKCS, RFC 5280, ...) and is a proven, deployed technology since the mid 90's.

How PKI responds to 5G security challenges

Overall, PKI provides a robust framework for establishing trust, securing communication channels, and verifying the authenticity and integrity of devices and data within 5G networks. This security foundation is vital to protect against various threats and vulnerabilities, making 5G networks more resilient and trustworthy. In this context, Public Key Infrastructure (PKI) plays a crucial role, offering secure authentication, data encryption, and integrity checks to 5G networks.

Secure Authentication

Certificate-Based Authentication uses digital certificates to authenticate devices and users in 5G networks. Each device or user is issued a unique certificate, signed by a trusted Certificate Authority (CA). This certificate-based authentication ensures that only authorized entities can access the network.

Mutual Authentication is performed when both the network and the device authenticate each other. This two-way verification enhances security by preventing unauthorized access and man-in-the-middle attacks.

Data Encryption

10101
01010
10101

End-to-End Encryption facilitates the establishment of secure, end-to-end encrypted connections between devices and the network. When data is transmitted, it is encrypted using the recipient's public key, and only the recipient's private key can decrypt it. This ensures data confidentiality & privacy.

Secure Key Exchange helps securely exchange encryption keys between devices. The use of asymmetric encryption for key exchange ensures that even if a malicious actor intercepts the keys, they cannot decipher the encrypted data without the private key

Integrity Checks

Digital Signatures allow to verify the integrity of data at rest and in transit. Data packets can be signed with a private key, and the recipient can verify the signature using the sender's public key. If the data has been tampered with during transit, the signature will fail validation, indicating potential tampering.

Certificate Revocation informs network components by means of certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) whether a device or user's credentials is compromised or not.

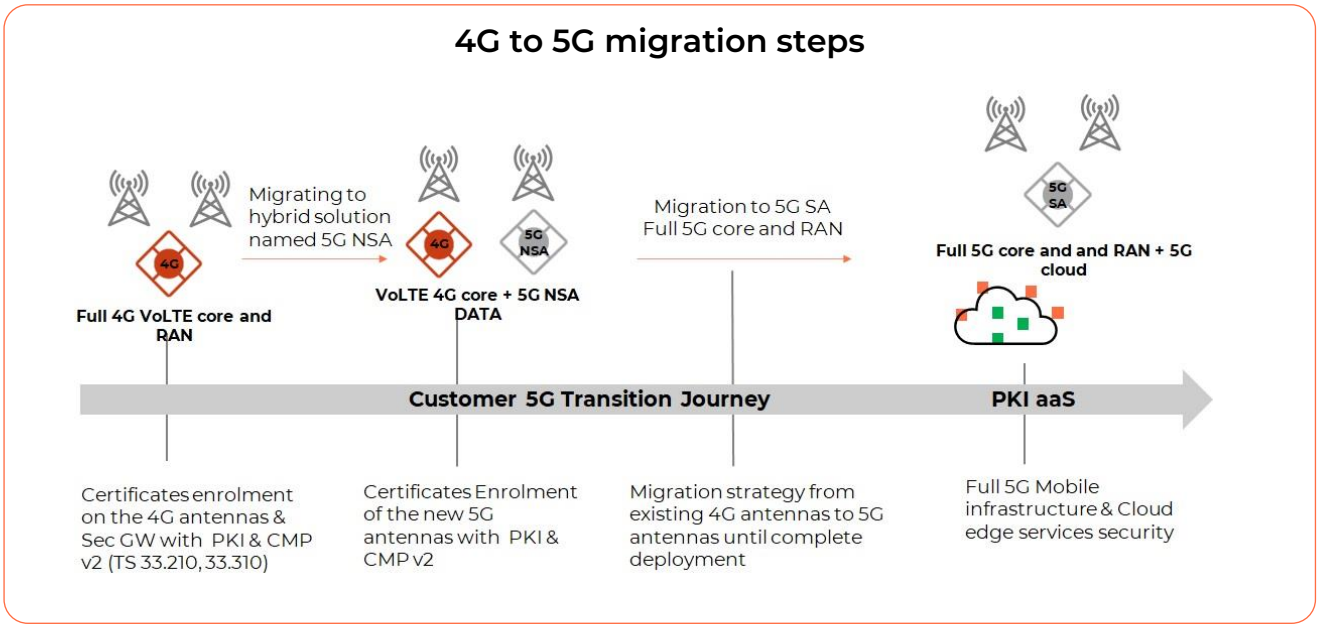
Migration Roadmap

PKI is a fundamental security mechanism that fortifies 5G networks, ensuring their security, trustworthiness, and compliance with stringent security requirements. It provides the foundation for secure communication, identity verification, and data protection in the evolving landscape of telecommunications.

Within this document, we are focusing on 4G (LTE) to 5G migration, as this infrastructure deployment issue is to be tackled prior to any more application-oriented projects.

In this domain, security awareness has much increased, leading to the endorsement of PKI technology by 3GPP standards such as TS 33.210, TS33.310, and TS.401. Therefore, one of today's challenge for CISOs is the swift change from 4G to 5G antenna networks.

The following figure illustrates the migration roadmap and its stakes:



Interactions with PKI

In essence, the process deals with generating for each network element (antennae and gateways) a digital identity, represented by an electronic certificate. These certificates must be deployed onto the respective devices.

Following a step-by-step approach, projects are often migrated using the existing 4G infrastructure (Non Standalone, NSA), before deploying a 5G dedicated one (Standalone, SA).

A major element in the deployment process is enrollment, i.e. the distribution of digital identities in form of electronic certificates to all antennae and gateways. The Certificate Management Protocol CMPv2 (RFC 4210) has been chosen by the 3GPP standards to be the enrollment protocol to use.

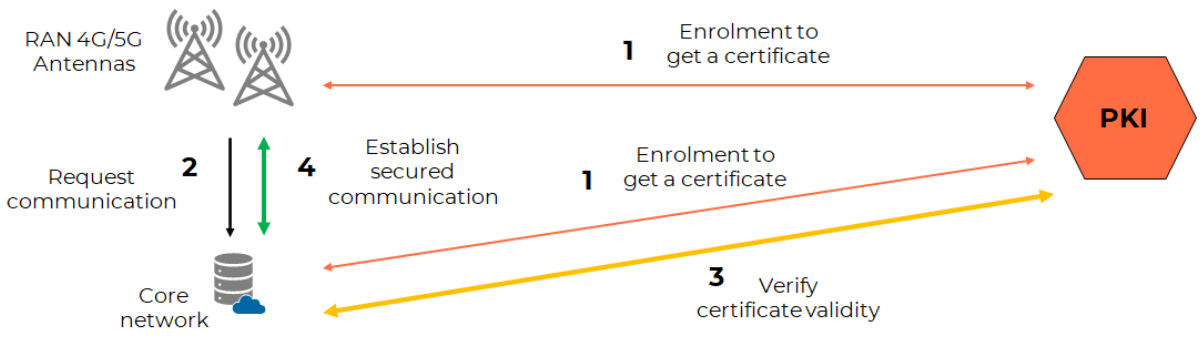
From a practical point-of-view, implementing standard based communication interfaces is a wise and sustainable approach, as interoperability is ensured, and evolutions managed in line with industry standards. Also, new projects can benefit from successful deployments by choosing products that have been tested with the widest set of different equipment in other projects.

The next figure explains step-by-step the interaction between PKI services and network elements.

1. The element (antenna) requests its digital identity (electronic certificate)
2. After reception, the antenna requests communication with the core network
3. The core network verifies towards the PKI that the antenna's certificate is valid, before engaging an information exchange
4. Upon validation, a secure connection between antenna and core network is realized.

With this trust relation successfully established, one can now cover the two major security concerns depicted before in our introduction, namely to ensure that only legitimate entities are connected and that all communication is protected by means of electronic certificates.

Telco network interactions with PKI



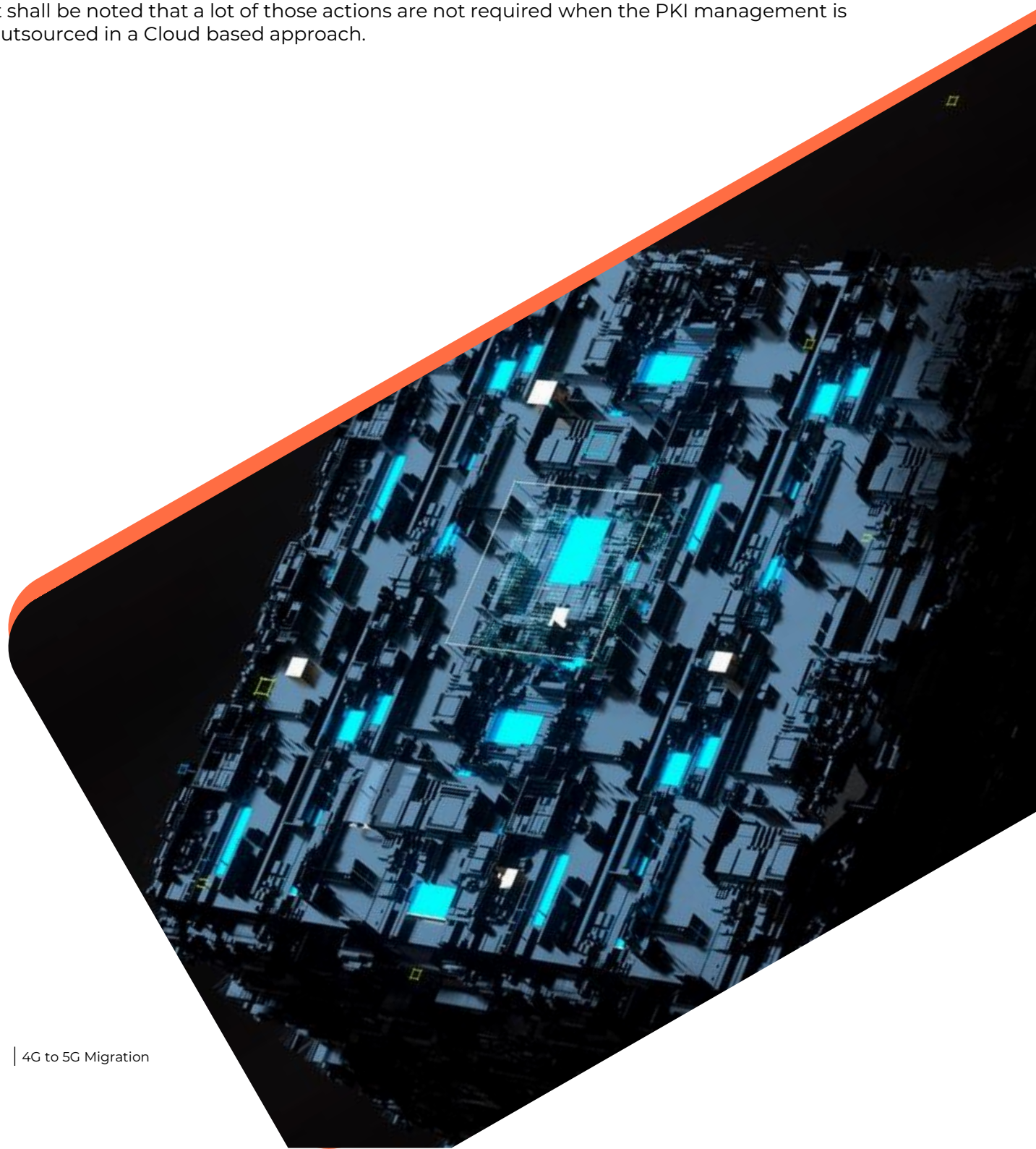
How to deploy PKI services?

Implementing such PKI services is nowadays a quite easy endeavor, especially since standards are guiding Telco players. Besides defining the PKI hierarchy (Certification Authorities and certificates with their respective properties), one must make sure that the target network devices can manage the cryptographic algorithms required. This can be achieved by dedicated crypto-microcontrollers or additional secure elements that interface with the network device.

Once the PKI system set up, configured, and initialized, each device will submit requests for electronic certificates to use.

In case the technical infrastructure is implemented “On Premise”, the Telco has a certain number of administrative and operational tasks to fulfill, such as the lifecycle management of certificates, maintenance of the PKI platform, management of cryptographic keys.

It shall be noted that a lot of those actions are not required when the PKI management is outsourced in a Cloud based approach.



Eviden’s PKI offer for 5G security

Eviden provides IDnomic PKI, a software suite enabling the management of trusted IT infrastructures based on the X.509v3 standards.

It provides powerful and advanced PKI services to secure organizations, ensure their IT governance and compliance, and simplifying the process of your digital identity management. With a strong focus on flexibility and functional richness, all industry segments can benefit from IDnomic PKI features, enabling them to implement all type of use cases required.

Especially for Telecommunication use cases, one can rely on many enrollment protocol connectors, which ensure that all kind of network devices can be equipped with digital certificates. A particular focus is CMPv2 for 4G to 5G migration. The connector has been qualified with various antenna providers such as Nokia, Ericsson, Huawei, and Samsung.

Focusing on high performance, high throughput, and multi-tenancy, IDnomic PKI exposes important characteristics that are decisive for Telco IOT deployment projects, that need to produce and manage hundreds of million digital identities.

Find more information on PKI, 5G security, and other digital identity use cases on our website: www.idnomic.com/

EVIDEN

About Eviden [1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 55,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

About Atos

Atos is a global leader in digital transformation with 107,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

1 Eviden business is operated through the following brands: Alia Consulting, AppCentrica, ATHEA, Atos Syntel, Bull, Cloudamize, Cloudreach, Cryptovision, DataSentics, digital.security, Eagle Creek, EcoAct, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Miner & Kasch, Motiv, Nimbix, Processia, Profit4SF, science+computing, SEC Consult, Visual BI, Worldgrid, X-Perion, zData.

Connect with us

eviden.com