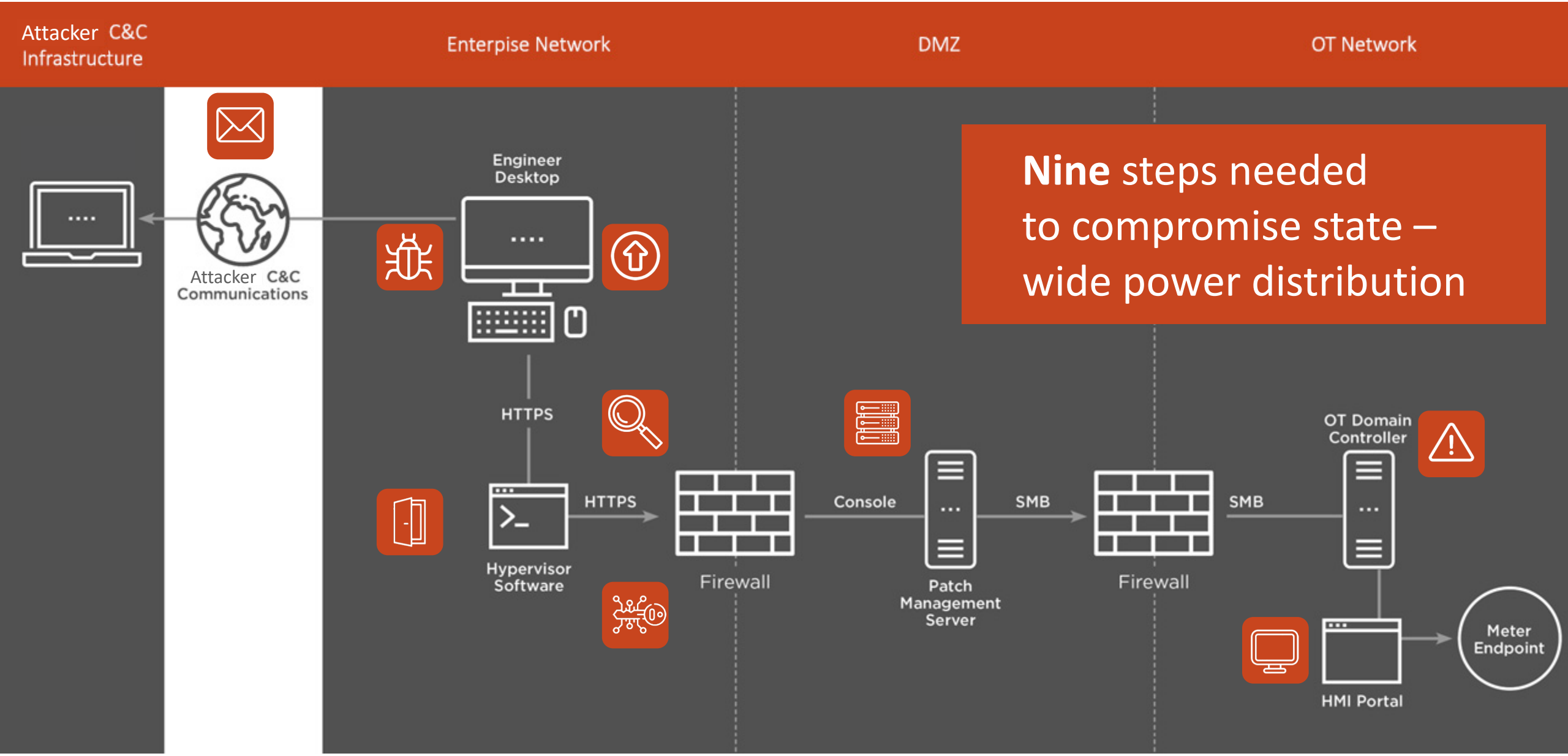
Protecting **Advanced Metering Infrastructure**

Krzysztof Swaczynski

Ninja Warrior - competitor

Offensive operation targeted at North American utility led to blackout via smart meters misuse


Attacker C&C Infrastructure
Enterprise Network
DMZ
OT Network
Nine steps needed to compromise state – wide power distribution
Attacker C&C Communications
Engineer Desktop
HTTPS
HTTPS
Hypervisor Software
Firewall
Console
Patch Management Server
SMB
Firewall
SMB
OT Domain Controller
HMI Portal
Meter Endpoint

Electricity Directive (EU) 2019/944 of the European Parliament and of the Council

„… Member States shall ensure the ***deployment of smart metering systems in their territories*** *…*

…Where the deployment of smart metering systems is assessed positively, at least 80 % of final customers shall be equipped with smart meters…

…*either within* ***seven years of the date of the positive assessment or by 2024*** *…”*

Stromversorgungsverordnung (StromVV) vom 14. März 2008 (Stand am 1. Oktober 2022)

*„… **Bis zehn Jahre** nach Inkrafttreten der Änderung **vom 1. November 2017** müssen **80 Prozent** aller Messeinrichtungen in einem Netzgebiet den Anforderungen **nach den Artikeln 8a und 8b entsprechen**. **Die restlichen 20 Prozent** dürfen bis zum Ende ihrer Funktionstauglichkeit im Einsatz stehen …"*

Four typical AMI security pitfalls

1. Questionable security of smart meter devices

2. Replicating secrets used to secure meters

3. Insufficient network segmentation and monitoring

4. Late or limited security dept. involvement in project

Swissness of securing smart metering components

Legislation enforcing **security certified meters** to be sold only

Industry led (swissmig) **security testing** standard methodology

Accredited testing labs with advanced capabilities

Federal agency with security **certification authority**

3 zero-days reported in popular
DLMS/COSEM stack implementation

Possibility of local and remote attack without authorisation

DOS attack

read the content
of the meter's memory

code execution
(to seize control over meter)

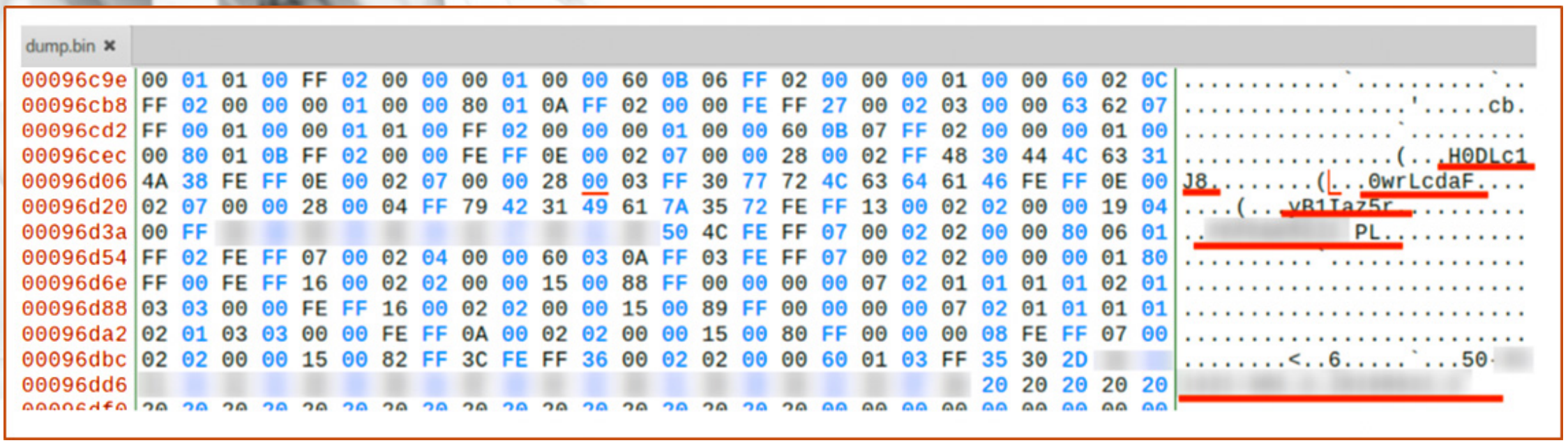
Solution: Make sure that tests executed address your risk model and understand scope and coverage of security tests by vendor

Sensitive data in non-volatile memories

APN name and access data

DLMS association keys

Association cryptographic keys



Solution: Make sure that tests executed address your risk model and understand scope and coverage of security tests by vendor

Storage of sensitive data in accordance with DLMS standards poses quite complex challenge – yet is critical to ensuring secure AMI operation

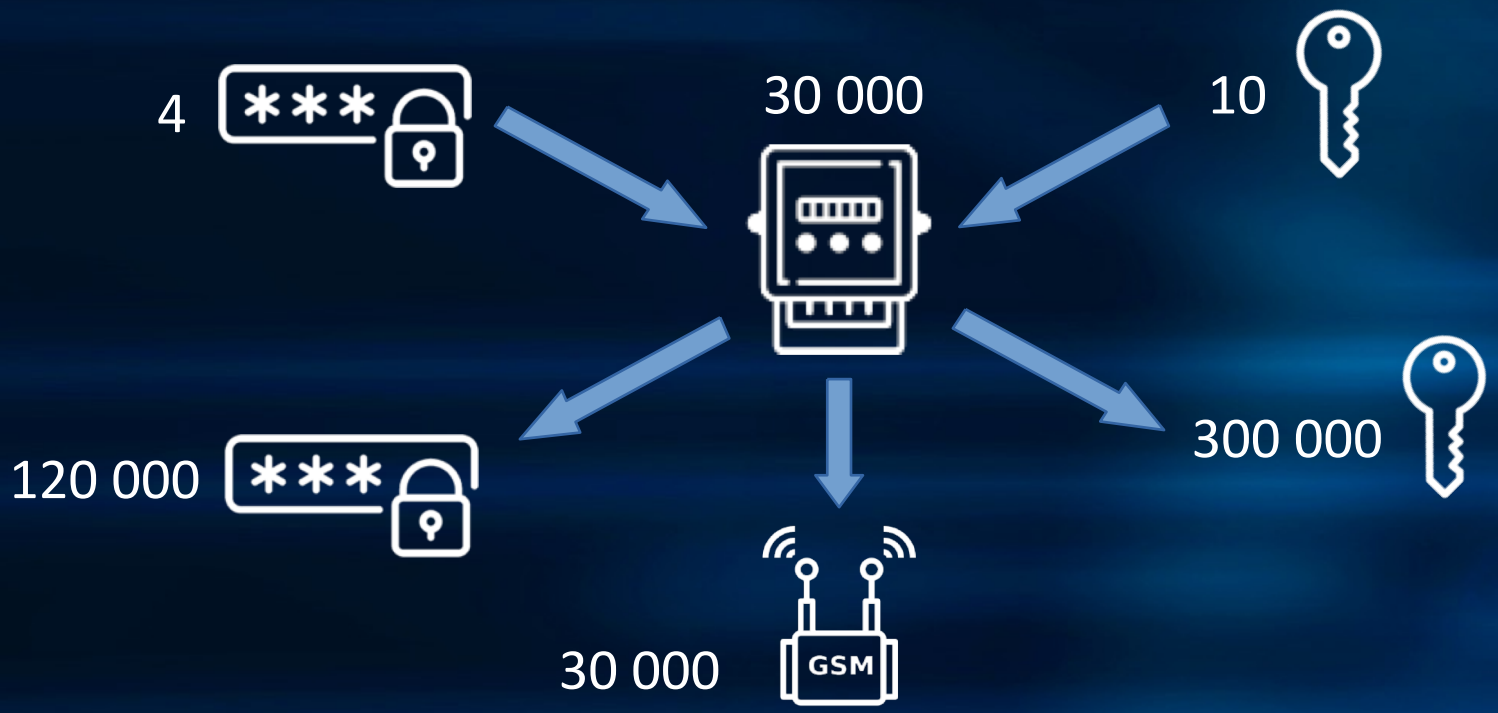
Association passwords
DLMS, LLS (Low Level Security)

- management
- reading
- firmware update
- HAN

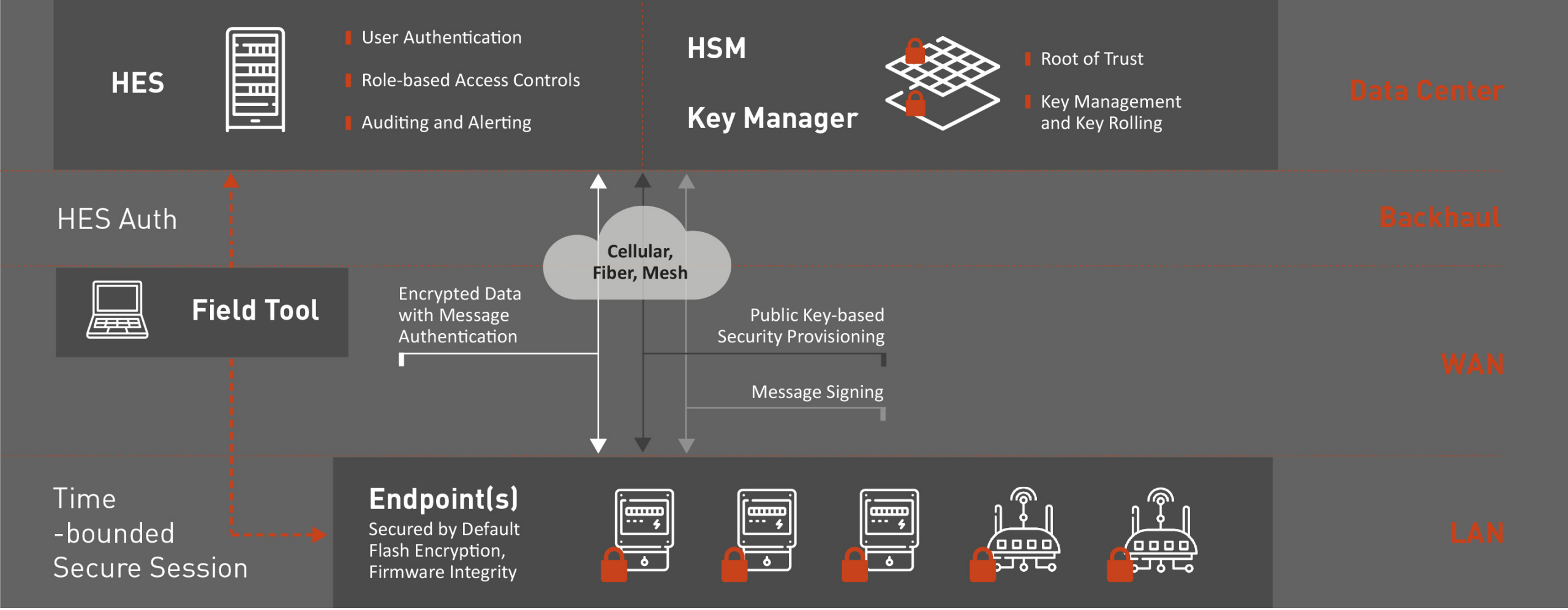
Encryption keys

- master
- authentication key
- global unicast encryption key
- global broadcast encryption key

Storage of sensitive data in accordance with DLMS standards poses quite complex challenge – yet is critical to ensuring secure AMI operation

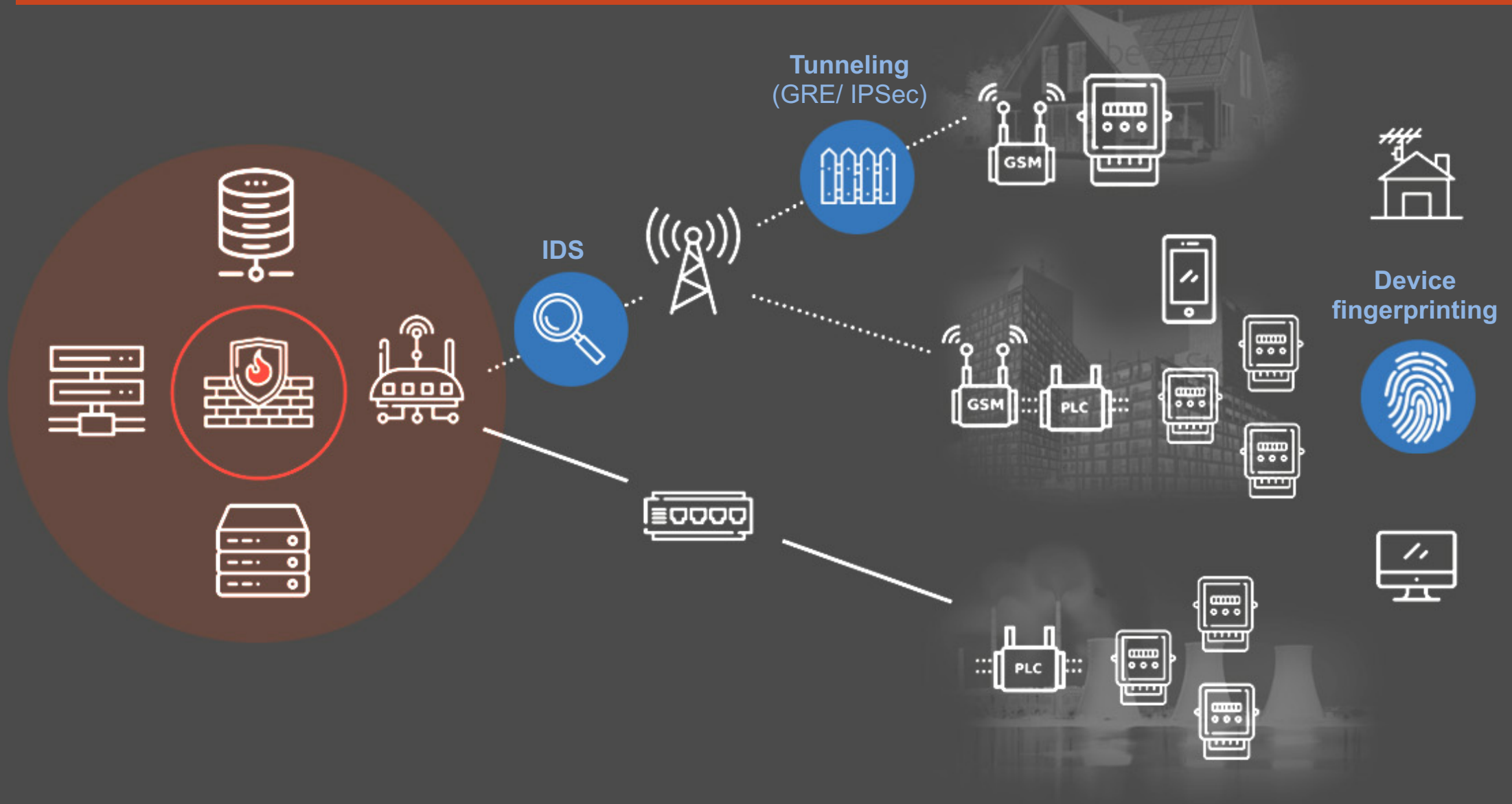


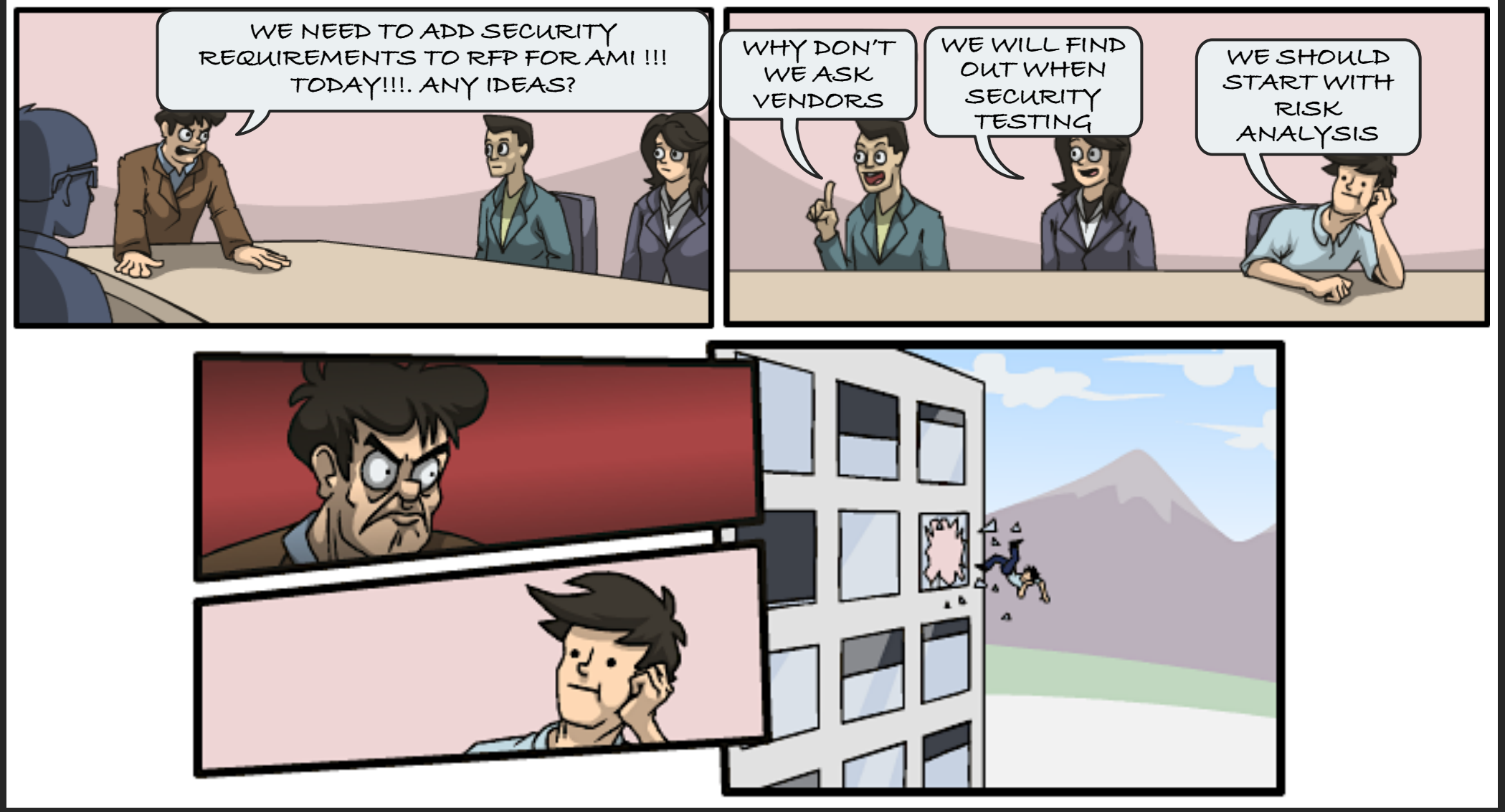
Sizable city
– over 450 000 passwords and keys



Solution: Involving PKI architect and/ or selecting implementation partner with proven AMI security architecture capability

Network architecture designed to limit attack options





Solution: Security architecture as a integral part of AMI project start from the get go and included in RFP/project scope

QUESTIONS?

SEQRED

Krzysztof Swaczynski

krzysztof.swaczynski@seqred.pl

https://www.linkedin.com/in/kswaczynski/