PHILIPS

sense and simplicity

Key Security Challenges in Smart Swarm of Things

NIST/CETA Workshop,
Gaithersburg (USA), November 2011

Oscar Garcia-Morchon, Sye Loong Keoh, Sandeep Kumar
Philips Research Europe

Agenda

- Smart Swarm of Things
- Key establishment
- ID-based symmetric-key agreement
- Conclusions

PHILIPS

Smart Swarm of Things

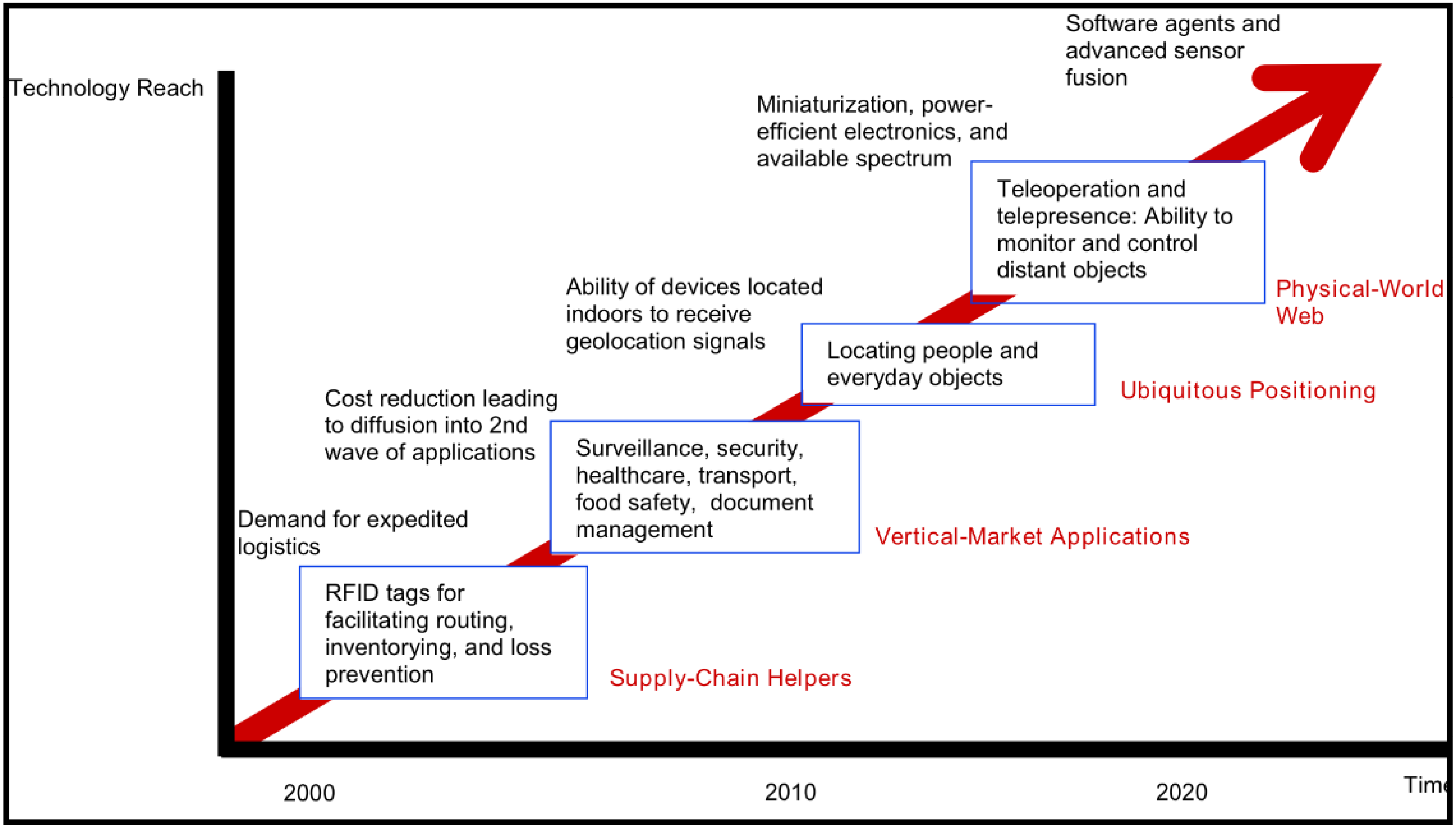
Smart Swarm of Things (1/2)

Low-Power RF
CC2530
Texas Instruments
The Internet of Things
AUTO-ID CENTER
Wi Fi
EPCglobal
I E T F
Lte
SANYO
HH CQ 7822
184
POWER NOW WATTS
126
186
ONZO
MELFI VENEZUELA

“Ubiquitous computing“ (1991, Mark Weiser)

Source: SRI Consulting Business Intelligence

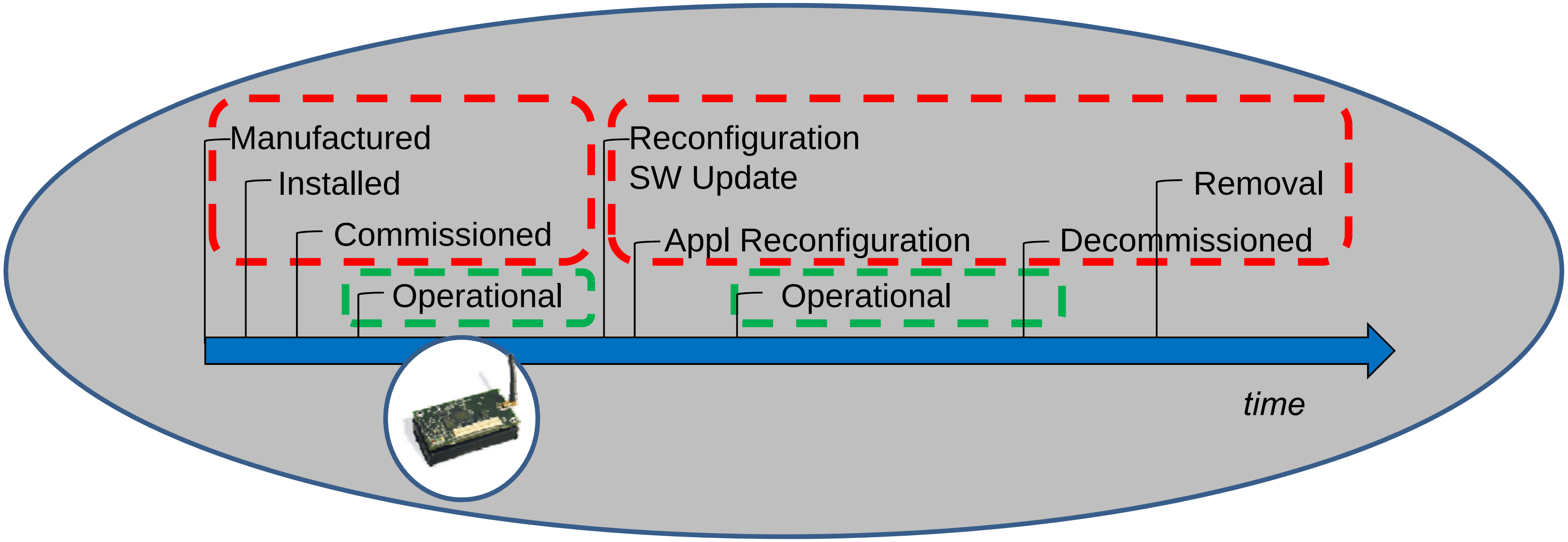
Smart Swarm of Things (2/2)



Technology Reach
Software agents and advanced sensor fusion
Miniaturization, power-efficient electronics, and available spectrum
Teleoperation and telepresence: Ability to monitor and control distant objects
Physical-World Web
Ability of devices located indoors to receive geolocation signals
Locating people and everyday objects
Ubiquitous Positioning
Cost reduction leading to diffusion into 2nd wave of applications
Surveillance, security, healthcare, transport, food safety, document management
Vertical-Market Applications
Demand for expedited logistics
RFID tags for facilitating routing, inventorying, and loss prevention
Supply-Chain Helpers
2000
2010
2020
Time

PHILIPS

Operational Requirements



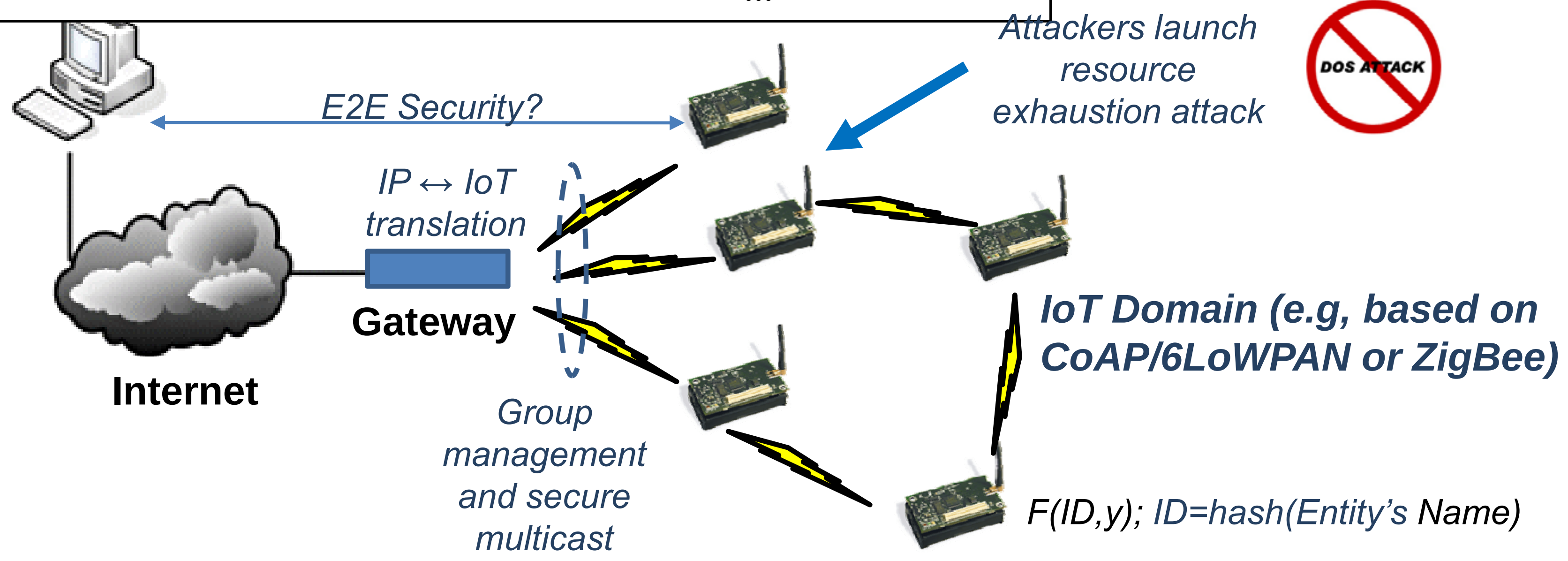
- **Lifecycle** of SSoT
- SSoT comprises **multi-vendo**r *Things*
- SSoT is featured by **multi-user control**
- **Heterogeneous** applications and networks comprise the SSoT

PHILIPS

SecurityNeeds

Bootstrapping	Operation
Incremental deployment	End-to-End security
Privacy protection	Mobility support
Group creation	Privacy protection
Identity and key management	Heterogeneous IoT domains
….	Group membership
	DoS resistance
	…

Distributed vs Centralized ??

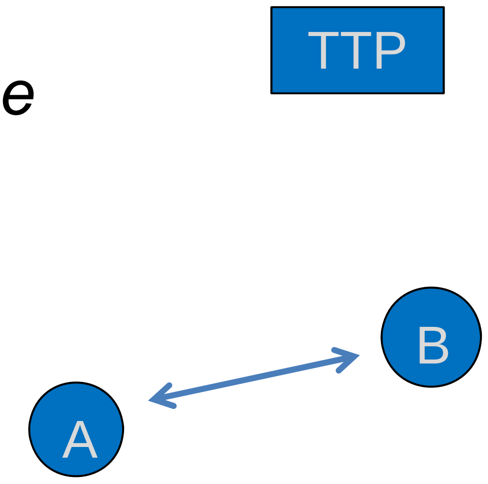

E2E Security?
IP ↔ IoT translation
Gateway
Internet
Attackers launch resource exhaustion attack
DOS ATTACK
IoT Domain (e.g, based on CoAP/6LoWPAN or ZigBee)
Group management and secure multicast
F(ID,y); ID=hash(Entity's Name)

http://tools.ietf.org/html/draft-garcia-core-security-03

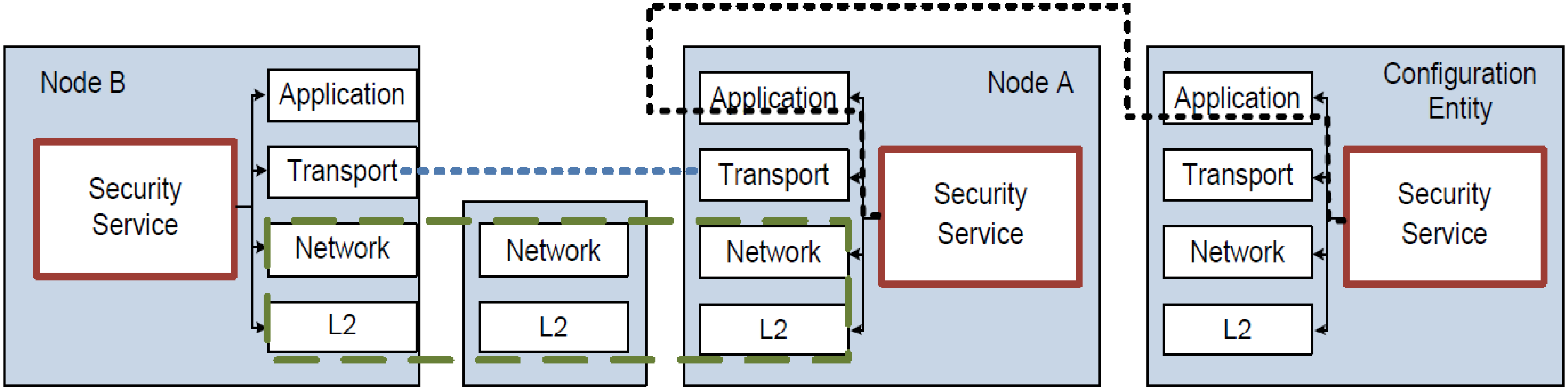
Identification and Key Establishment

Goals (*and reasons*)

- Suitable for SSoT operation
  - *for simple usage*
- Feasible in constrained devices/networks
  - *to guarantee a basic & interoperable solution*
- Mutual identification/authentication
  - *to verify the involved parties*
- Establish a secure connection
  - *to ensure the secure data exchange*



SSoT operation

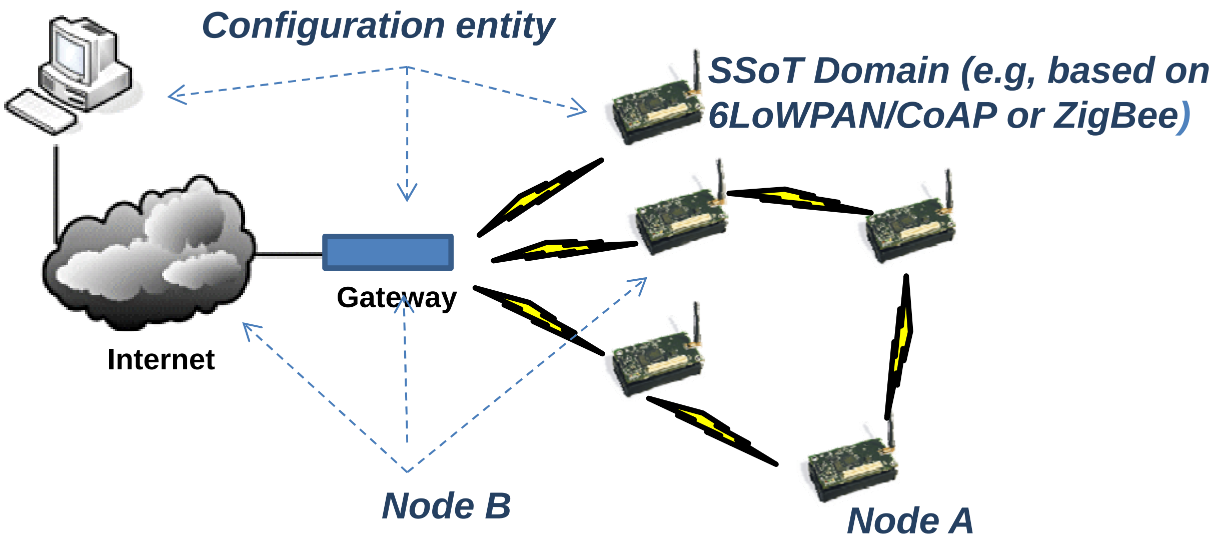


Application security ▪▪▪▪▪

Bootstrapping ▪▪▪▪▪

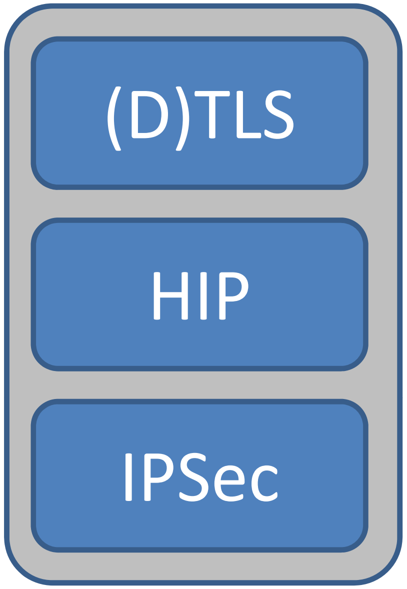
Network security ▭

Thing security model 🟥



At which level?

- e.g., in the IP-based SSoT -



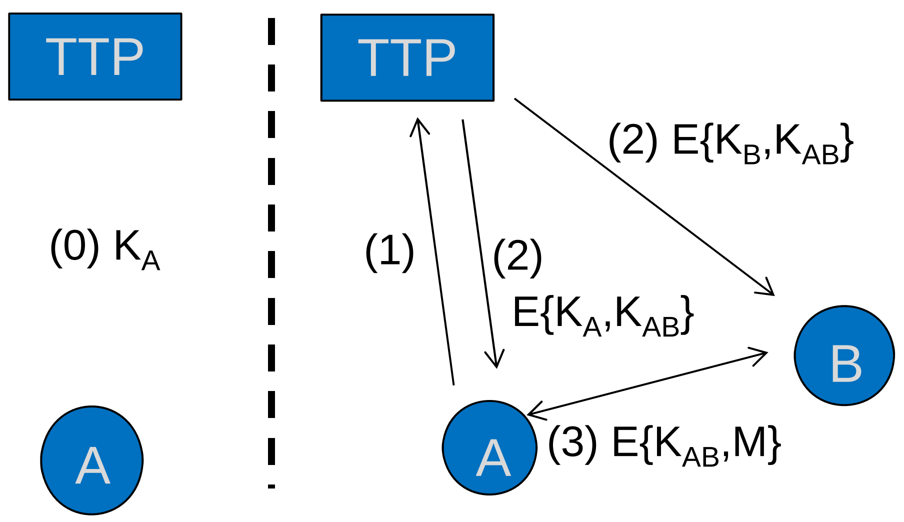
Application level:
Security connection bound to a socket

Device level:
Security connection bound to a HIT

Interface level:
Security connection bound to an IP address

- SSoT should be able to identify "*Things*"
- Conceptually, the device level seems to be the most suitable

Online KDC



TTP

(0) K_A

A

TTP

(1)

(2) $E\{K_A,K_{AB}\}$

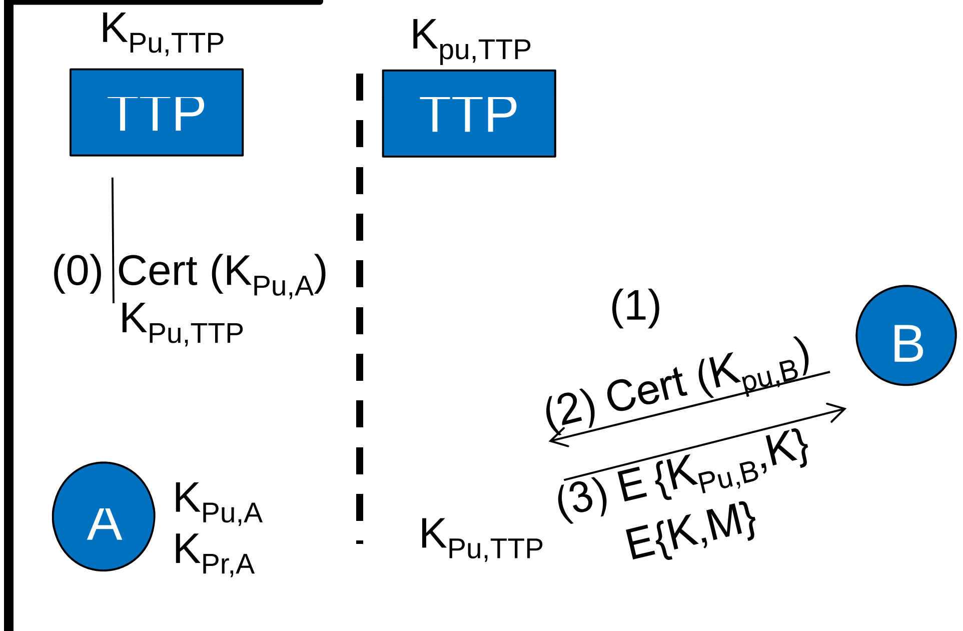
(2) $E\{K_B,K_{AB}\}$

A

B

(3) $E\{K_{AB},M\}$

PKI



$K_{Pu,TTP}$

TTP

(0) Cert ($K_{Pu,A}$)

$K_{Pu,TTP}$

A

$K_{Pu,A}$

$K_{Pr,A}$

$K_{pu,TTP}$

TTP

(1)

B

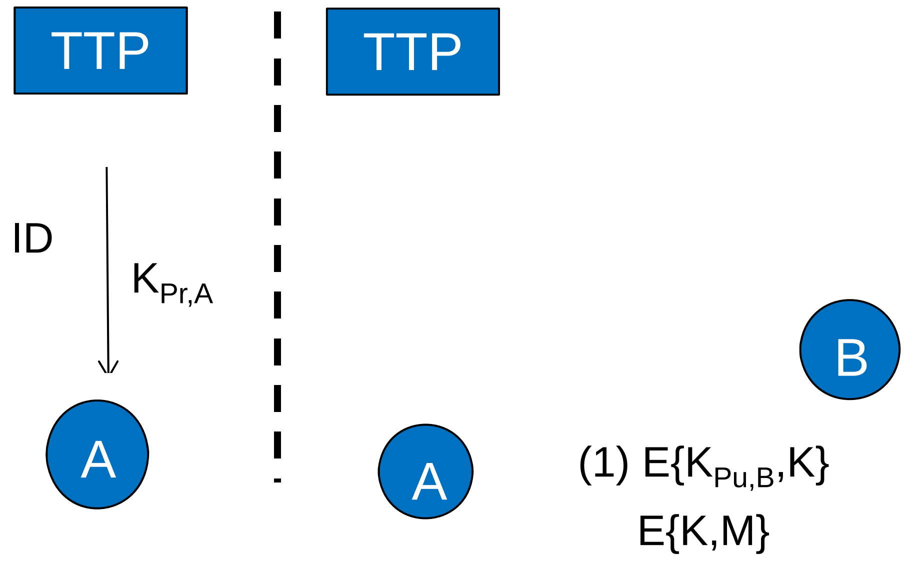
(2) Cert ($K_{pu,B}$)

(3) E $\{K_{Pu,B},K\}$

$E\{K,M\}$

$K_{Pu,TTP}$

IBE



TTP

ID

$K_{Pr,A}$

A

TTP

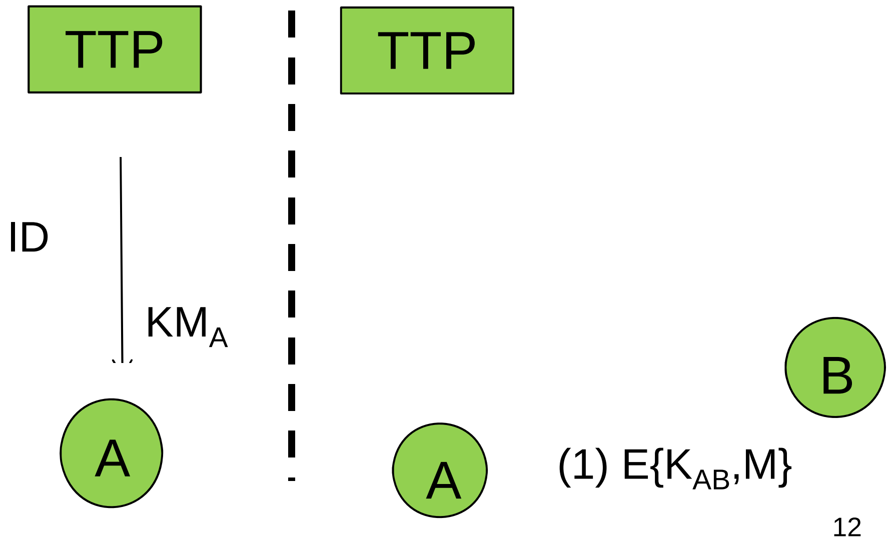
B

A

(1) $E\{K_{Pu,B},K\}$

$E\{K,M\}$

ID-based symmetric-key



TTP

ID

KM_A

A

TTP

B

A

(1) $E\{K_{AB},M\}$

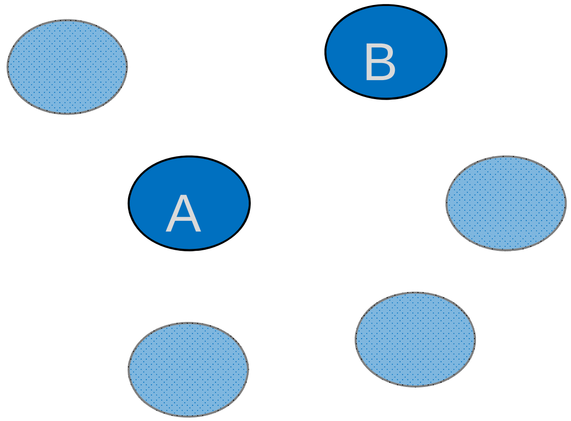
A single solution to ensure interoperability?

- Online Key Distribution Center
  - scalability
- Public-key infrastructure
  - Resources needs/message exchange
- Identity-based Crypto
  - ID can be bound to a *Thing* identifier, e.g., HIT
  - But…bad performance
- Existing ID-based symmetric-key
  - Good performance,
  - But bad scalability

ID-based scheme for direct lightweight symmetric-key generation??

ID-based symmetric-key agreement

ID-based symmetric-key agreement (1/4)



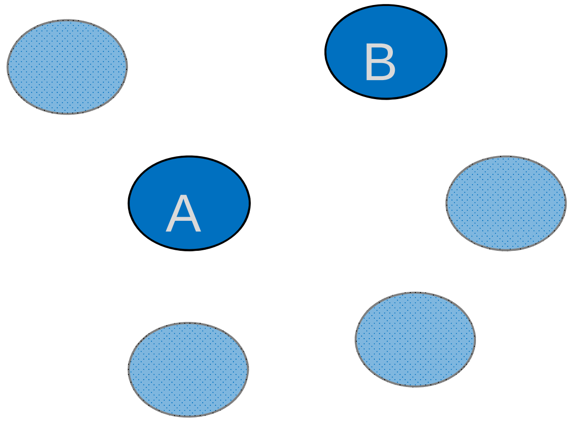
Fully pairwise scheme

- Each pair of *Things* shares a pairwise key

Features

- Each *Thing* stores N-1 keys
- In the system N(N-1)/2 keys
- It does not scale

ID-based symmetric-key agreement (2/4)



Polynomial scheme (*)

- TTP owns a symmetric polynomial f(x,y)
- Each *Thing* with identifier ID receives f(ID,y)
- Optionally,
  - ID = hash (Identification Information)
  - ID could be the network address

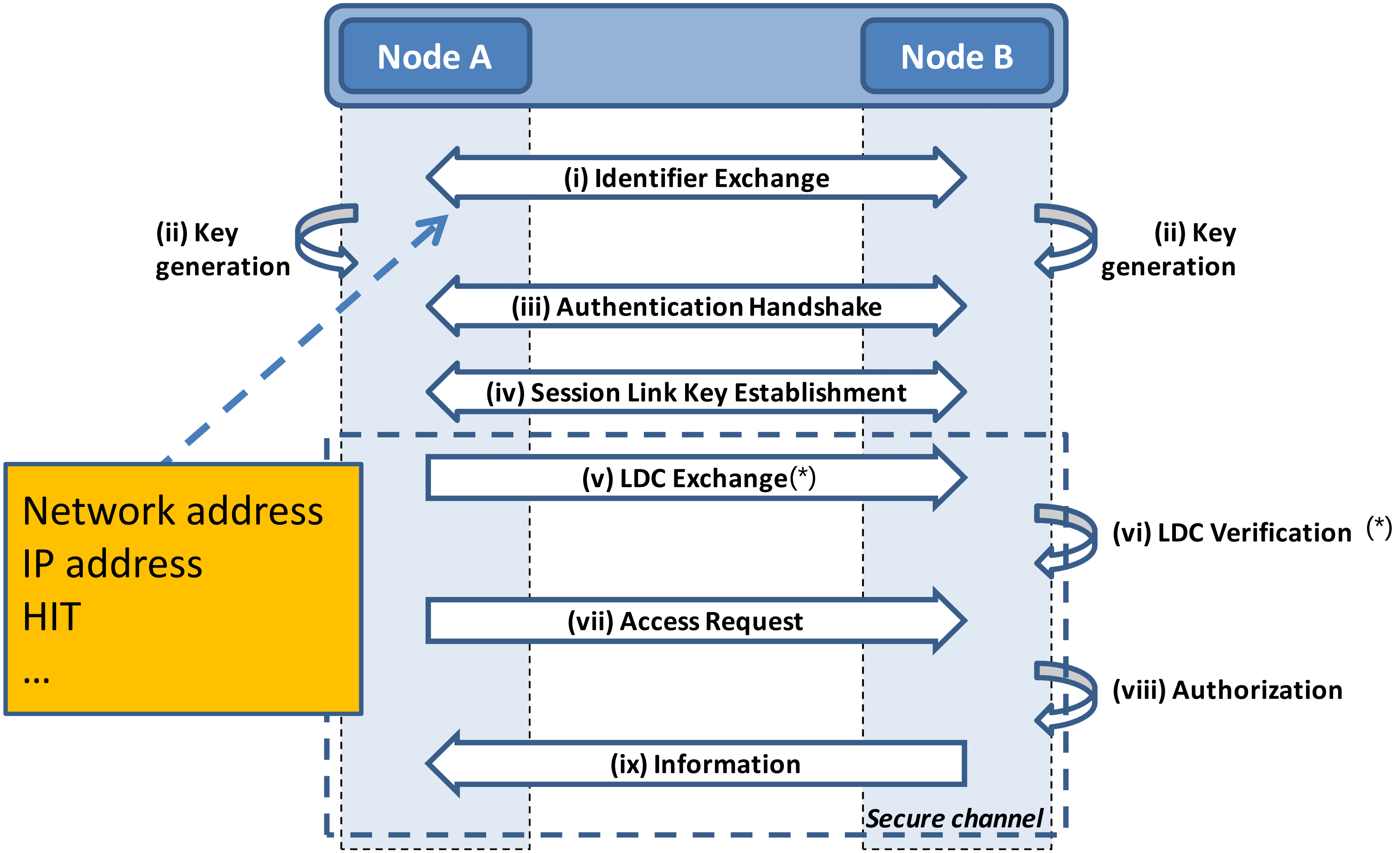
Features

- Effortless key establishment between any pair of *Things*
- Implicit verification of identification information
- But, scalability & performance limited by the polynomial degree

(*) related to Blom, R.: "An Optimal Class of Symmetric Key Generation Systems," in proc. of Advances in Cryptology, 335-338, 1984.

PHILIPS

ID-based symmetric-key agreement (3/4)



NIST CETA Workshop, November 2011

(*)LDC = Identification Information

ID-based symmetric-key agreement (4/4)

- Polynomial schemes
  - Nice operational features
  - But limited scalability

- If we had… an ID-based scheme
    - with the operational features of a polynomial scheme,
    - but without the t-threshold
  - Any pair of *Things* would be able to
    - directly generate a pairwise key from their identities (IP, HIT,…)
    - mutually authenticate to each other
    - verify configuration parameters

- Attempt to create such a scheme based on “perturbation-polynomials”
  - However, it is broken

Conclusions

Conclusions

- SSoT: evolution & revolution
- Identification and key establishment are key in SSoT
  - at which level?
  - a single solution to ensure interoperability?
- An interesting way: ID-based symmetric-key agreement @ device level

PHILIPS