

#### Becoming a 5G PKI



#### Antonio Pedone

Service Manager Telecom Italia Trust Technologies

### Agenda

- 1. PKI participants
- 2. Mobile networks basics
- 3. PKI service model in 3GPP networks
- 4. CMPv2 in depth
- 5. Conclusions

## The QTSP TrustTechnologies

Telecom Italia **Trust Technologies** is a TIM Group company, accredited as a European Qualified Trust Service Provider, with **20+ years** of experience in PKI services and develops, integrates and delivers solutions for Digital Transformation:

- Digital Identity of people and things;
- Rationalization of business processes;
- Dematerialization, management and storage of data and documents.



## The Customer

the leading ICT group in **Italy** and Brazil.

For the purpose of this presentation, TIM is the customer who had the need to **secure its 4G/5G mobile network**.

In terms of customers in Italy, key numbers at September 30, 2022, are:

#### 30.5 million mobile lines

- 16 million fixed lines
- 10.5 million fixed ultra-broadband lines
- Over 94% fixed ultra-broadband coverage (FTTx)



#### 3GPP

3<sup>rd</sup> Generation Partnership Project

It is a collaboration between telecommunications organizations, which aims to produce **globally applicable technical specifications** for third-generation (3G) mobile systems, as well as enhancements to 4G and 5G mobile systems.

3GPP specifications are used by mobile network operators and equipment manufacturers around the world to ensure that their networks and devices are **compatible with each another**.

3GPP topics are grouped in series.

**33.310** handles the specifications for "Security Aspects" (33) and "**Network Domain Security** (NDS); **Authentication Framework** (AF)" (310).

## PrimeKey

#### by KeyFactor





As mobile networks have become more critical to society, they have also become a target for cyberattacks, leading to more focus on infrastructure security. As operators have progressed from 4G to 5G infrastructure, ensuring security has become more difficult through the growing number of vendors and devices, and thereby more complex processes.

With the customer experience of utmost importance, operators have adopted standard-based approach (3GPP) for the development and integration of solutions for digital identities for infrastructure components across the national and international networks.

ment to secure the delivery of services to over 90 million oustomers across its fixed, mobile, and cloud infrastructures and data centres. The TIM Group portfolio of services and products for communication and entertainment are complemented by IoT capabilities that provide an integrated digital solution for citizens, businesses, and public administrations.

For the TIM Group, a leading telecommunication and ICT solution provider in Italy and Brazil, it is a critical require-





## Mobile network background



eNodeB/gNodeB → wireless base stations that provide wireless access for users

**Core Network** → backbone of the 4G/5G network and control/administration functionalities

**IP-RAN Backhaul** → transport of data from the base stations to the Core Network.

## Backhaul secured by 3GPP

#### Architecture of 4G/5G mobile networks



Without additional security, the interface that carries user data has authentication mechanisms but **no encryption**.

#### **3GPP requires:**

- 1. Use of IPSec Encapsulated Security Payload Protocol (ESP)
- 2. Authentication IKEv2 based on **certificates** issued by a specific CA (**Operator CA**)

#### **PKI Service Model**



..and some number:

- 70 security gateways
- 55.000 base stations
- 5 different vendors

## Better if done by a PKI specialist"

Keyfactor | #TechDays2023

## The QTSP

The **eIDAS** Regulation covers multiple types of electronic solutions at the European level and provides one single **framework** for electronic Identification (eID) and **trust services**.



A **QTSP** (**Q**ualified **T**rust **S**ervice **P**rovider) to provide qualified digital certificates under eIDAS has to guarantee at least:



Infrastructures with physical security facilities





Processes, procedures and compliance to rules and standards



Deep knowledge of x.509 certificates profiles and HSM management



por hierarchie	*
Paid	Take .
Adjust for United for	Juli Pare March Mademinia
Etheral loy inge	Sever Authention (3.3.6
Cartificate Policies	()CartRole PolicyPolicy Me
CR. Dahladar Park	(00% Debilisher Part) Deb
Arterio Monator	kome ((Authority (H) Acome Acc
107 M	<ul> <li>artistation</li> </ul>
Charles Connected	<ul> <li>vit, ad Parts (CTD) all bridges.</li> <li>tot formation all of formation all bridges.</li> <li>total formation all of formation all bridges.</li> </ul>
EAC of Constant of Constant of Constant Constant of Constant Of Constant of Constant Of Constant Of Constant of Constant Of Co	vi, arfankistraaseadan. 19 Tana oo balkahaa Tana Santa Santa Santaa Nata

## elDAS Subject Identification



De-visu (physical presence in front of a local Registration Authority)



Subject Identification is the main duty of a CA.



VideoID (remote identification using a dedicated video operator)





With eIDAS, services identification can be done in sevaral ways



E-ID (SPID) or Digital Signature (using existing Qualified Certificate)



#### The downside

## I'm used to deal with persons, how should I trust devices ? "



# CMPv2 does all the work for you ! "





## CMPv2 messages

**CMPv2** (Certificate Management Protocol, specified in IETF RFC 4210) defines protocol messages for **X.509v3 certificate creation** and management.

- Initialization request (IR)
- Initialization response (IP)
- Certification confirm (certConf)
- Confirmation (**PKIconf**)

Device 1. Discover CA Address 2. Generate public/private key pair 3. Sign initialization request (IR) 4. Send Initialization Request (IR) 5. Authenticate initialization request (IR)6. Generate base station certificate 7. Sign Initialization Response (IP) 8. Receive Initialization Response (IP) 9. Authenticate Initialization Response (IP) 10. Sign Certificate Confirm (certconf) 11. Certificate Confirm (certconf) 12. Authenticate Certificate Confirm (certconf) 13. Sign Confirmation (pkiconf) 14. Confirmation (pkiconf) 15. Authenticate Confirmation (pkiconf)

.

. . . . . . . . . .

### CMP – IR authentication



- 1 Base station pre-provisioned with a private/public key pair and a certificate signed by a Vendor CA
- 2 Issuing Operator CA configured to **trust** the certificate of the **Vendor CA** and the **DN** of the base station
- **3** Base station signs the **IR message** by the vendor provided certificate/key
- **4** Operator CA **authenticate** initial certificate requests through:
  - a) Validation of IR signature up to Vendor CA certificate
  - b) Proof-of-possession of the private key
  - c) Validation of Identity (subjectDN) of end-entity
- 5 Operator CA **issues** the end-entity certificate and sends it back to the base station

#### CMP – KUR authentication



- 1 Base station signs the **KUR message** by private key related to the last received operator base station certificate
- 2 Operator CA **authenticate** key update certificate requests through:
  - a) Validation of KUR signature up to its (Operator) CA certificate
  - b) Proof-of-possession of the private key
  - c) Validation of Identity (subjectDN) of end-entity
- 3 Operator CA issues the new end-entity certificate and sends it back to the base station

#### **PKI** Architecture and Roles



#### **PKI Hierarchy**

**Operator Root CA** 

#### **Operator Issuing Sub-CAs** :



Vendor 2 (**eNodeB**)

•••••

- Vendor n (**eNodeB**)



# In an increasingly complex world, we all need certainty"



Speed 20 GB/s Latency 1-4 ms Mobility Up to 500 Km/h 1 Mln device per Km2



Mobile Private Networks



lot services







#### the same PKI service model can be applied

#### References

[CMP] IETF RFC 4210: "Internet X.509 Public Key Infrastructure Certificate Management Protocol" [3GPP] TS 33.310 Network Domain Security (NDS); Authentication Framework (AF) [eIDAS] Regulation (UE) n. 910/2014

**CUSTOMER STORY** (available on PrimeKey website) "Powering 5G innovation through security, open standards and flexible integration"

#### Thanks for your attention !

