Considerations (and solutions) for a lightweight, usable, and quantum-secure IoT

Oscar Garcia-Morchon
and Ronald Rietman, Ludo Tolhuizen, Sauvik Bhattacharya, Jose Luis Torre-Arce

Philips Research

innovation + you

PHILIPS

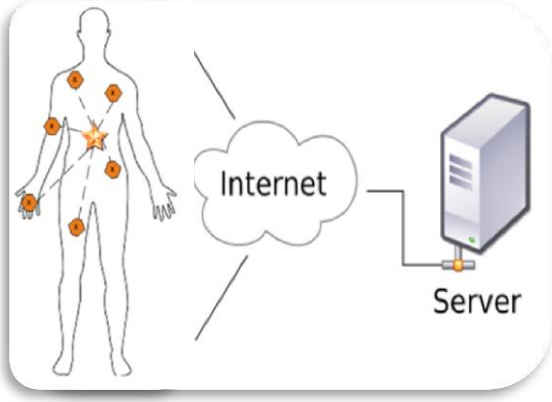
Agenda

- Use cases and requirements
- Challenges
- Architectural options and HIMMO
- HIMMO directions
- Conclusions

Use cases and requirements

Internet of Things

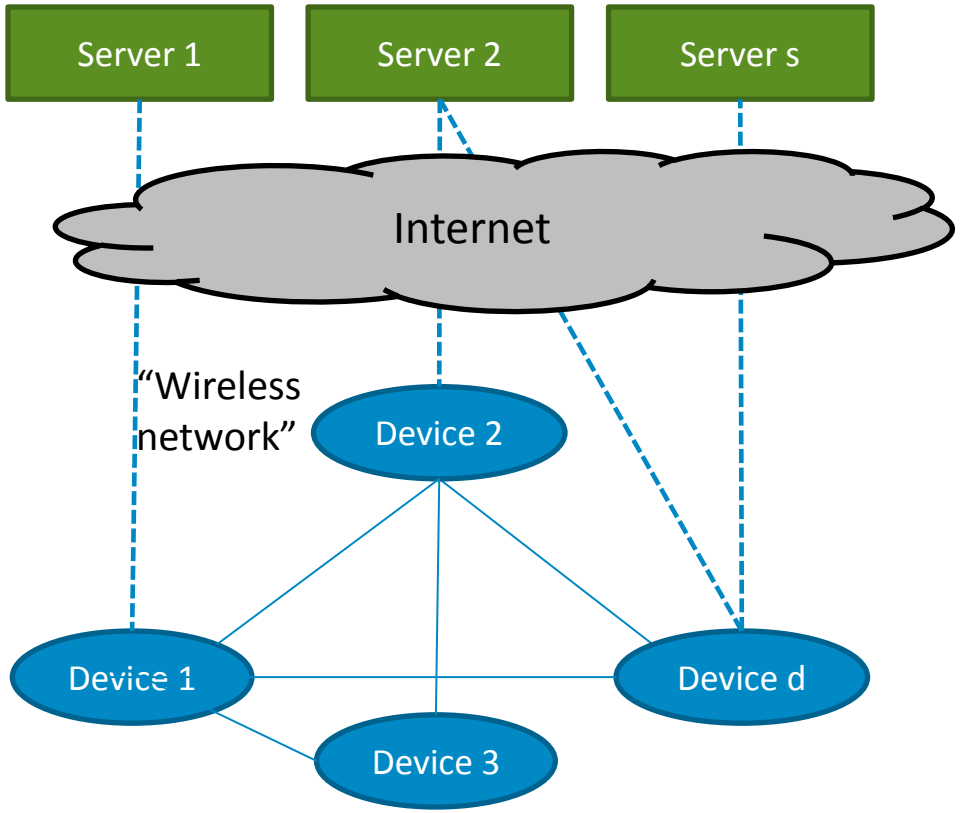
Some use cases and features



- Constrained links
- Device to device
- Large network
- Low power
- Long-term

- Robust architecture
- Small packets
- Private data
- Low power
- Long term

Abstracting



- Low energy (battery or harvesting)
- Small (100s bytes) packet
- Low (100s Kbps) data rate
- Long term (>10 years)
- Relatively slow CPU (10s MHz)
- Limited RAM (<10 KB)
- Limited memory (256 – 1024 KB)

Why Security in IoT?

Your privacy & safety

Company image and IPR

National security

Economy

Challenges

Why is Security Challenging in IoT?

Main reasons

- Business case →budget constrains → tight resources
- Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

- DoS resistance
- Protocol translation
- End-to-end security
- Bootstrapping security
- Network access control (IP networks)
- Group membership and security
- IP network dynamics
- Long term security
- Software upgrade
- Intrusion detection
- Penetration testing
- Fine grained access control
- Re-selling devices
- System heritage
- Crypto agility (limited resources)
- Quantum-resistance

Why is Security Challenging in IoT?

Main reasons

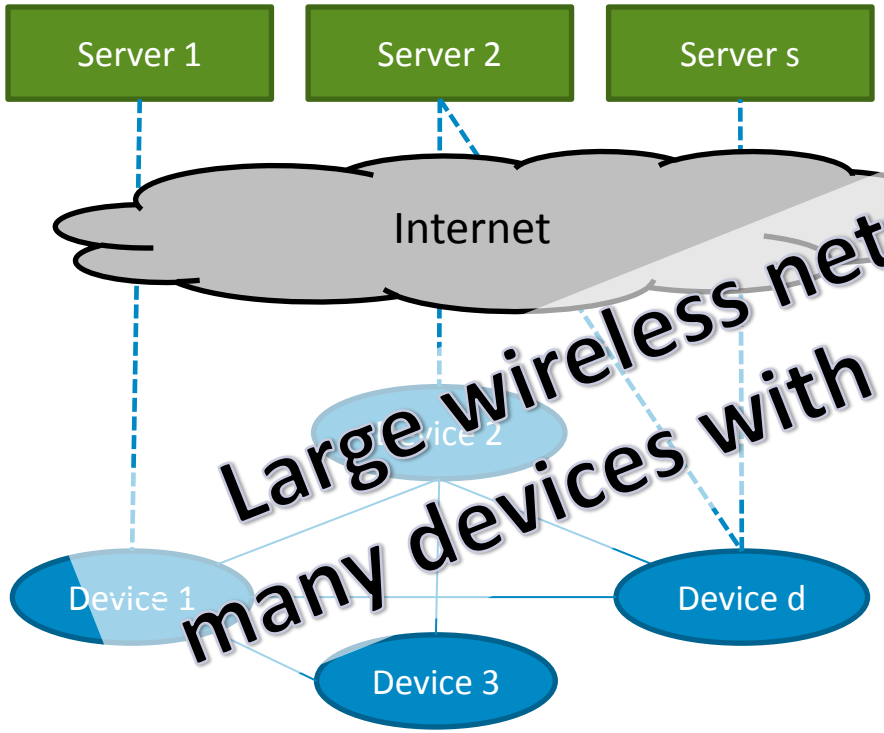
- Business case →budget constrains → tight resources
- Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

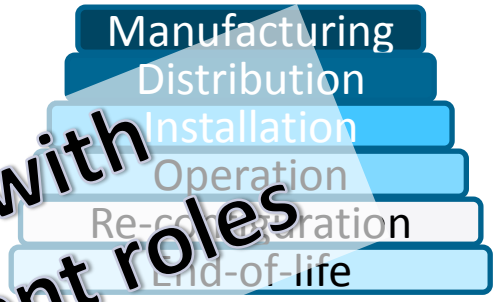
- *DoS resistance*
- Protocol translation
- *End-to-end security*
- *Bootstrapping security*
- *Network access control* (IP networks)
- *Group membership and security*
- IP network dynamics
- Long term security
- *Software upgrade*
- Intrusion detection
- Penetration testing
- *Fine grained access control*
- *Re-selling devices*
- System heritage
- Crypto agility (limited resources)
- Quantum-resistance

Challenge: efficient and scalable management of keys/credentials of devices

Why this challenge?



Large wireless network with many devices with different roles



Device lifecycle

Simple operation

Challenge: efficient and scalable management of keys/credentials of devices

Why is Security Challenging in IoT?

Main reasons

- Business case →budget constrains → tight resources
- Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

- DoS resistance
- Protocol translation
- End-to-end security
- Bootstrapping security
- Network access control (IP networks)
- Group membership and security
- IP network dynamics
- **Long term security**
- Software upgrade
- Intrusion detection
- Penetration testing
- Fine grained access control
- Re-selling devices
- System heritage
- Crypto agility (limited resources)
- **Quantum-resistance**

Why is Security Challenging in IoT?

Main reasons

- Business case →budget constrains → tight resources
- Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

- DoS resistance
- Protocol translation
- End-to-end security
- Bootstrapping security
- Network access control (IP networks)
- Group membership and security
- IP network dynamics
- **Long term security**
- Software upgrade
- Intrusion detection
- Penetration testing
- Fine grained access control
- Re-selling devices
- System heritage
- Crypto agility (limited resources)
- **Quantum-resistance**

Challenge: Long term efficient and scalable management of keys/credentials of devices

Why is Security Challenging in IoT?

Main reasons

- Business case →budget constrains → tight resources
- Application lifecycle → operational constrains

Many technical challenges (from www.ietf.org/id/draft-irtf-t2trg-iot-seccons-00.txt)

- *DoS resistance*
- Protocol translation
- *End-to-end security*
- *Bootstrapping security*
- *Network access control* (IP networks)
- *Group membership and security*
- IP network dynamics
- **Long term security**
- *Software upgrade*
- Intrusion detection
- Penetration testing
- *Fine grained access control*
- *Re-selling devices*
- System heritage
- ***Crypto agility*** *(limited resources)*
- **Quantum-resistance**

Challenge: Long term efficient and scalable *management of keys/credentials* of devices

Why is long-term security a challenge?

The construction of a large scale fault tolerant quantum computer would mean:

Symmetric primitive	Security level
AES128	64
AES256	128
ECC	0
RSA	0

Challenge: Long term efficient and scalable *management of keys/credentials* of devices

Why is long-term security a challenge?

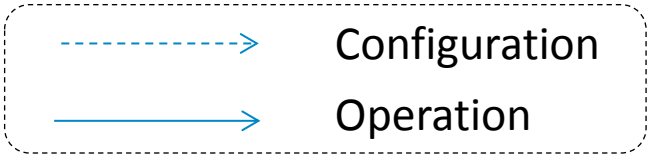
There are some proposed public-key primitives, but there are performance challenges:

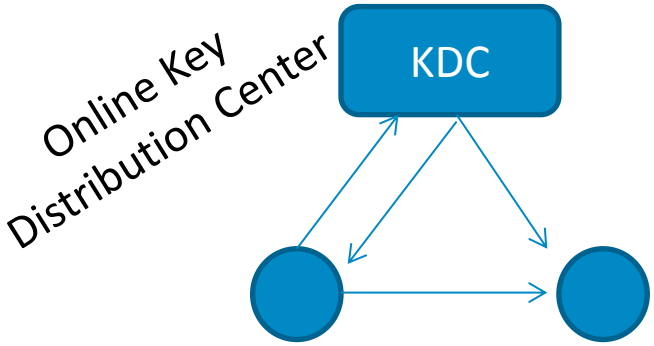
Primitive	Communication overhead	Challenges
XMSS	$\sim 39000\ bits\ (w = 4)$	Scheme with short signatures?
New Hope	$\sim 3800\ bits$	Efficient key exchange?
Frodo	$\sim 22500\ bits$	
AES128		How to upgrade deployed hardware?

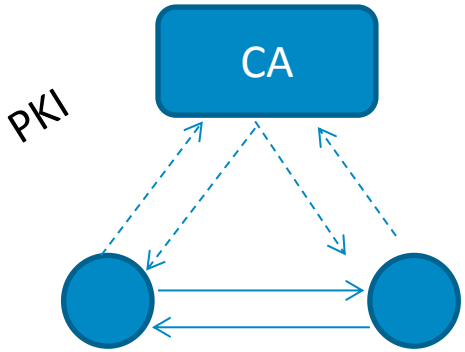
Challenge: Long term <u>efficient</u> and scalable <u>*management of keys/credentials*</u> of devices

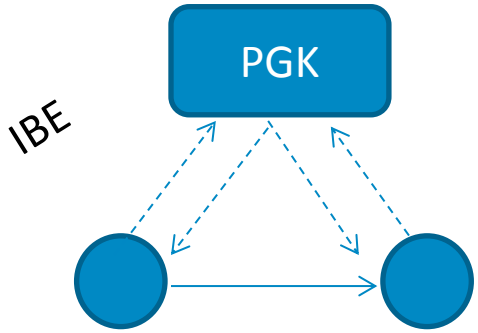
Architecture options

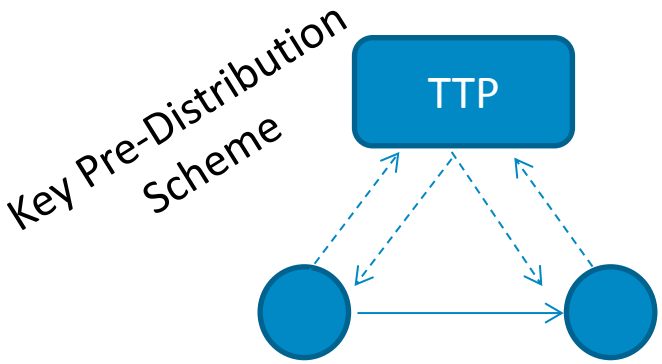
Architectural Options



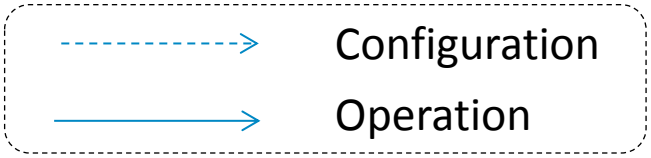


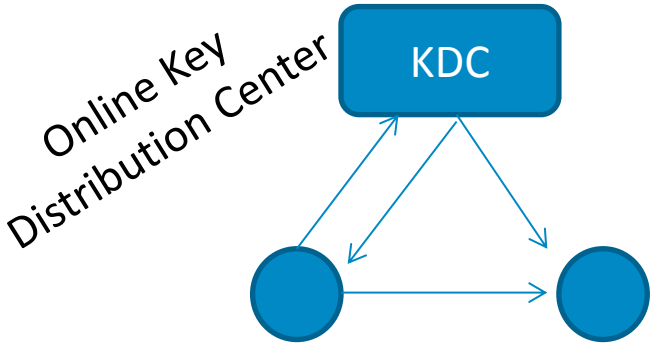


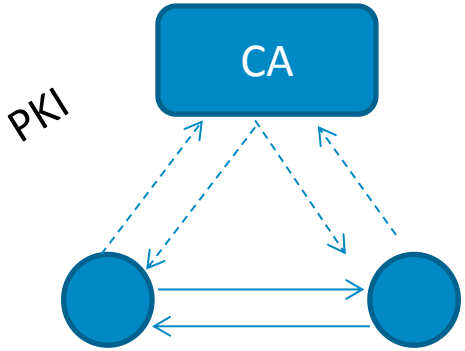


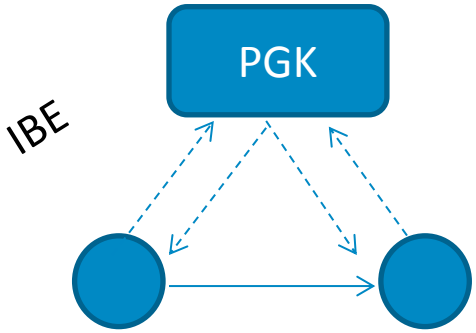


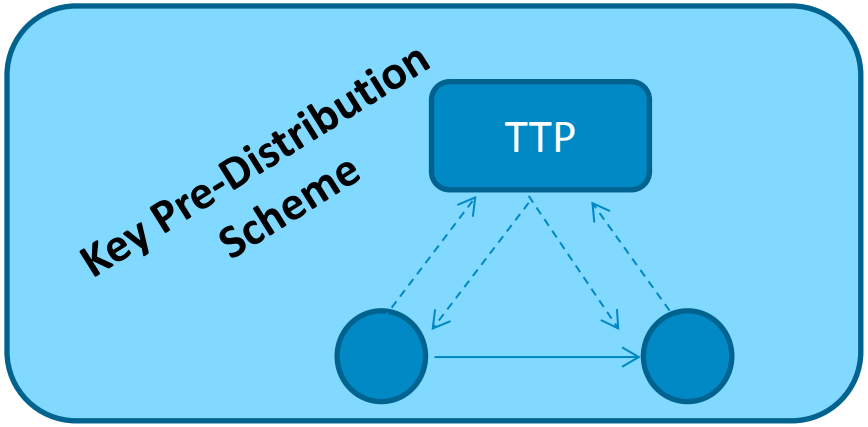
Architectural Options





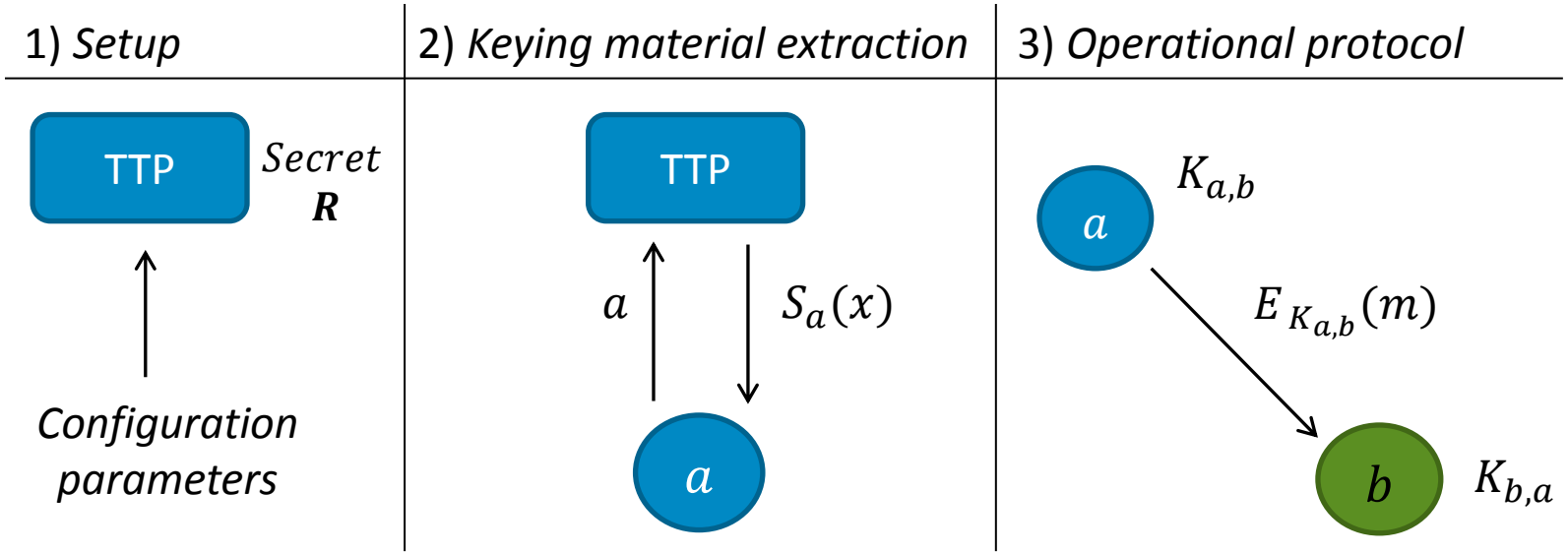






HIMMO

Efficient Collusion- and Quantum-Resistant Key Pre-Distribution Scheme



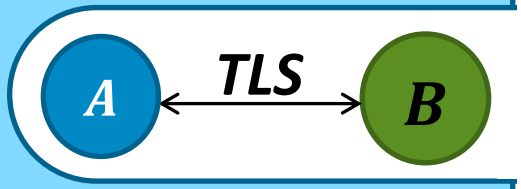
Identity-based key exchange with implicit authentication

HIMMO

www.himmo-scheme.com

- **Efficient collusion- and quantum- resistant**

- Easy protocol integration (TLS, MAC-layer level protocols, etc)
- Features
  - Key exchange
  - Identity-based
  - Multiple TTP support
  - Credential certification and verification
  - One-way key exchange and authentication in 30 Bytes



- Advantages
  - Very low overhead
  - Blacklisting feasible
  - Resilient TTP infrastructure
  - Out-of-the-box secure by factory configuration
  - Architectures able to support both forward secrecy and key escrow

HIMMO directions

HIMMO directions

- Running challenge with HIMMO design according to *https://eprint.iacr.org/2016/152.pdf*
- We have kept analyzing HIMMO and also ways of optimizing design

Current HIMMO design (online challenges)

Setup

N: odd integer of bit length $3b$

m numbers $q_i = N - \beta_i 2^b$ for β_i a secret b bits number

$\boldsymbol{R_i}$ be a random symmetric $t\ x\ t$ matrix over Z_{q_i}, for $0 \leq i \leq\ m-1$

Keying material extraction

TTP

$$\mathbf{s_a} = \left\langle \sum_{i=0}^{m-1} \langle \mathbf{aR_i} \rangle_{q_i} \right\rangle_N$$

$$\boldsymbol{a}, \boldsymbol{b} \in [0, 2^b - 1]^t$$

$\mathbf{s_b}$

Operation

Alice (a)

$$s_{a,b} = \left\langle \langle \boldsymbol{s_a} \boldsymbol{b}^T \rangle_N \right\rangle_{2^b}$$

$$k_{a,b} = \left\lfloor \frac{s_{a,b}}{2^u} \right\rfloor$$

$$h = \langle s_{a,b} \rangle_{2^u}$$

$$E_{K_{a,b}}(m),\ h \longrightarrow$$

Bob (b)

$$s_{b,a} = \left\langle \langle \boldsymbol{s_b} \boldsymbol{a}^T \rangle_N \right\rangle_{2^b}$$

$$s_{a,b} = f(s_{b,a}, h)$$

$$k_{a,b} = \left\lfloor \frac{s_{a,b}}{2^u} \right\rfloor$$

As in https://eprint.iacr.org/2016/152.pdf but with different notation

Simplifying the HIMMO design

Setup

N be an integer of bit length $3b$

$\boldsymbol{R}$ be a random symmetric $t\ x\ t$ matrix over Z_N

Keying material extraction

TTP

$\mathbf{s_a} = \langle \boldsymbol{aR} + \boldsymbol{\epsilon_a} \rangle_N$

$\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{\epsilon_a}, \boldsymbol{\epsilon_b} \in [0, 2^b - 1]^t$

$\mathbf{s_b}$

Operation

Alice (a)

$s_{a,b} = \langle \boldsymbol{s_a b}^T \rangle_N$

$k_{a,b} = \left\lfloor \frac{s_{a,b}}{2^{2b+u}} \right\rfloor$

$h = \left\langle \frac{s_{a,b}}{2^{2b}} \right\rangle_{2^u}$

$E_{K_{a,b}}(m), h$

Bob (b)

$s_{b,a} = \langle \boldsymbol{s_b a}^T \rangle_N$

$s_{a,b} = f(s_{b,a}, h)$

$k_{a,b} = \left\lfloor \frac{s_{a,b}}{2^{2b+u}} \right\rfloor$

Note: Before $\boldsymbol{\epsilon_a}$ determined by β_i, $\boldsymbol{R_i}$ and **a**. Now random

About the simplified design

- Operationally equivalent to existing HIMMO design (eprint 2016/152)
- For work done so far, same attacks and security parameters seem to apply.
- It shares some similarities with LWE, but it is not LWE.
  - Key difference: identity vector is not evenly distributed in Z_N since it is short.
  - The fact that the identities are shorter implies that a larger value of t is required to deal with existing attacks
- Further simplifications are feasible.

Parameters and performance

- Security notion
  - **Information-theoretically secure:** attacker needs $c > 3t/2$ nodes to attack a system. In a small network with d devices, we can use small $t = 2d/3$
  - **Computational security:** for b parameter (e.g., 16) and a relatively large t (e.g., 2000) a high quality (slow) lattice reduction algorithm is needed to obtain a lattice basis with a small enough root Hermit factor (e.g., < 1.005)
- Estimated performance

	Inf.-theor. Security	Computational security
Parameters (*t/b*)	$200/32$	$2000/16$
Network size	e.g., $d = 300$	Any
Communication overhead	$48\ B$	$96\ B$
Keying material size	$6.25\ KB$	$30 - 60\ KB$
Code / RAM size	$< 500\ B, \sim 40\ B$	
Security level	128 bits long key	Up to 256 bit long key

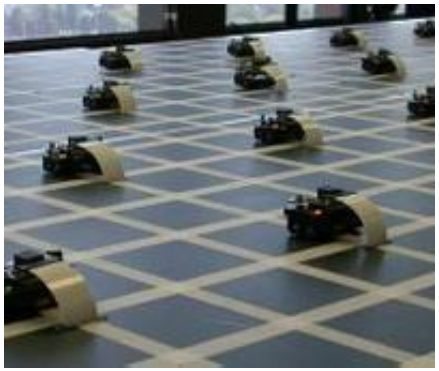
Conclusions

- The IoT covers a plethora of use cases with very diverse needs
- IoT has many security challenges ahead; many more in the advent of quantum computers: efficiency, transition, key/credential management
- The key challenge: efficient and scalable long-term management of keys/credentials of devices through their lifecycle
- HIMMO (www.himmo-scheme.com) is an efficient collusion- and quantum-resistant scheme overcoming this problem

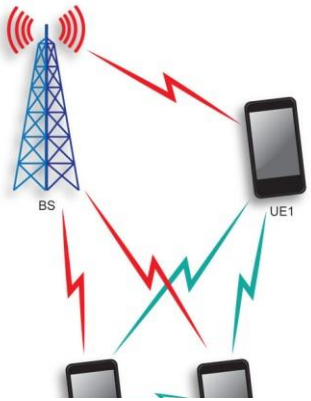
PHILIPS

Many Requirements

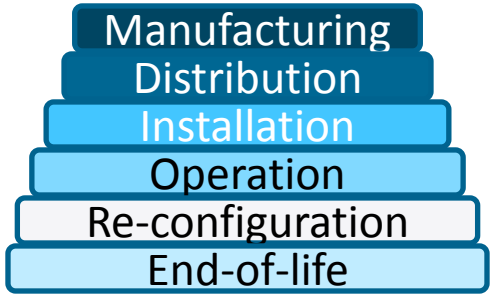
Energy efficiency



Small and real-time



Simple operation



Device lifecycle

Long term **security**

Attacks Paths and Security Analysis

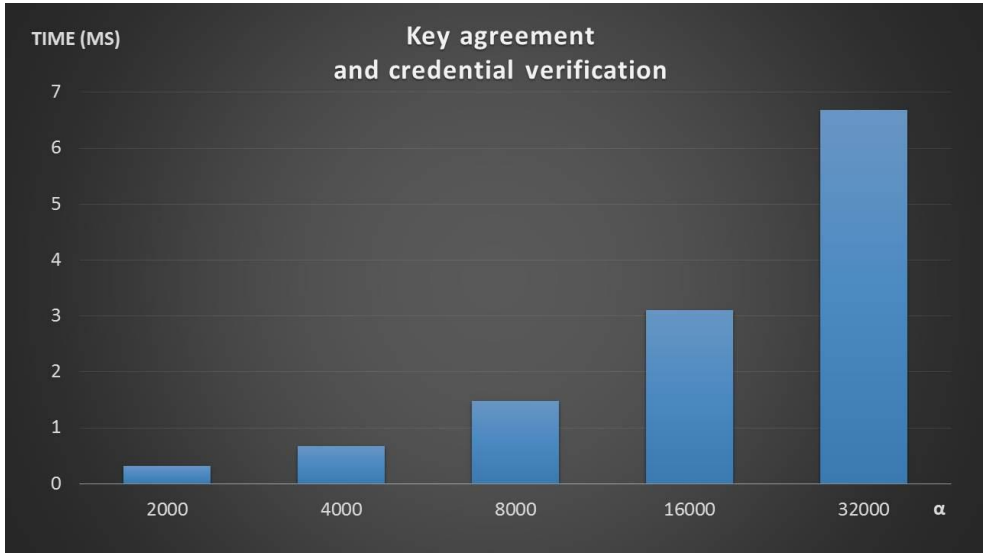
- Eve has any set of c compromised keying materials $\boldsymbol{s_{x_1}}, \dots, \boldsymbol{s_{x_c}}$. Eve's goal is to find the key shared between Alice and Bob, $k_{a,b}$.
- Attack paths:
  - Try to recover $k_{a,b}$ by attacking the TTP: recovers $\boldsymbol{R}$, $\boldsymbol{s_x}$, and any $k_{x,y}$.
  - Try to recover $k_{a,b}$ by attacking Alice's $\boldsymbol{s_a}$ (or Bob): recovers $\boldsymbol{s_a}$, and any $k_{a,y}$.
  - Try to recover $k_{a,b}$ only.
- Security analysis for the above attack paths is described here

  O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, M.S. Lee, D. Gomez-Perez, J. Gutierrez, B. Schoenmakers, "Attacks and parameter choices in HIMMO", ", IACR ePrint Archive, Report 2016-152

About the HIMMO Contest

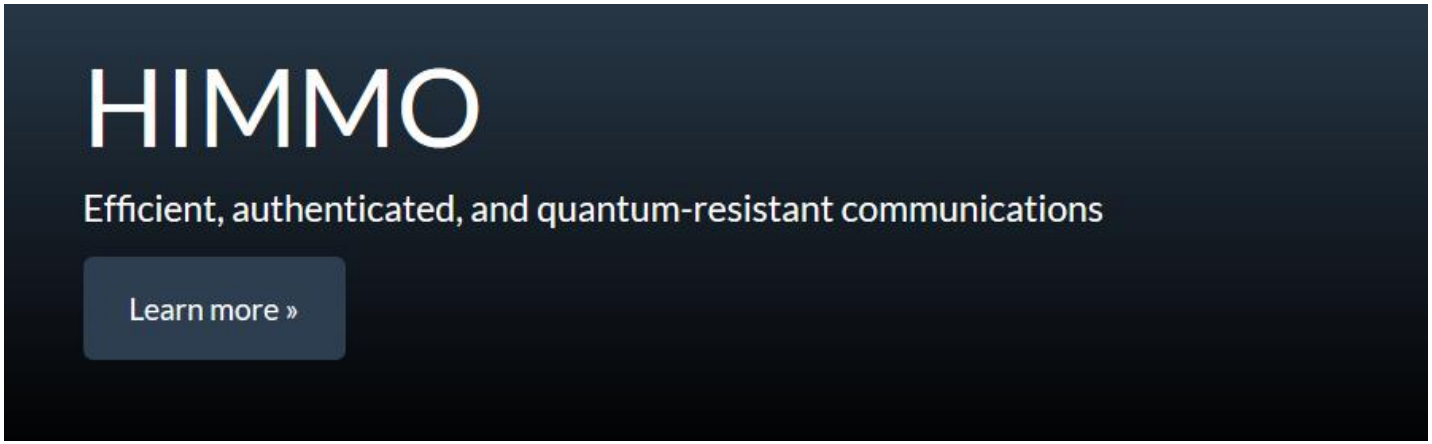
- No time limit, you can take as much time as you need
- Five challenges for $b = 32$
- 1000 Euros per solved challenge

Challenge	t
HIMMO1	2000
HIMMO2	4000
HIMMO3	8000
HIMMO4	16000
HIMMO5	32000



+ Information and Contest for Open Verification

www.himmo-scheme.com



Key Pre-Distribution Scheme

A key pre-distribution scheme involves a trusted third party TTP and nodes $N_1, \ldots, N_l$ and consists of the following three components.

- **Setup.** An algorithm run by TTP for generating secret root keying material R and public system parameter P, given a security parameter.
- **Extract.** An algorithm run by TTP for generating secret keying material s_x for a given node N_x, given root keying material R and system parameter P.
- **Key establishment.** A protocol run by node N_x and N_y for generating shared key $k_{x,y}$, given secret keying material s_x and s_y, and system parameter P.

Rationale

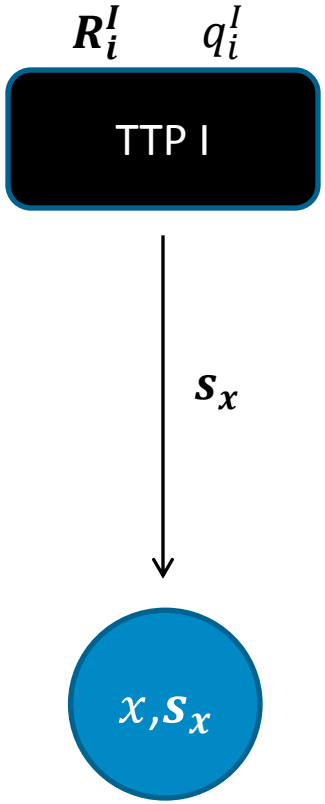
Features of KPS

- ✓ Efficient
- ✓ Any node can directly obtain a pairwise key with any other any node
- ✓ Based on identities so that it is possible to verify them
- ✓ Multiple TTP support so that a single TTP does not have access to all keys
- X KPS collusion resistance

Our goal with HIMMO was to achieve collusion resistance while keeping the rest of nice features

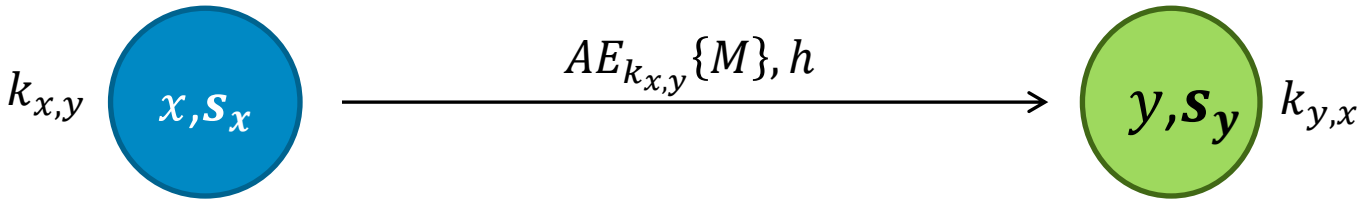
HIMMO in Practice

Extraction



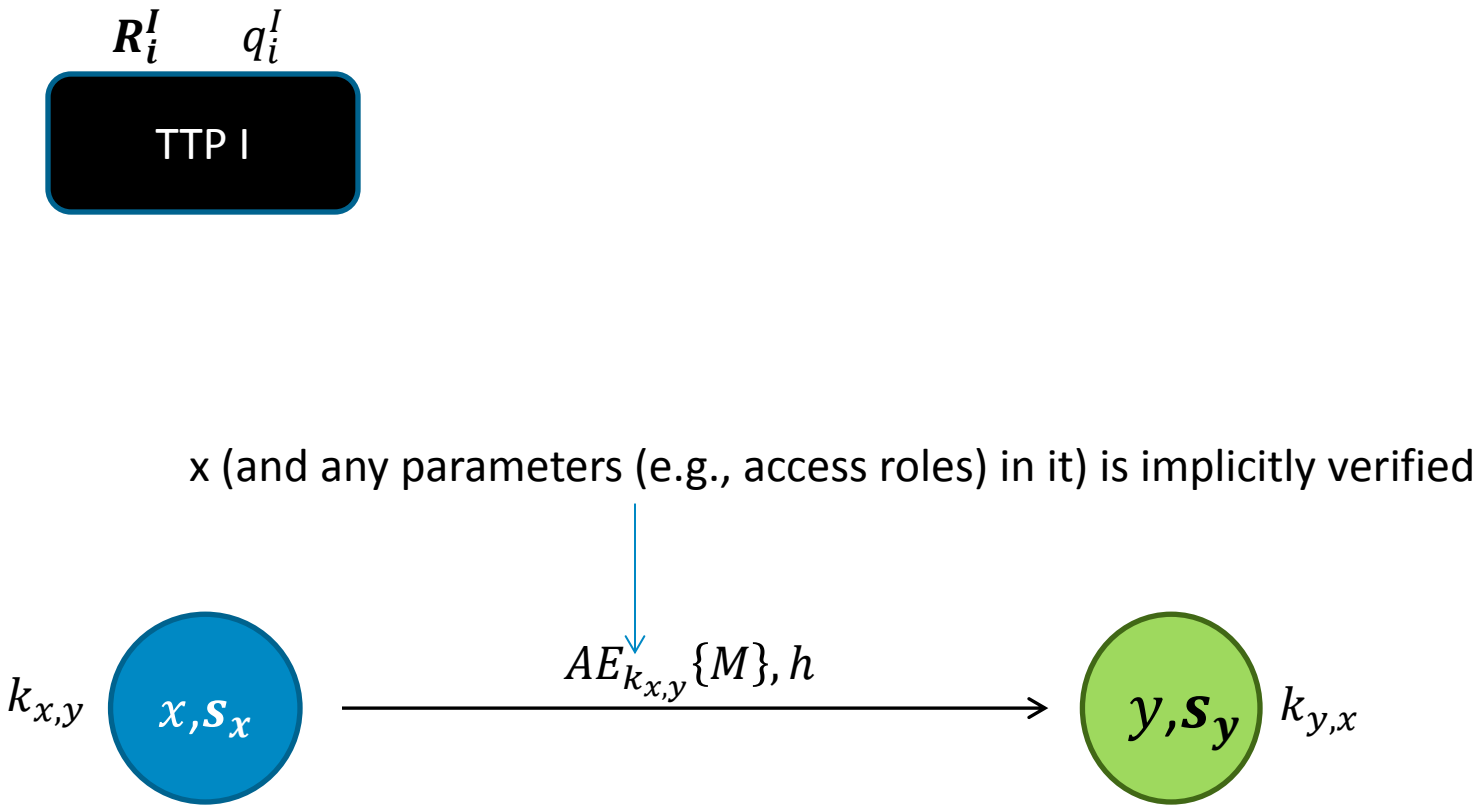
HIMMO in Practice

One-way key exchange and entity authentication



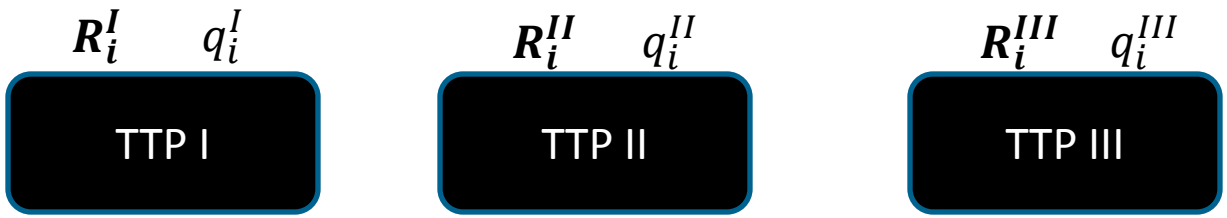
HIMMO in Practice

Implicit certification and verification of parameters

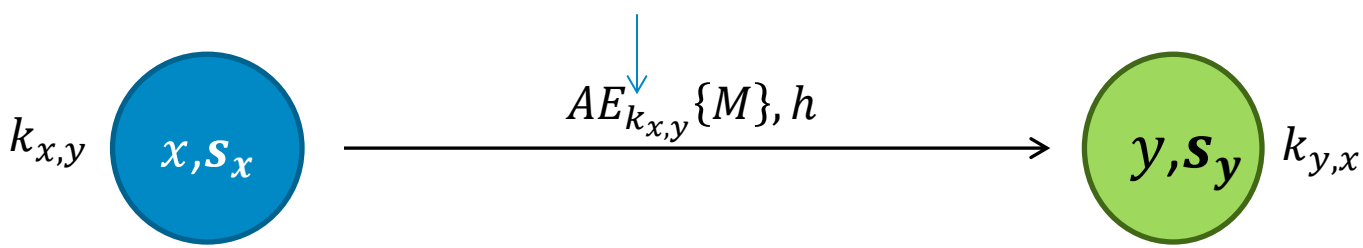


HIMMO in Practice

Multiple TTP support



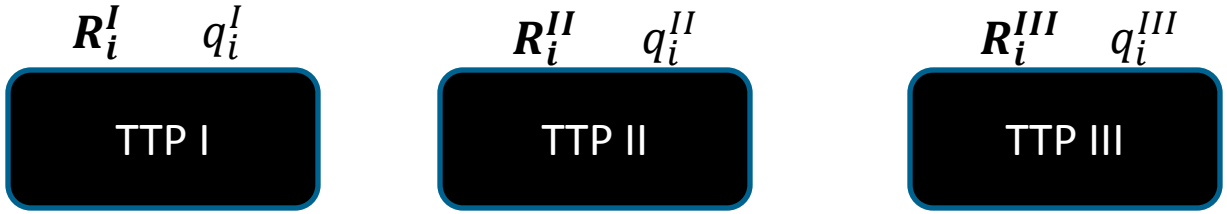
x (and any parameters (e.g., access roles) in it) is implicitly verified
Single TTP does not have access to communication



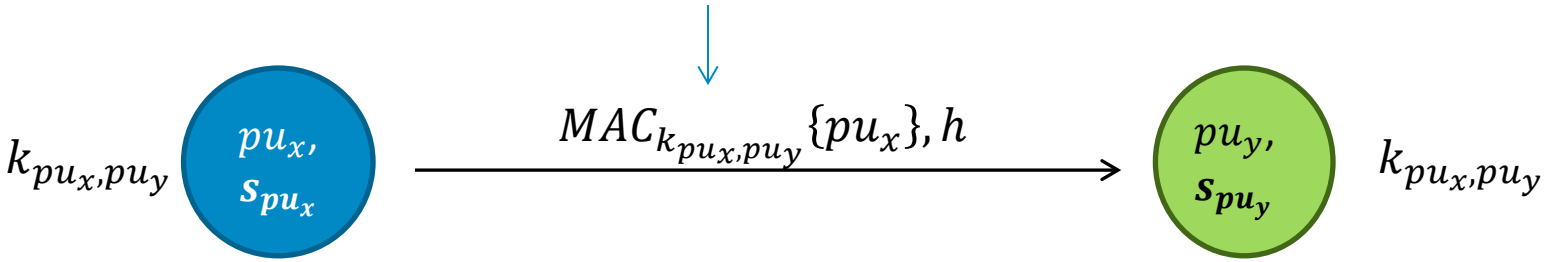
O. Garcia-Morchon, R. Rietman, S. Sharma, L. Tolhuizen, J.L., Torre-Arce. DTLS-HIMMO Efficiently Securing a Post-Quantum World with a Fully-Collusion Resistant KPS. In ESORICS 2015; also presented at NIST workshop on Cybersecurity in a Post-Quantum World, 2015.

HIMMO in Practice

HIMMO for certification of public-keys

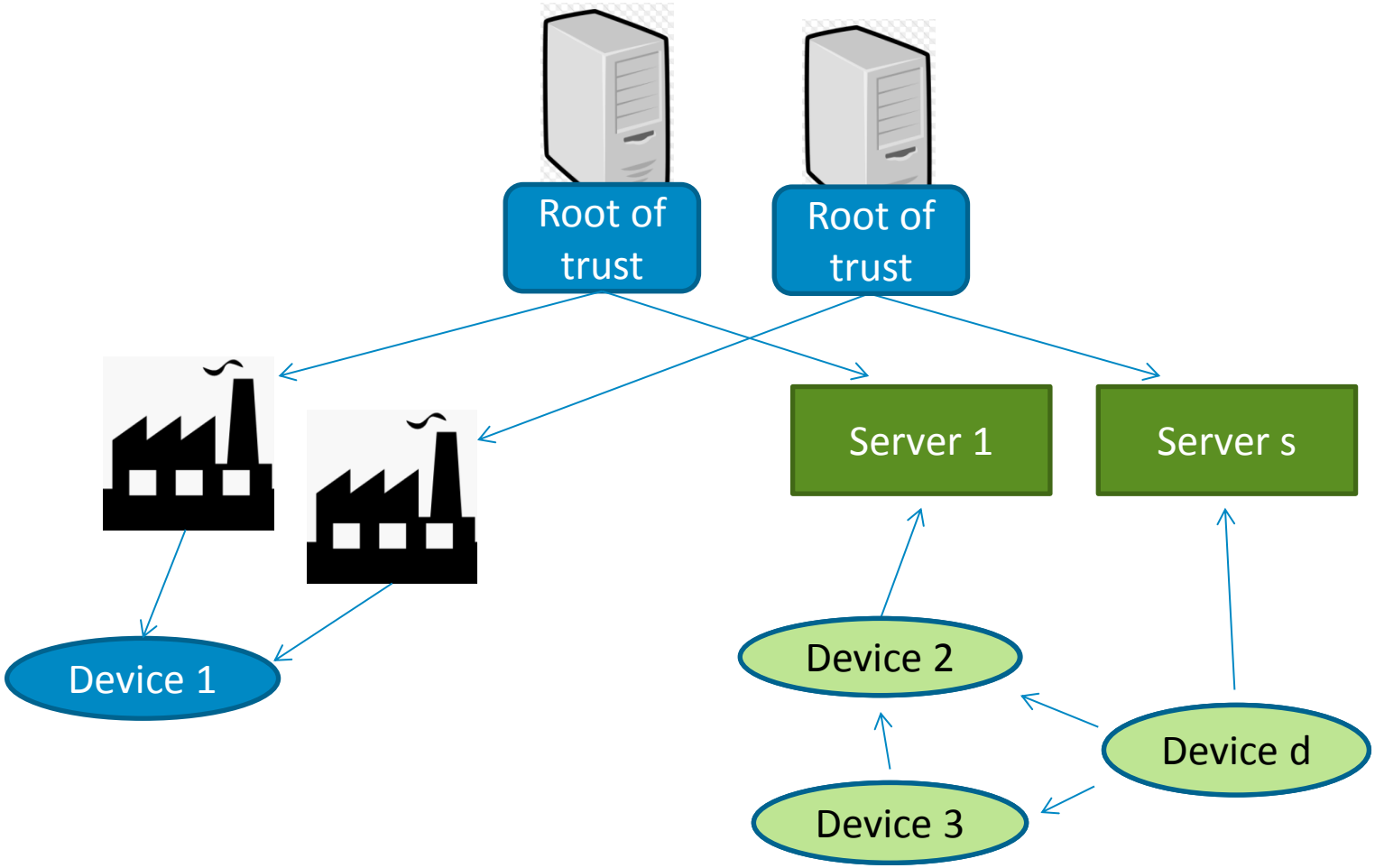


Single TTP cannot fake the MAC that verifies x's public key (pu_x)

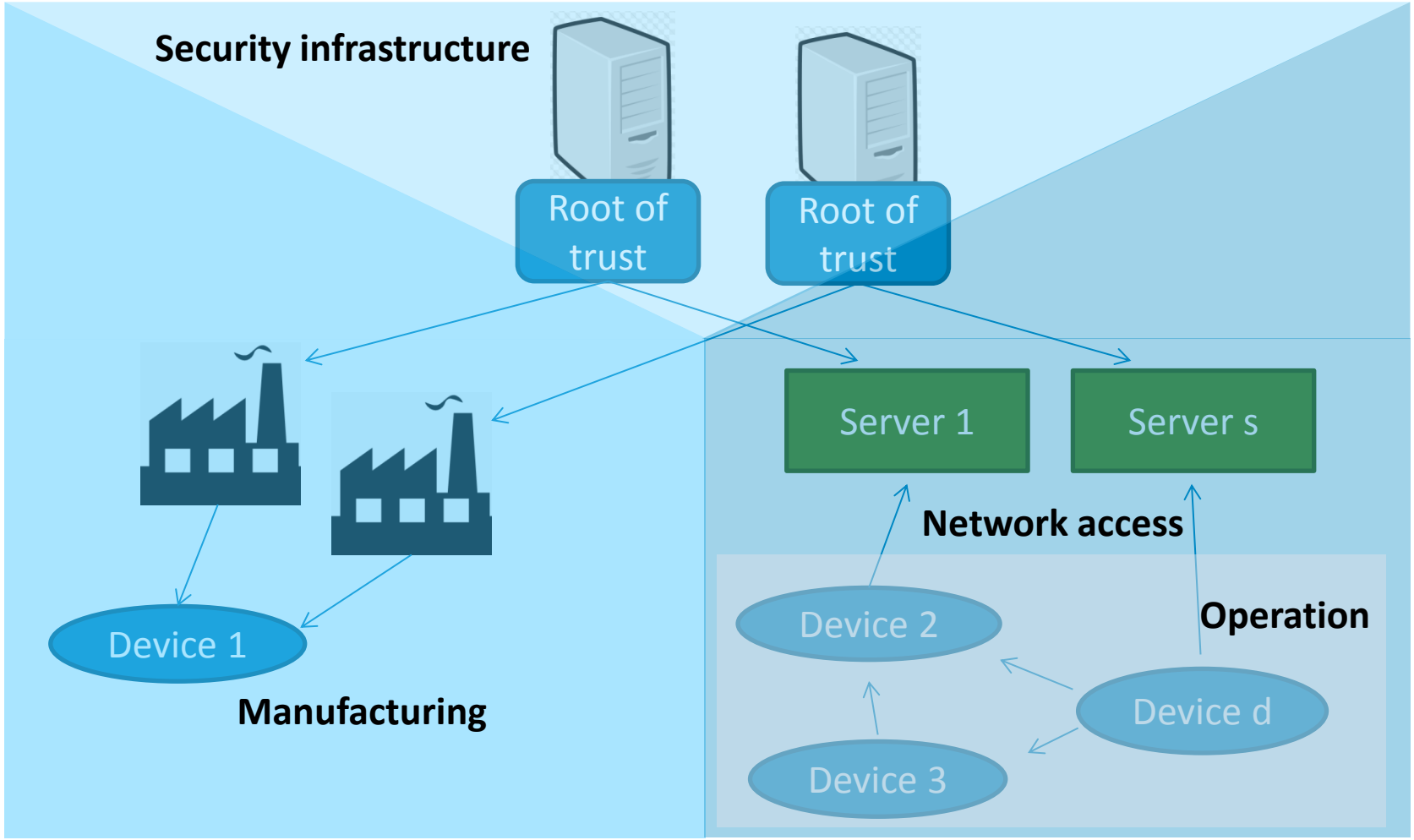


O. Garcia-Morchon, R. Rietman, L. Tolhuizen, J.L. Torre-Arce, S. Bhattacharya and M. Bodlaender "Efficient quantum-resistant trust Infrastructure based on HIMMO", IACR ePrint Archive, Report 2016-410

Device Lifecycle and Security Needs



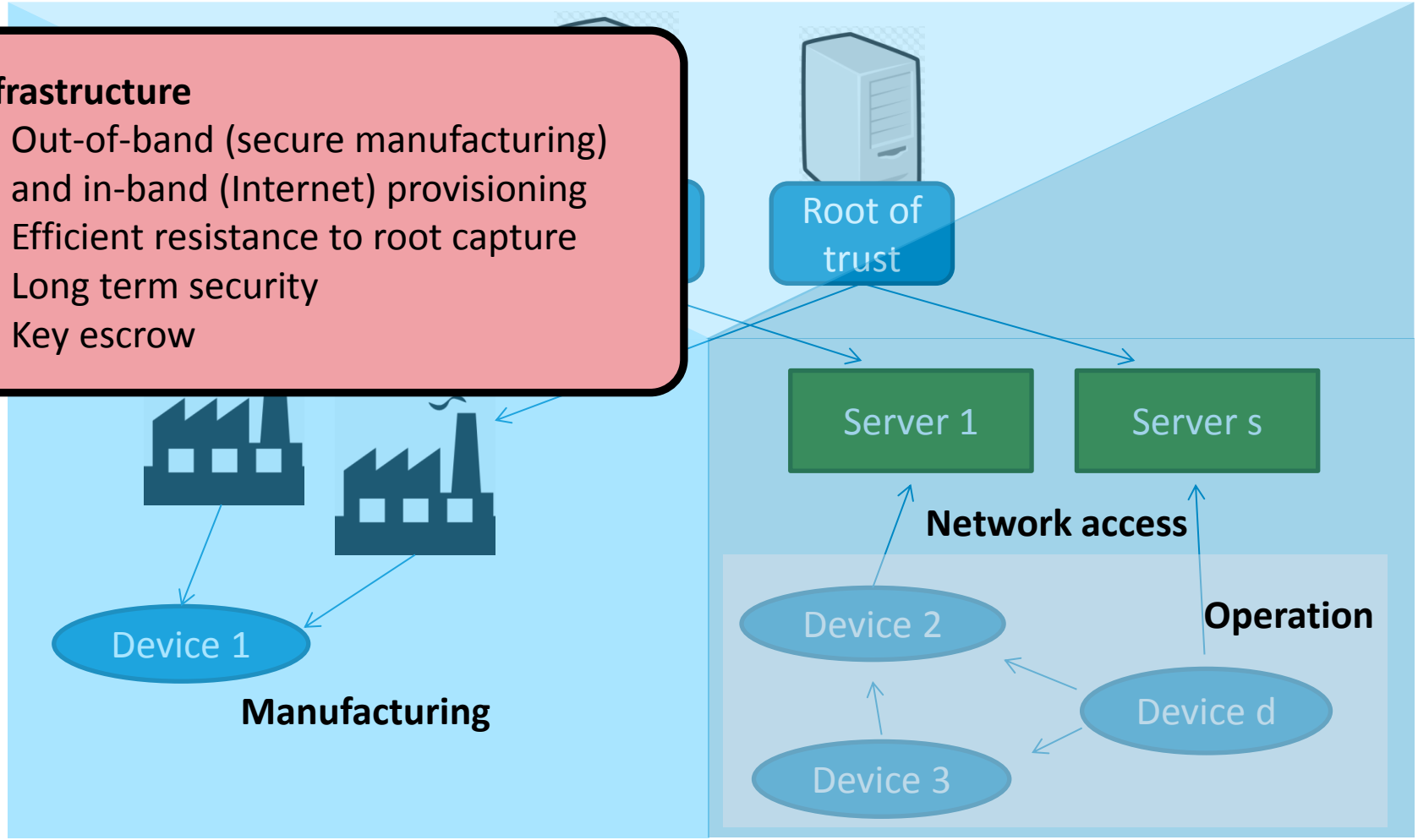
Device Lifecycle and Security Needs



Device Lifecycle and Security Needs

Infrastructure

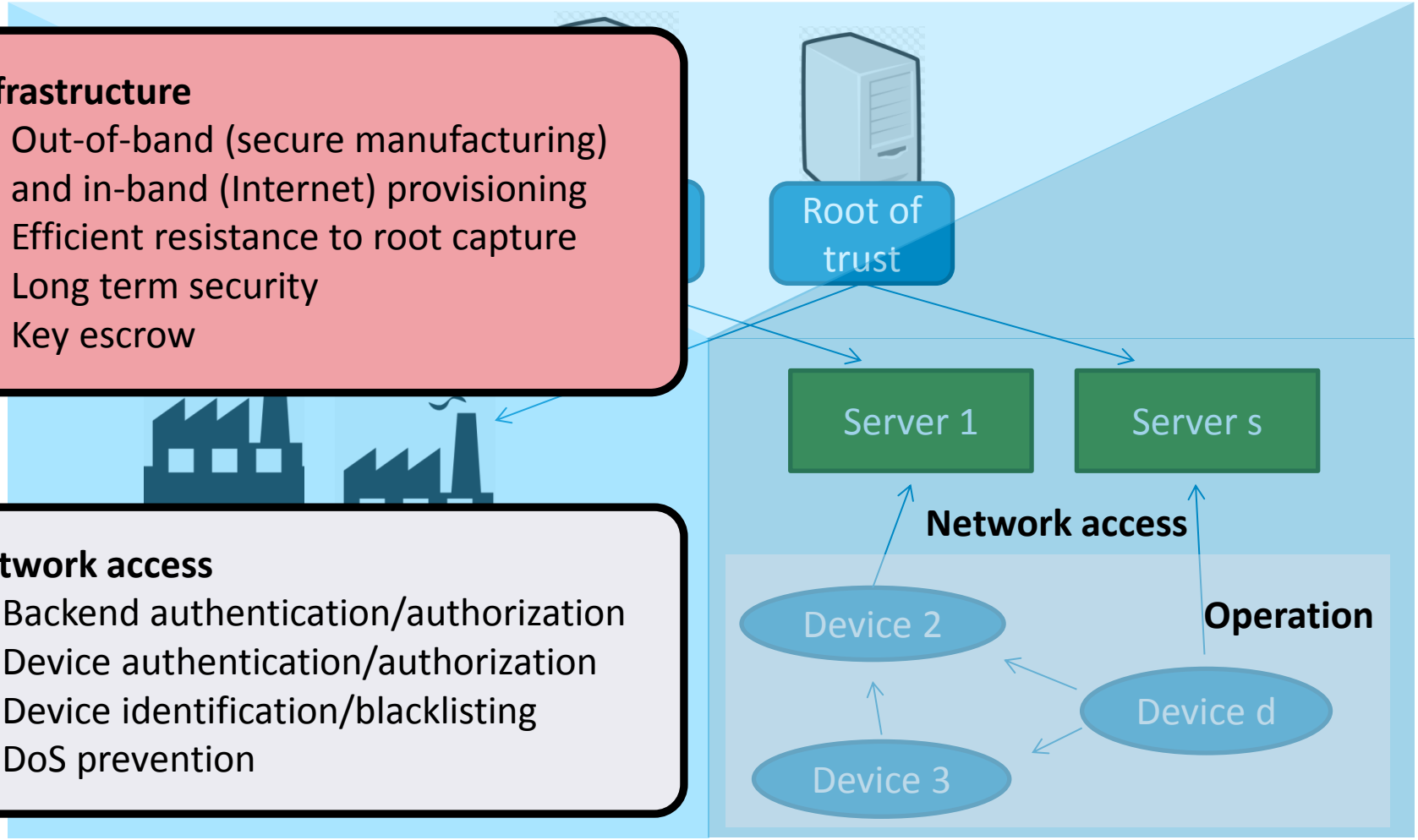
- Out-of-band (secure manufacturing) and in-band (Internet) provisioning
- Efficient resistance to root capture
- Long term security
- Key escrow



Device Lifecycle and Security Needs

Infrastructure

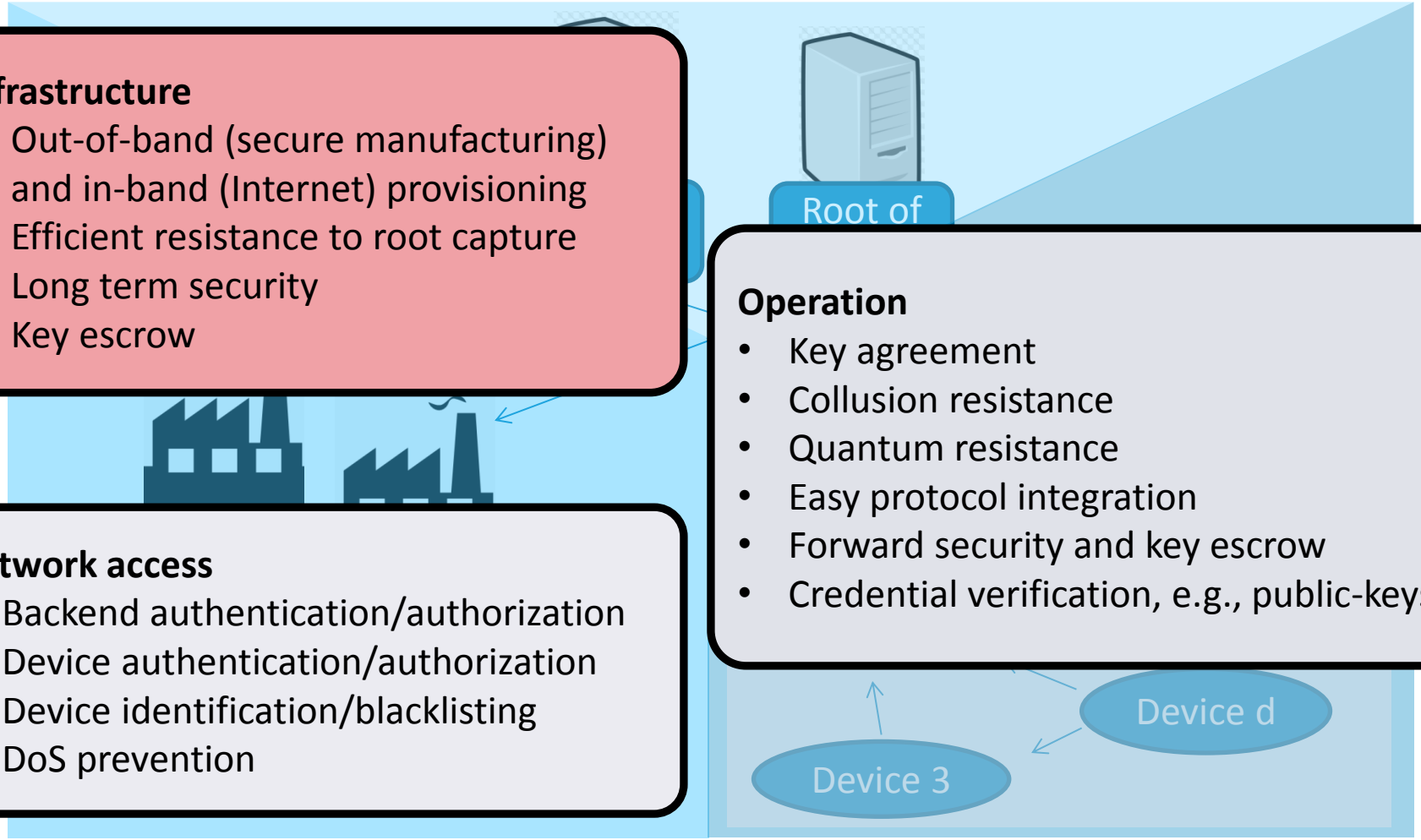
- Out-of-band (secure manufacturing) and in-band (Internet) provisioning
- Efficient resistance to root capture
- Long term security
- Key escrow



Network access

- Backend authentication/authorization
- Device authentication/authorization
- Device identification/blacklisting
- DoS prevention

Device Lifecycle and Security Needs



Infrastructure

- Out-of-band (secure manufacturing) and in-band (Internet) provisioning
- Efficient resistance to root capture
- Long term security
- Key escrow

Operation

- Key agreement
- Collusion resistance
- Quantum resistance
- Easy protocol integration
- Forward security and key escrow
- Credential verification, e.g., public-keys

Network access

- Backend authentication/authorization
- Device authentication/authorization
- Device identification/blacklisting
- DoS prevention