ITUWebinars

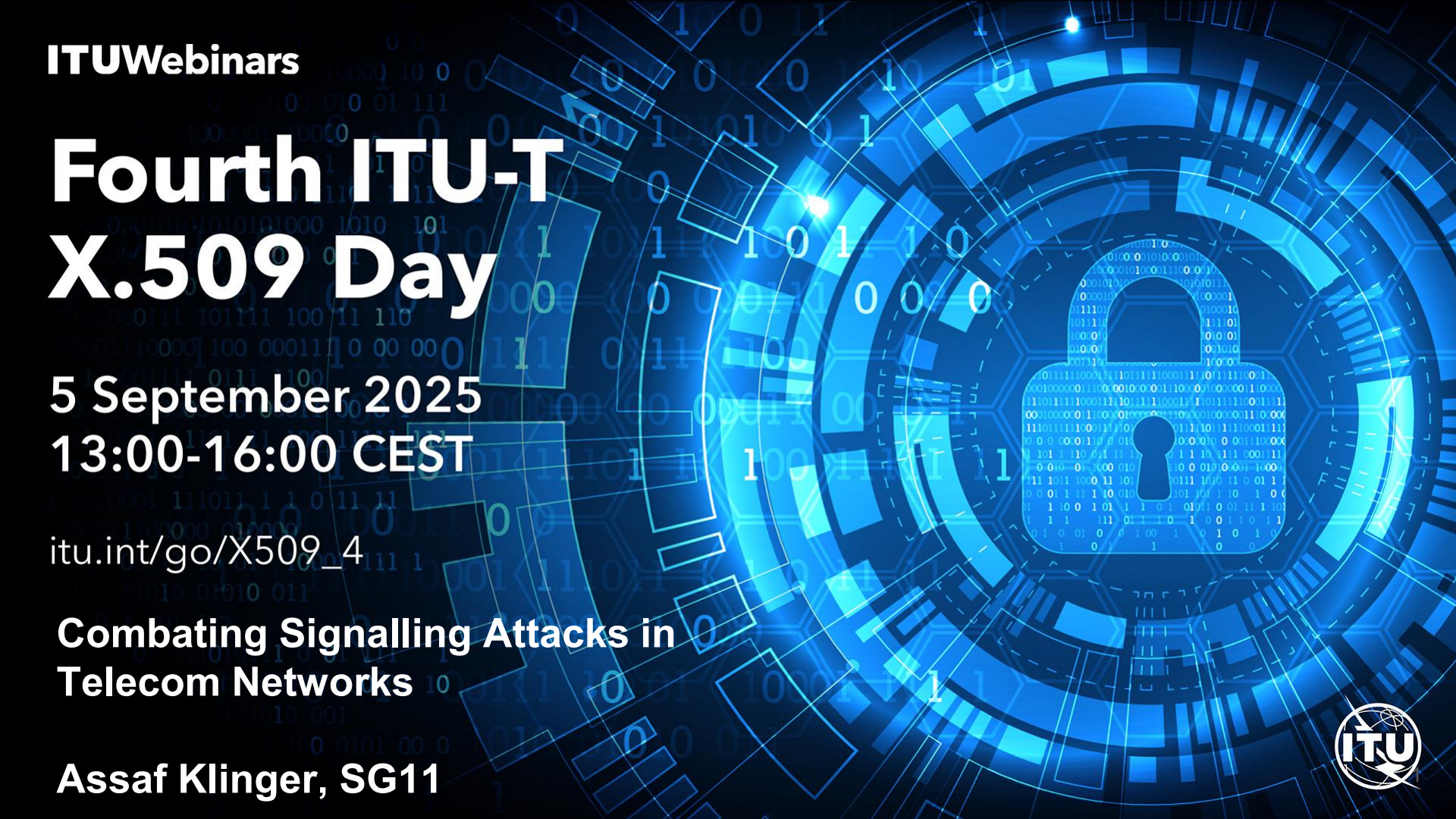
Fourth ITU-T X.509 Day

5 September 2025
13:00-16:00 CEST

itu.int/go/X509_4

Combating Signalling Attacks in Telecom Networks

Assaf Klinger, SG11



A little about myself

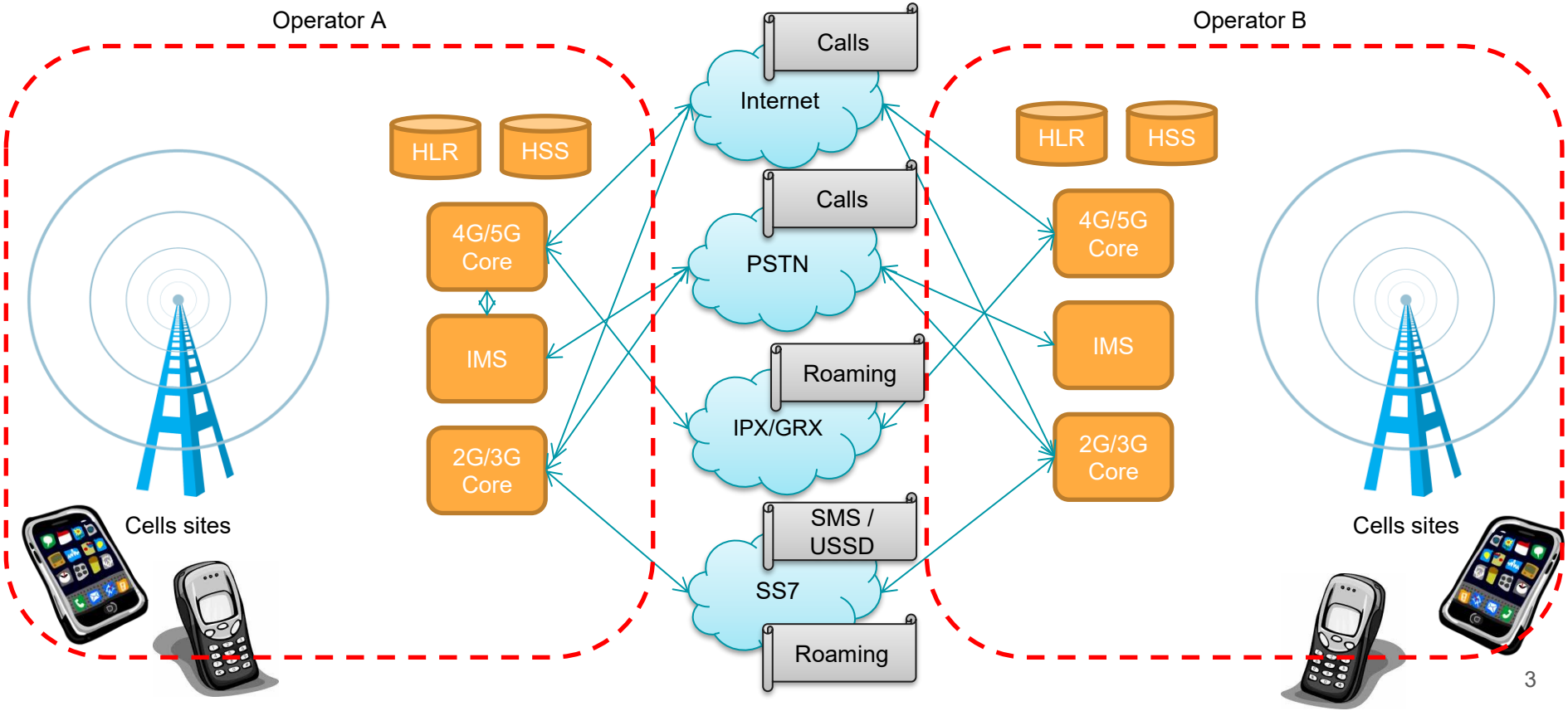
- Husband, father (+2), geek 8-)
- Security researcher for the last 18 years
  - Specialize in telecom, IoT & blockchain
  - Editor of ITU-T Study Group 11 recommendations
  - Member of FIGI SIT WG & DFGI SA WG
- Handles:

Assaf.klinger@gmail.com

@AssafKlinger

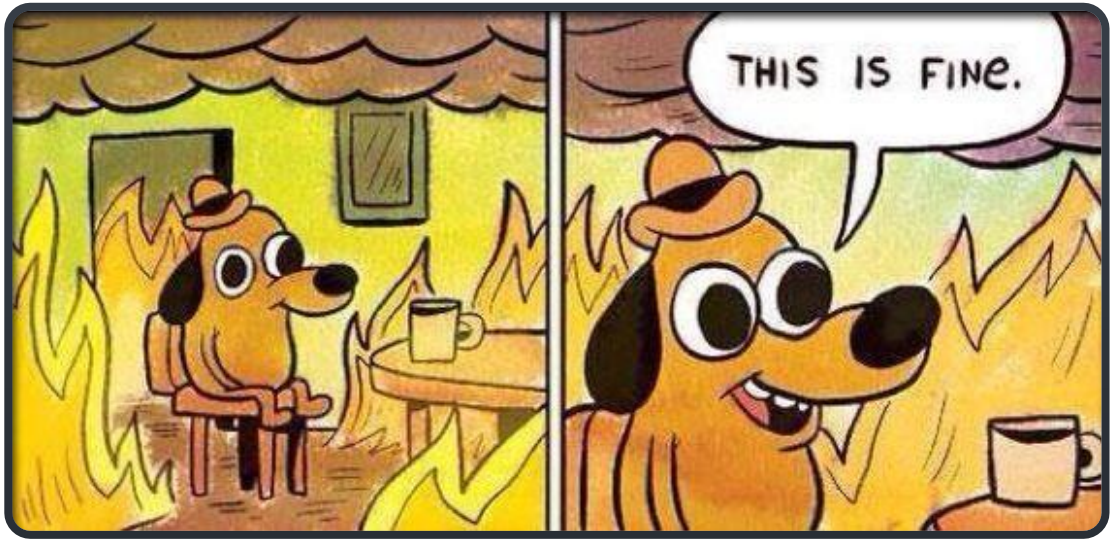
https://www.linkedin.com/in/assaf-klinger-8a0b7159/

Telco’s core network & telecom services



Telecom signalling networks: vulnerability by design

- Flat network (switched, not routed, no NATs)
- Static address allocation
- All network elements are trusted without question
- No encryption
- No authentication required to join the network



Major attacks on telecom networks in the wild

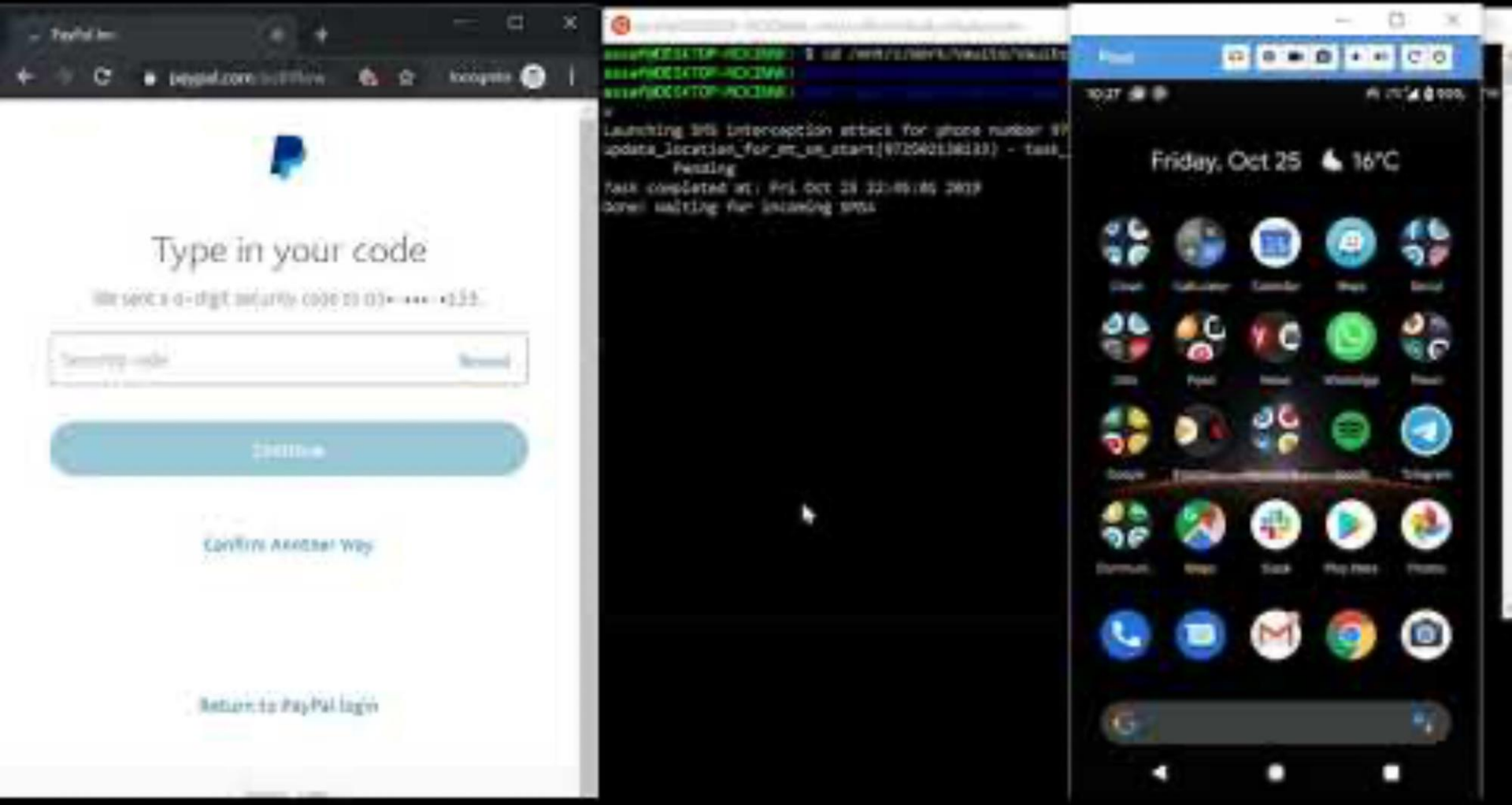
Caller ID spoofing

2FA account takeover

Geo Location

2FA SMS interception via SS7 attack

Example

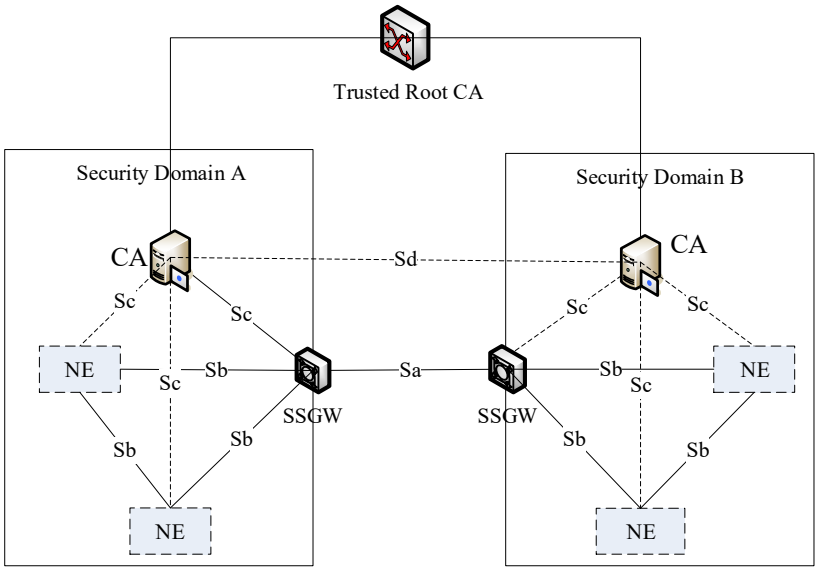

Type in your code
Confirm Another Way
Return to PayPal login
Launching SMS intercepction attack for phone number
Friday, Oct 25
16°C

The solution to the problem was here all along

- SG11 is building a signaling security framework to add an authenticity and integrity layers to signaling transactions to enable trustable communications
- Some example of applications:
  - Calling Line Identification (CLI) authentication
  - Secure 2FA
  - Prevent mobile banking fraud
  - And more…
- The framework consists of several recommendations

Published recommendations

- ITU-T Q.3057 and ITU-T Q.3062
  - Adds a digital signature to SS7 signaling to authenticate the sender (using X.509 certificates)
  - Prevents hackers from impersonating legitimate network functions on the SS7 network
  - Enables operators to manage trust of other operators
  - Using the internet as a reference trust model
- ITU-T Q.3063
  - Uses *Q.3057* and *Q.3062* as infrastructure for CLI authentication
  - Uses authentication tokens to prevent CLI spoofing



But what about the trust model?

Trust model

- We will need to build a hierarchy of trust, country/regional first, then global. where each local regulator will have to determine how to implement the certification depending on their local forms of identification and rules
- **Technically the digital certificates must be interoperable across domains** (SIP, SS7 and others).
- This trust chain and certification standard must account for the fact that numbering is no longer geographical, and different authorities can govern the same numbering range
- **The trust anchor needs to be a globally trusted SDO**, preferably one already in charge of numbering and this anchor must interoperate with existing repositories (such as the ones in the US and Canada)

vetting/certification process

- **We will need to formulate a way to standardize these local/regional certification processes** in order to keep the bad actors out. This standardization process should involve as many counties as possible in order to improve its applicability on the global scale
- The certification process implemented in the US and Canada for STIR/SHAKEN is a good use case to learn from in order to standardize it on the global scale
- These certification process standardization must be connected to a largely accepted digital identity management frameworks for the operator plane and for the individual plane

Work in progress - Q.TSCA

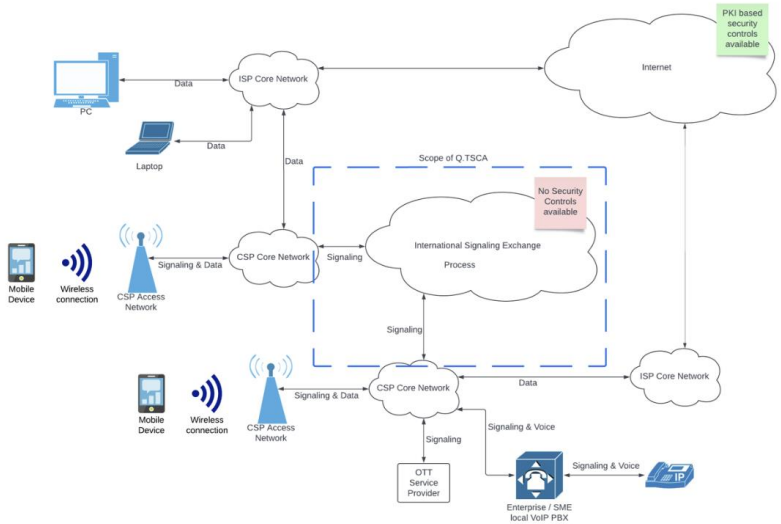


Figure 1 - current connectivity of CSPs to the international signalling exchange networks

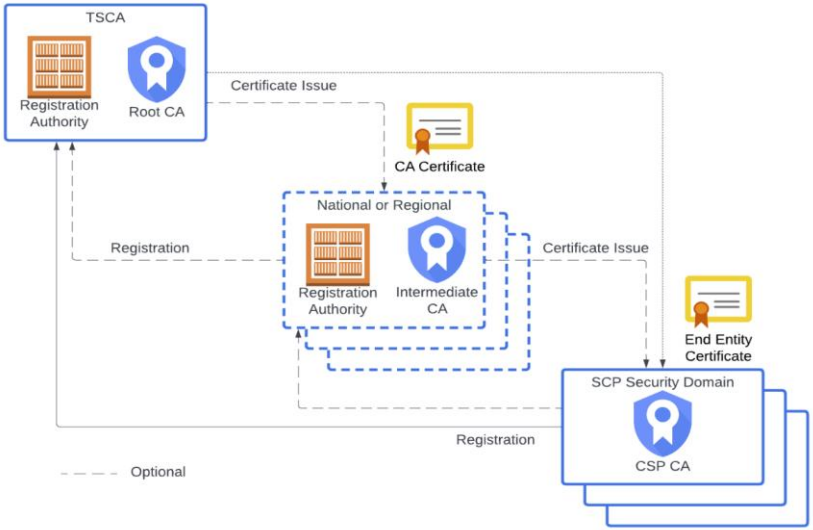


Figure 2 - general representation for the TSCA trust chain.

Create a security posture baseline - Q.DMSA

- Telecom signaling networks are critical to the operation of mobile networks
- they are also susceptible to a range of sophisticated attacks.
  - Simple, Single Request Attacks
  - Single Protocol, Multi-Request Attacks
  - Multi-Protocol Attacks
  - Cross-Generational Signaling Attacks

Thank you

Assaf.klinger@gmail.com

@AssafKlinger

https://www.linkedin.com/in/assaf-klinger-8a0b7159/