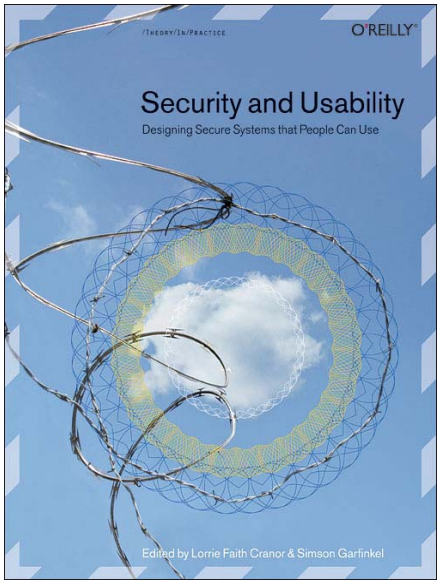
Security and Ease of Use

René Struik
(Certicom Research)
E-mail: rstruik@certicom.com

"For those viewing via webcast, please submit questions for this presentation to kmwquestions@nist.gov"

Security and Ease of Use



"Computer users have been taught for years that computer security systems can't be effective unless they are complex and difficult to use. In reality, this conventional wisdom is completely wrong."

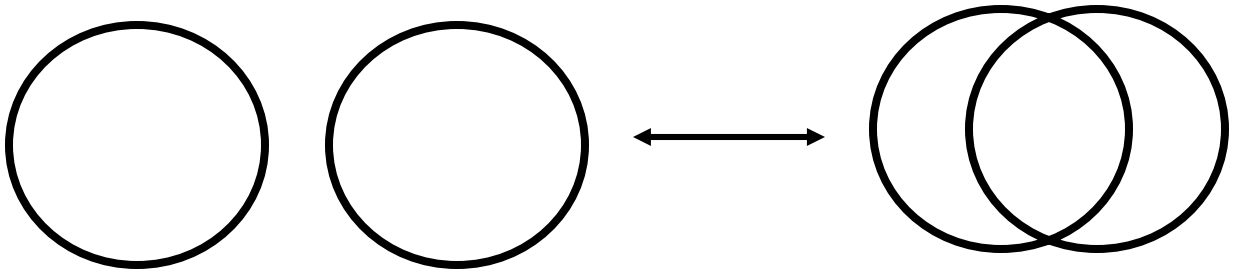
— Lorrie Faith Cranor, Carnegie Mellon University

Security technology can make trust lifecycle management intuitive and hidden from the user.

Figure 1. Connecting a laptop to a secured wireless network in 32 seconds. All the user has to do is briefly align the infrared ports of laptop and access point and press the Enter key twice. These are snapshots from a live Network-in-a-Box demonstration.

Source: D. Balfanz, G. Durfee, R.E. Grinter, D.K. Smetters, P. Stewart, "Network-in-a-Box: How to Set Up a Secure Wireless Network in under a Minute," in *Proceedings of the 13th USENIX Security Symposium*, August 9-13, 2004.

Ease of Configuration and Reconfiguration



Ease of configuration:
- Merging of networks
- Partitioning of networks
- Device portability and orphaning
- Hand-over of control (remote, backup)

Security and Ease of Use – Bridging the Gap

Challenge:

Bridge the gap between state-of-the-art security that is known and security that is actually being used.

Education gap. Conventional wisdom is that “computer security systems can’t be effective unless they are complex and difficult to use”. While this may once have been true, the security profession has witnessed dramatic insights over the last ten years, which has not all been embraced yet by the field.

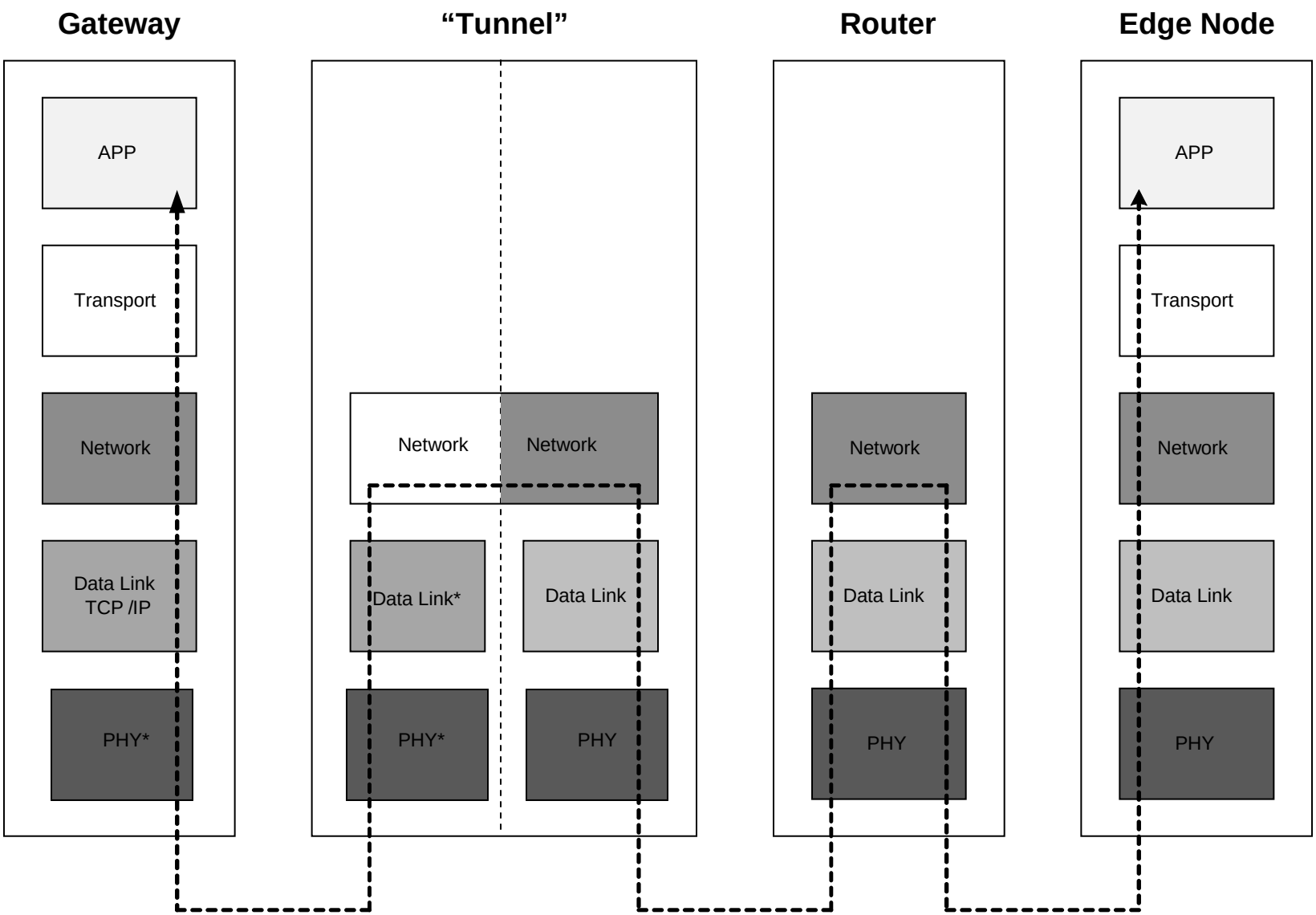
Perception gap. Conventional wisdom is that security technologies are too expensive to implement with sensor and control networks, due to energy constraints, computational and storage constraints. Anno 2008, this perception is challenged for all but the most mundane devices.

Examples: e.g., Bluetooth v2.1, ZigBee Smart Metering, and RFID e-Passport.

Affordability gap. Conventional wisdom is that the licensing cost of security technologies may present a hurdle. Licensing models, such as those used with the consumer electronics industry, may have some merit for ubiquitous computing as well, since both are concerned with mass-scale deployment of networked devices ("the internet of things") and enforcement of compliance.

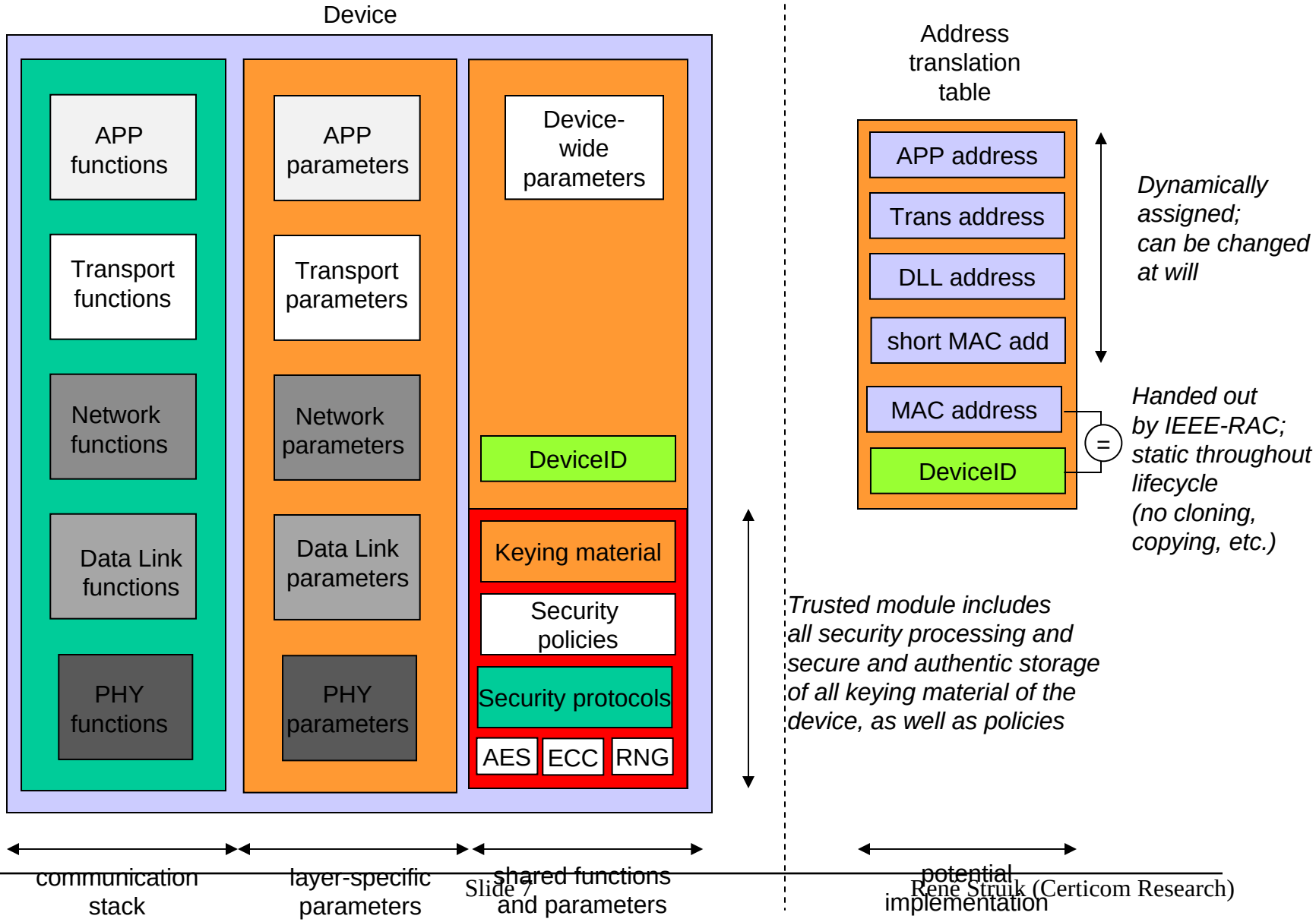
Examples: ZigBee Smart Energy licensing model for public-key technology; flexible business models for deployment tailored to best fit requirements of various players in the supply chain (i.e., can be moved to most suitable point, so as to promote wide-scale adoption).

Devices and Device Ids

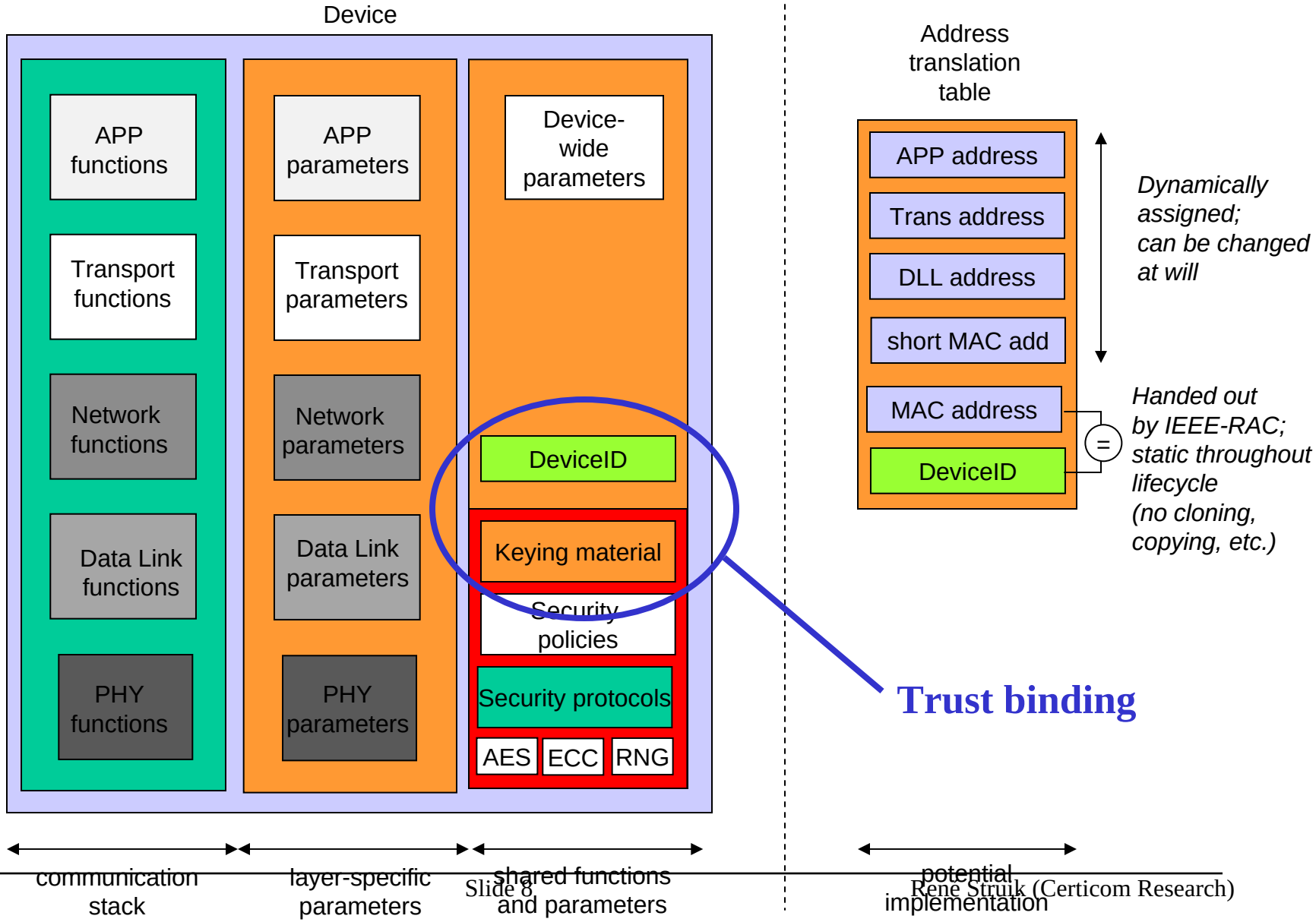


Source: Networking Transport Diagrams for discussion (Jay Werb, March 1, 2007).ppt

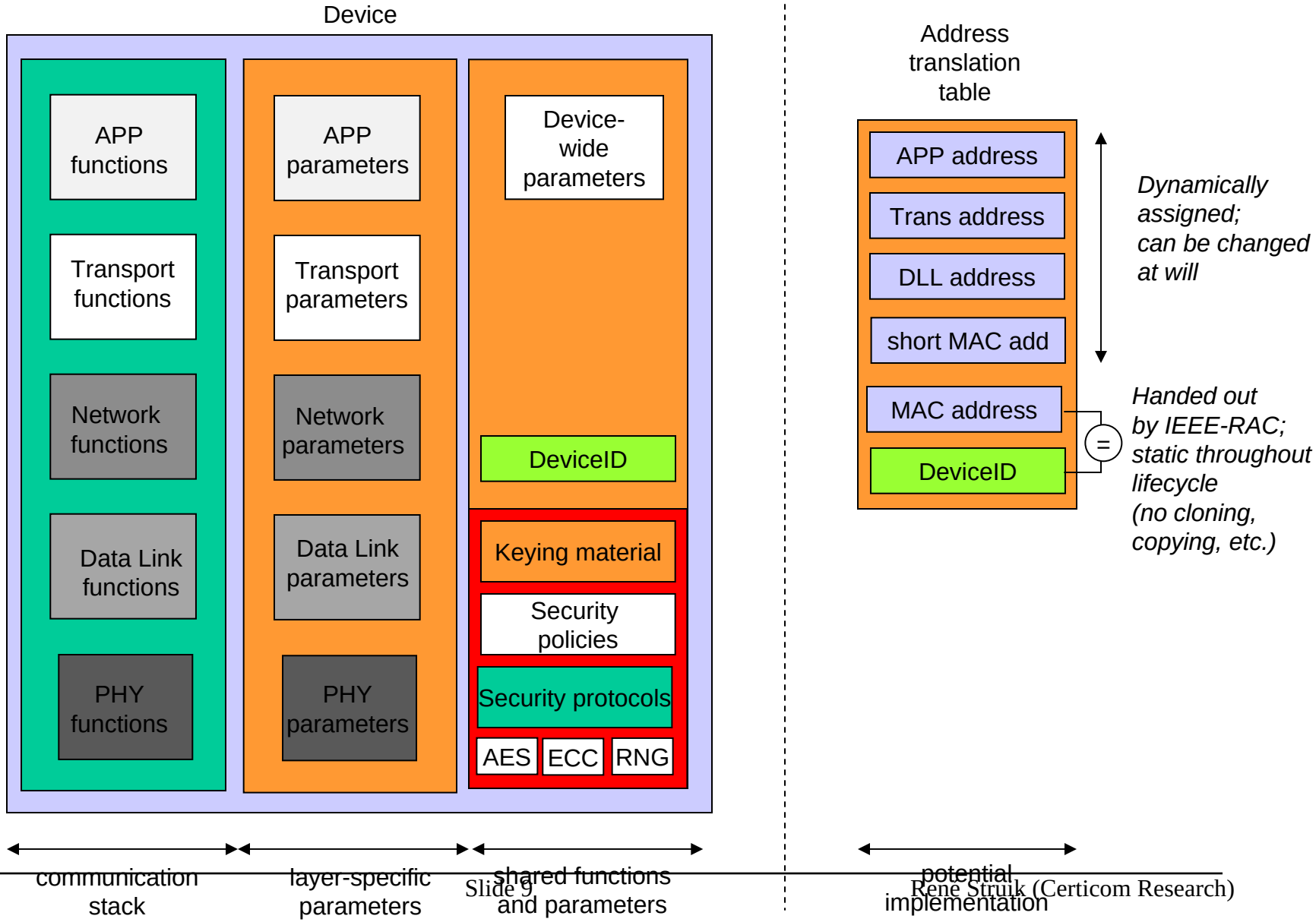
Full stack device, including per-layer and shared parameters



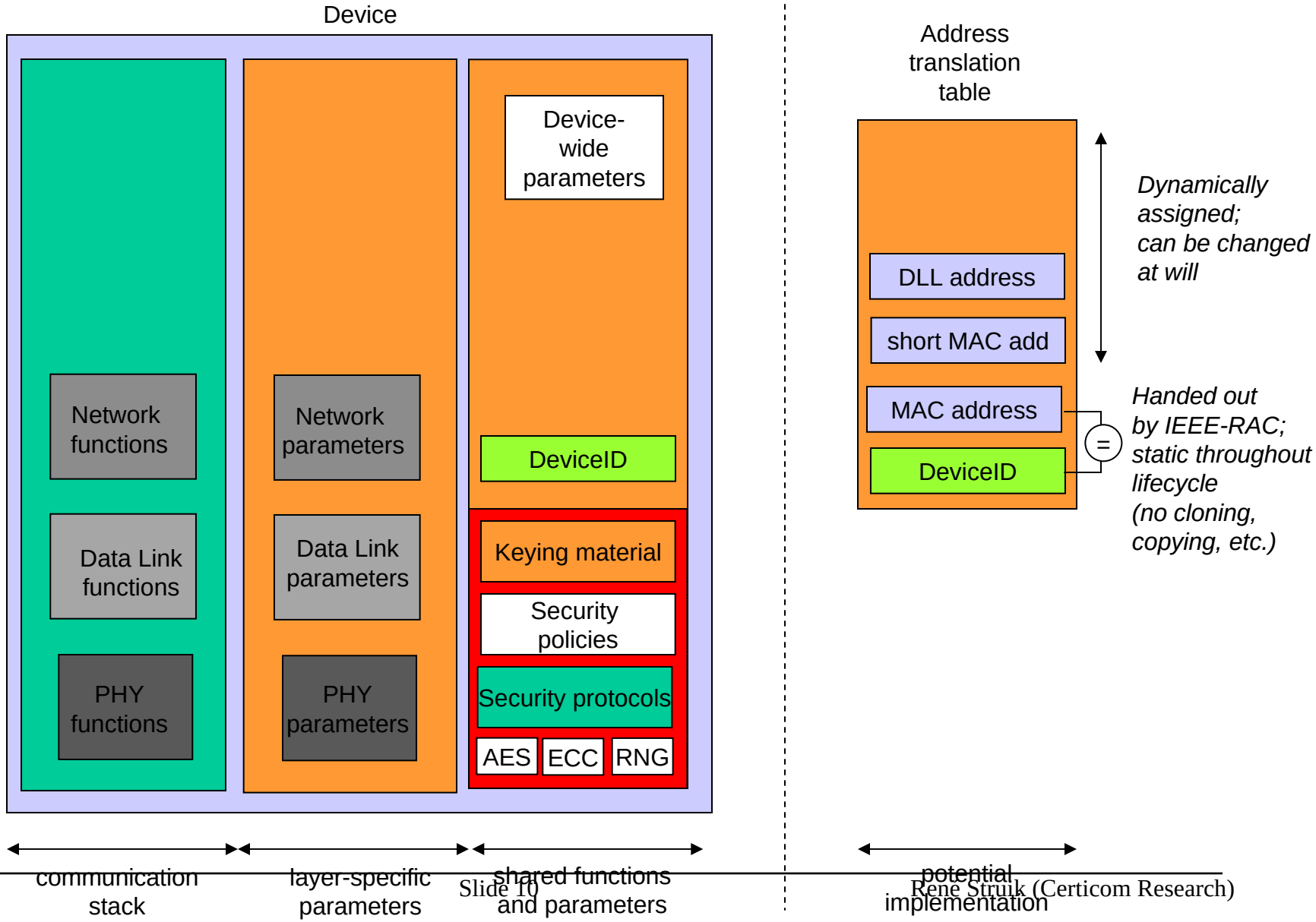
Full stack device, including per-layer and shared parameters



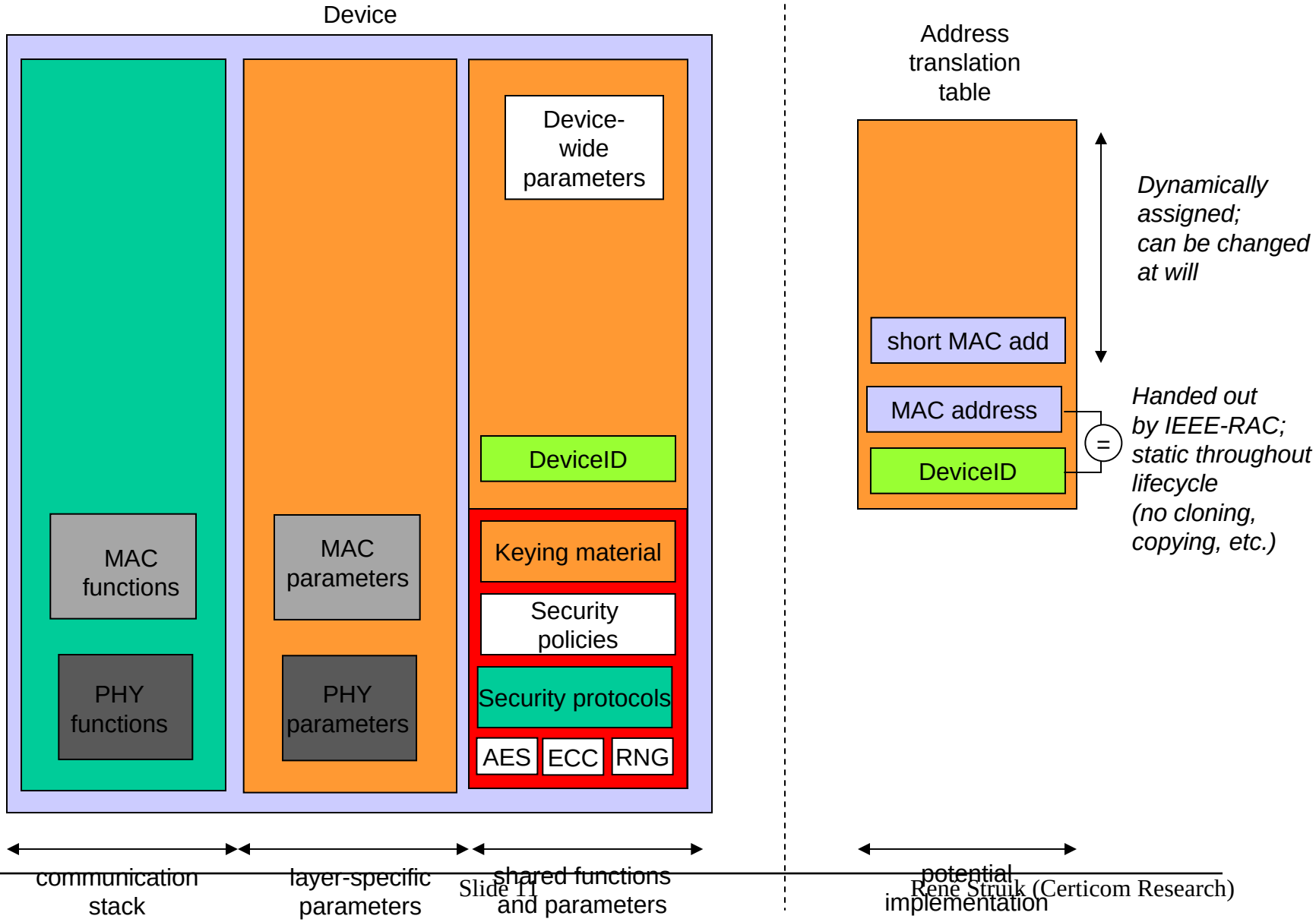
Full stack device, including 802.15.4-2006 transceiver



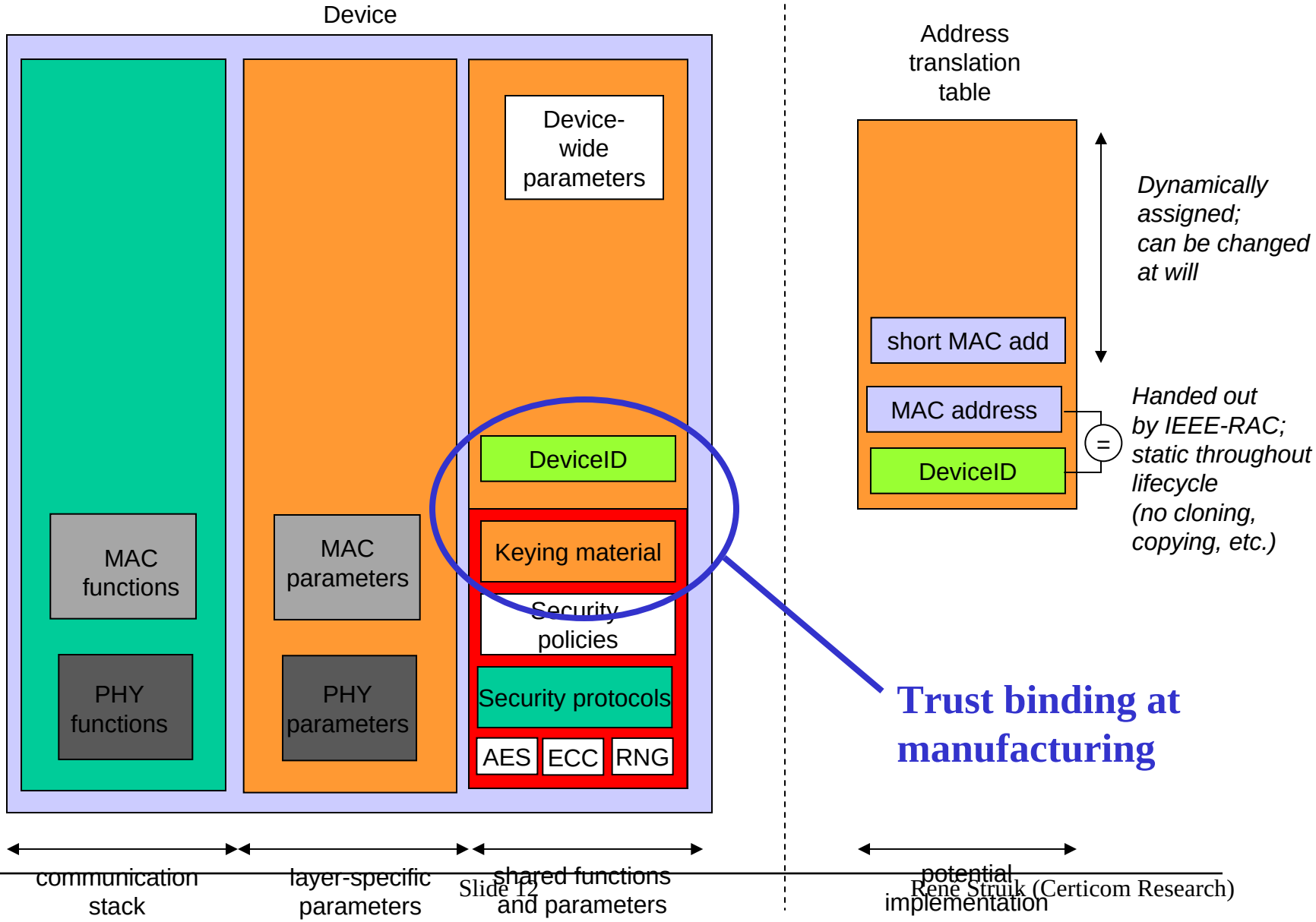
"Lower"-stack device, including 802.15.4-2006 transceiver



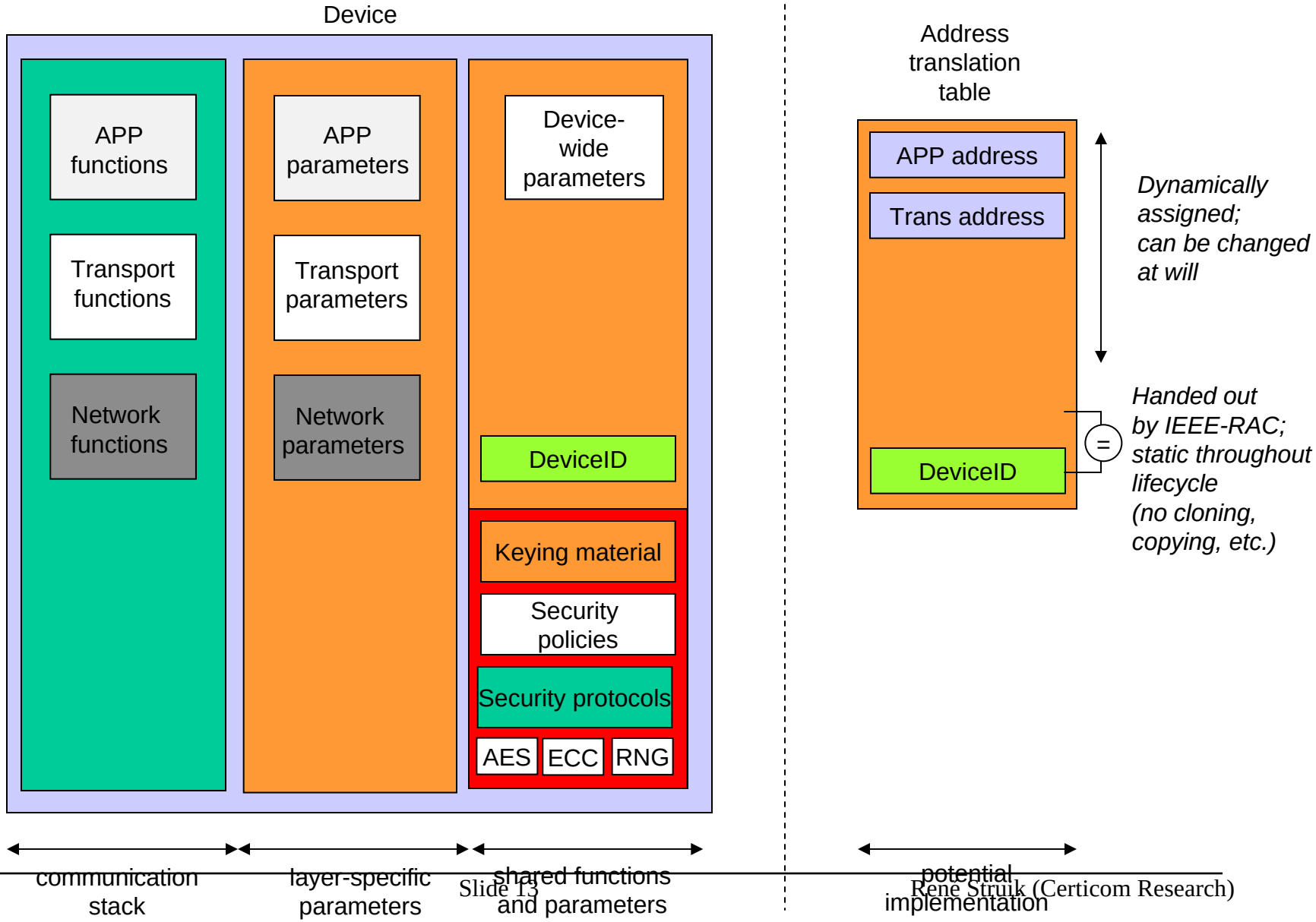
"Lower"-stack device, with just 802.15.4-2006 transceiver



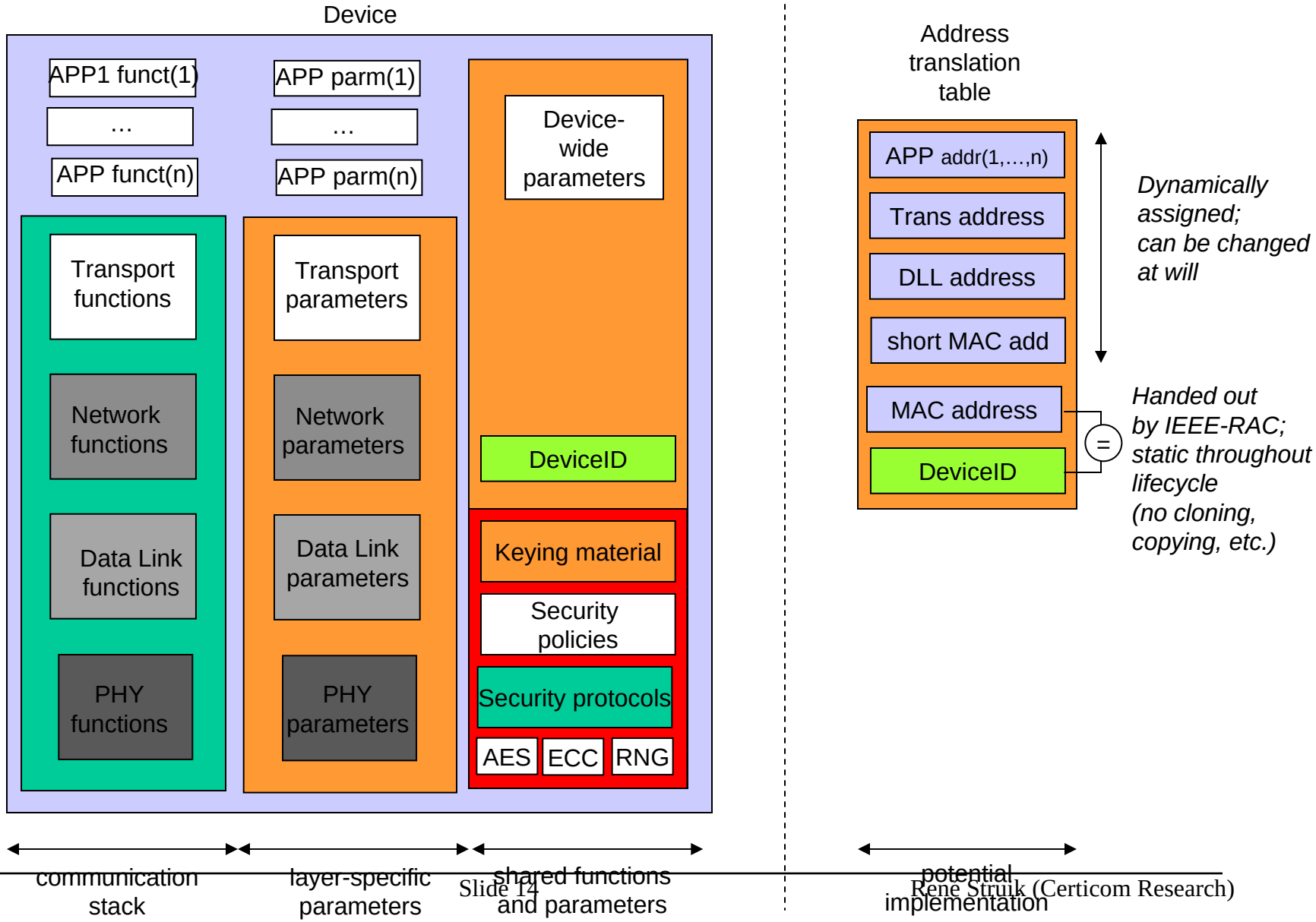
"Lower"-stack device, with just 802.15.4-2006 transceiver



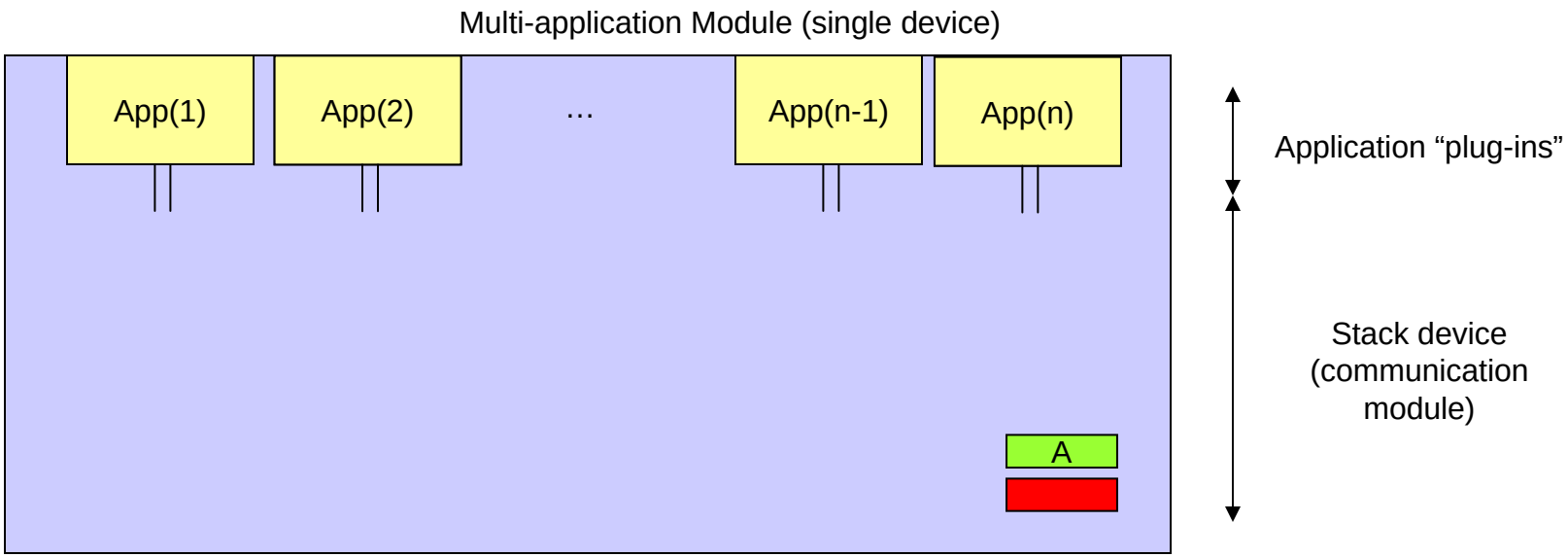
"Upper"-stack device, without 802.15.4-2006 transceiver



Multi-application device, including 802.15.4-2006 transceiver



Multi-application device



This multi-application module is a single device

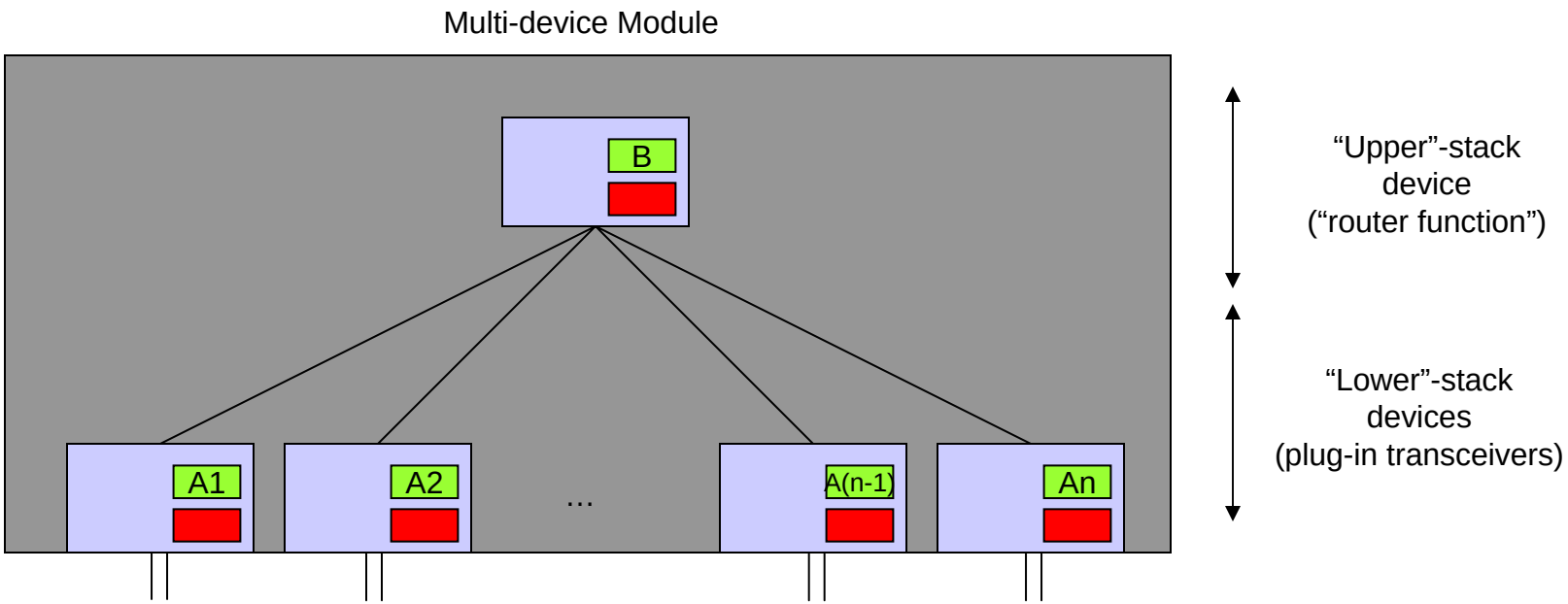
– Device A: takes care of complete communication stack

– "Plug-ins" App(1, ...,n): handle applications, e.g., FieldBus, HART, PROFIBUS

Different applications are independently sourced, but rely on shared communication stack and "open" trust model within device A

Non-monolithic stack device, including 802.15.4-2006 transceiver

"router", akin to WiFi router with multiple transceivers



Conceptually, this device is a little network, with n+1 nodes

- Device B: takes care of upper-stack/ "transport-and-up" traffic
- Devices A1, …, An: take care of lower-stack/ "kicking traffic to next hop"

Different components are independently sourced, with <u>individual</u> trust routines and <u>individual</u> (partial) communication stack

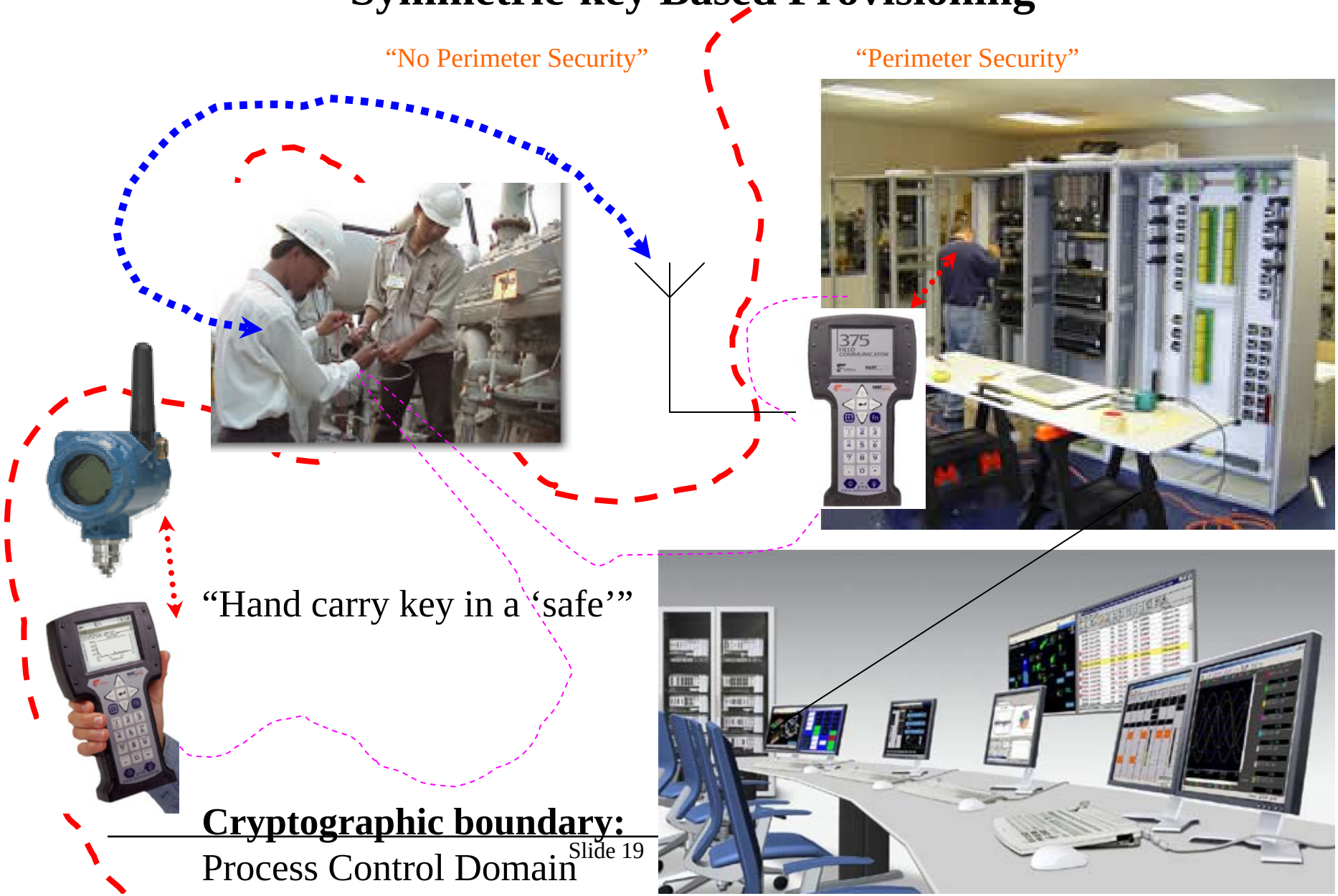
Deployment Scenarios

Idealized Provisioning

"No Perimeter Security"

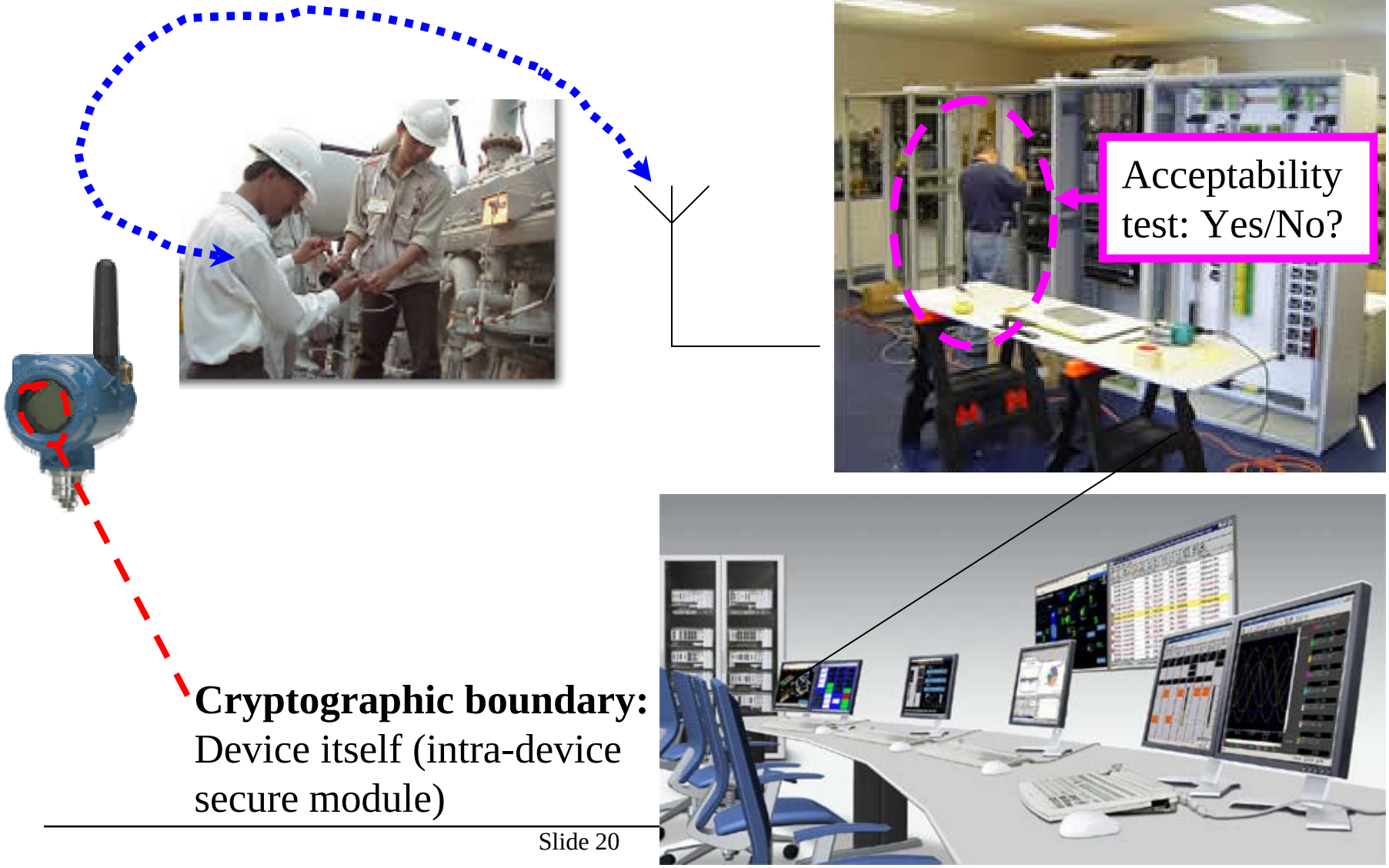
"Perimeter Security"

Symmetric-key Based Provisioning



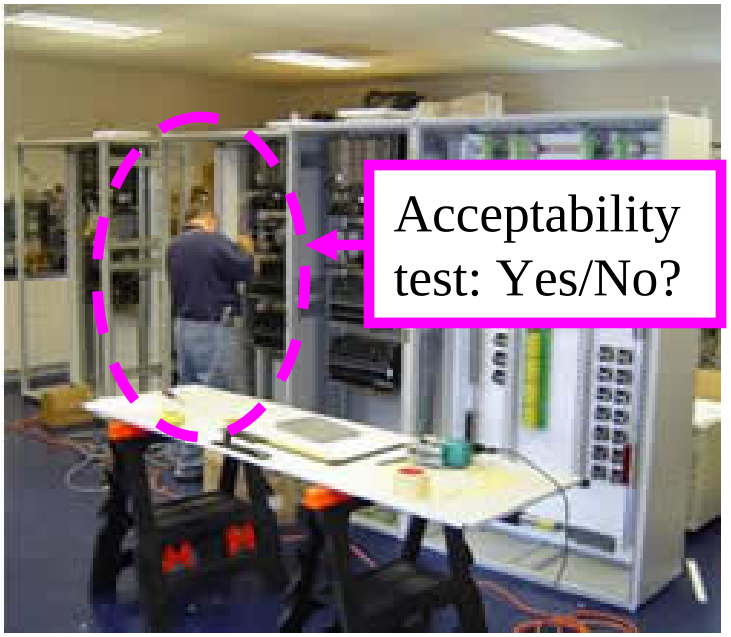
Public-key Based Provisioning (1)

"No Perimeter Security" "Perimeter Security"



Cryptographic boundary: Device itself (intra-device secure module)

Public-key Based Configuration (2)



Acceptability test based on
- Device Id
- Tag Name
- Device Label
- Open enrolment
- Proximity-based techniques

…

Trust management via device identities

Trusted module

- **AES, ECC, RNG**
- **Security policy engine**
- **Storage of keys**

Deployment Scenarios[1]

Scenario #1:
mix-and-match of nodes from different vendors
Scenario #2:
addition of nodes to operational network
Scenario #3:
security audit
Scenario #4:
device repair and replacement (roaming in/out different user sites)
Scenario #5:
network separation (devices joining wrong network)
Scenario #6:
thwarting malicious attacks by (former) insiders
Scenario #7:
thwarting attacks by outsiders via insiders (held at ‘gunpoint’)
Scenario #8:
addition of subsystem (‘skid’) assembled elsewhere to operational network

[1]Deployment scenarios discussed with ZigBee, ISA SP100.11a user community

Desired Features and Benefits (1)

Ease of use. Trust lifecycle management appears the *same* as that of an unsecured network and relies on

- proper identification of devices (e.g., reading off a label of physical module);
- proper management of device roles (e.g., adding these to, resp. removing these from a white list, e.g., via a workstation GUI).

Thus, trust lifecycle management relies completely on handling of *public* information.

Flexibility. Virtually no restrictions w.r.t. support for

- mix-and-match of devices from different vendors;
- changes to network topology (merging or partitioning of networks, device replacement or addition, addition of pre-assembled subsystem);
- changes to device roles (e.g., smooth hand-over of system manager, security manager roles, via ‘soft reboot’);
- back-up and failure recovery (since management fully relies on *public* information).

Desired Features and Benefits (2)

Minimizes trust dependencies. If secret information is never disclosed,

- Greatly reduced reliance on trustworthy personnel;
- Virtually no training requirements for operational personnel;
- Virtual removal of trust dependencies between different entities in value chain (whether OEM, vendor, system integrator, installer, or user).
- Ease of security auditability.

Support for flexible deployment and business models. If no secret information is ever disclosed during a device's or network's lifecycle, network topology changes or device role changes present a 'clean' logical separation between state prior to and after such an event (thus, allowing subscription-based services, outsourced management, re-contracting, etc.).

Enforcement of standards compliance. Enforced by only issuing a certificate to devices from vendors that passed conformance testing.

No reliance on configuration tools and out-of-band configuration steps. A configuration tool may be used, but is not strictly necessary for trust enforcement.

Evaluation criteria (1)

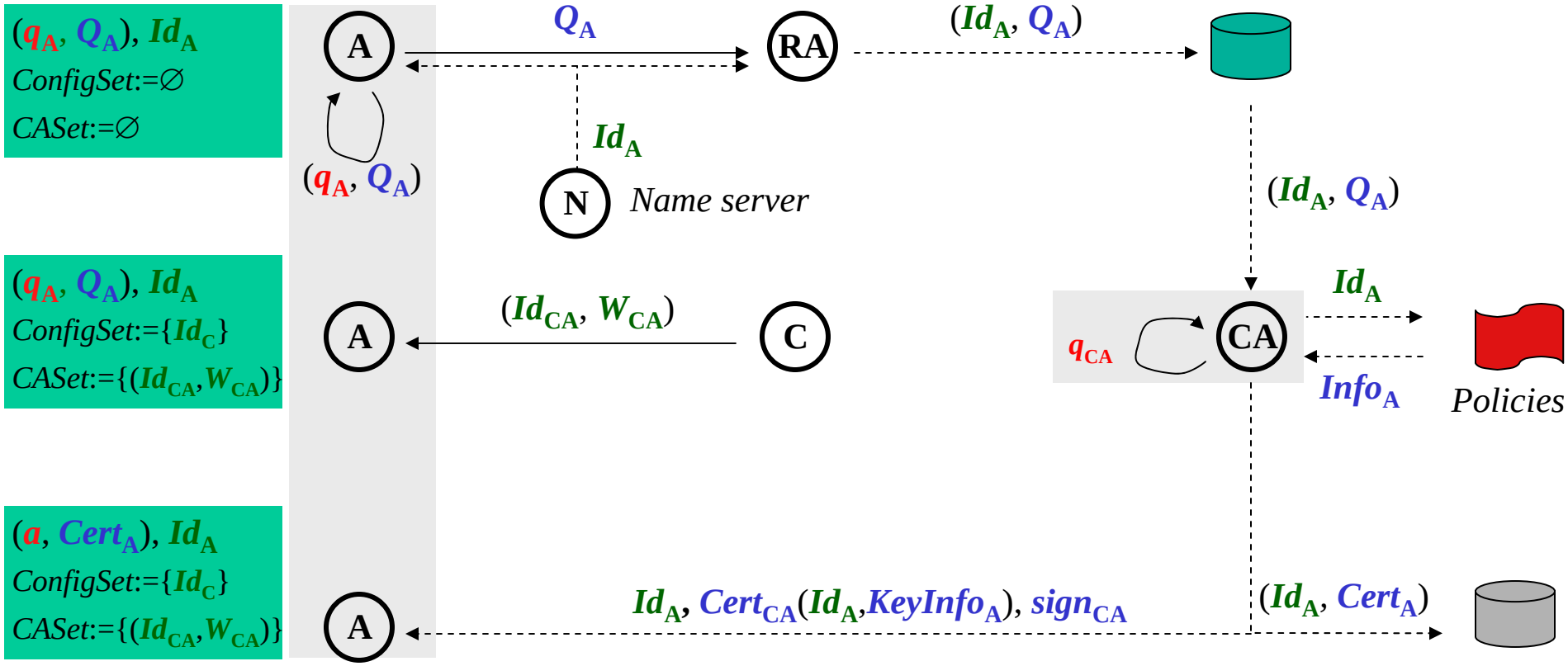
1. How does approach address deployment scenarios – per-scenario comparison
2. Vulnerabilities of devices/subsystems in transit from vendor to user
3. Dependencies on trustworthiness personnel
4. Simplicity
5. Ease of use
6. Flexibility
7. Minimizes dependencies
8. System resources (bandwidth, time, energy consumption, join time)
9. Availability (24/7)
10. Human element
11. Externalities (robustness, do we need special boxes, tools, etc.)
12. Does facilitate over-the-air provisioning
13. Interoperability
14. Implementation cost (incremental cost)
15. Where cost occurred?
16. Ability to put more data on device (as required to bootstrap behavior on different layers)

Evaluation criteria (2)

17. Ability to put date on a device that does not have an 802.15.4 radio (e.g., gateway, backbone router, system manager), so that the same end state can be reached
18. Ability to de-provision device (i.e., bring back to ex-factory state and sell, e.g., on e-bay to someone who can then still securely use it)
19. Number of tools required
20. Ability to move from devices between sites (e.g., smart sea containers) – roaming in/out of different user sites
21. Economies of scale issues

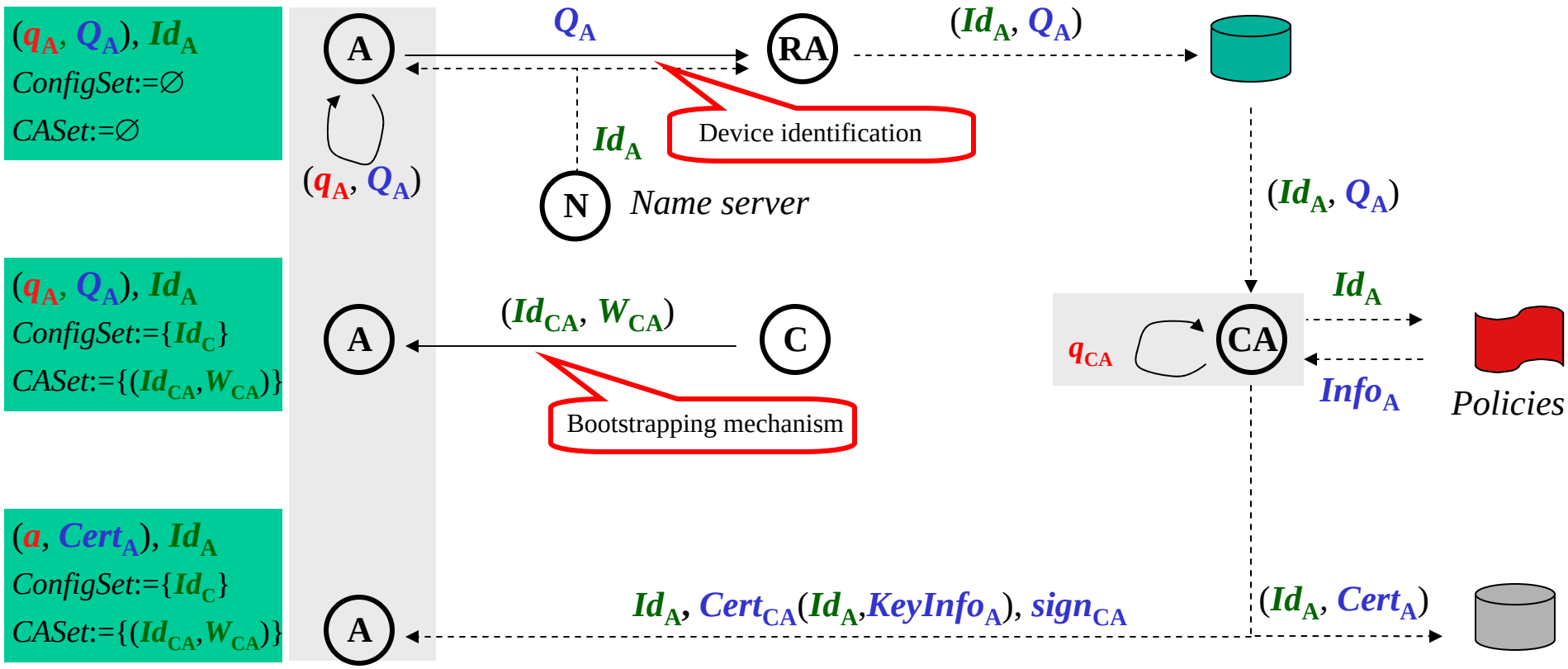
Device Certificates

Certificate Generation (1)



Device roles		Keying information		Device information	
A	Ordinary device	(q_A, Q_A)	ephemeral private/public key A	Id_A	identifier of device A
RA	Registration authority	$(a, Cert_A)$	private key, resp. certificate A	Id_{CA}	identifier of CA
CA	Certificate authority	W_{CA}	public root key CA	Id_C	identifier of C
N	Name server	$sign_{CA}$	signature over certificate info		
C	Configuration manager	$KeyInfo_A$	keying information for device A		

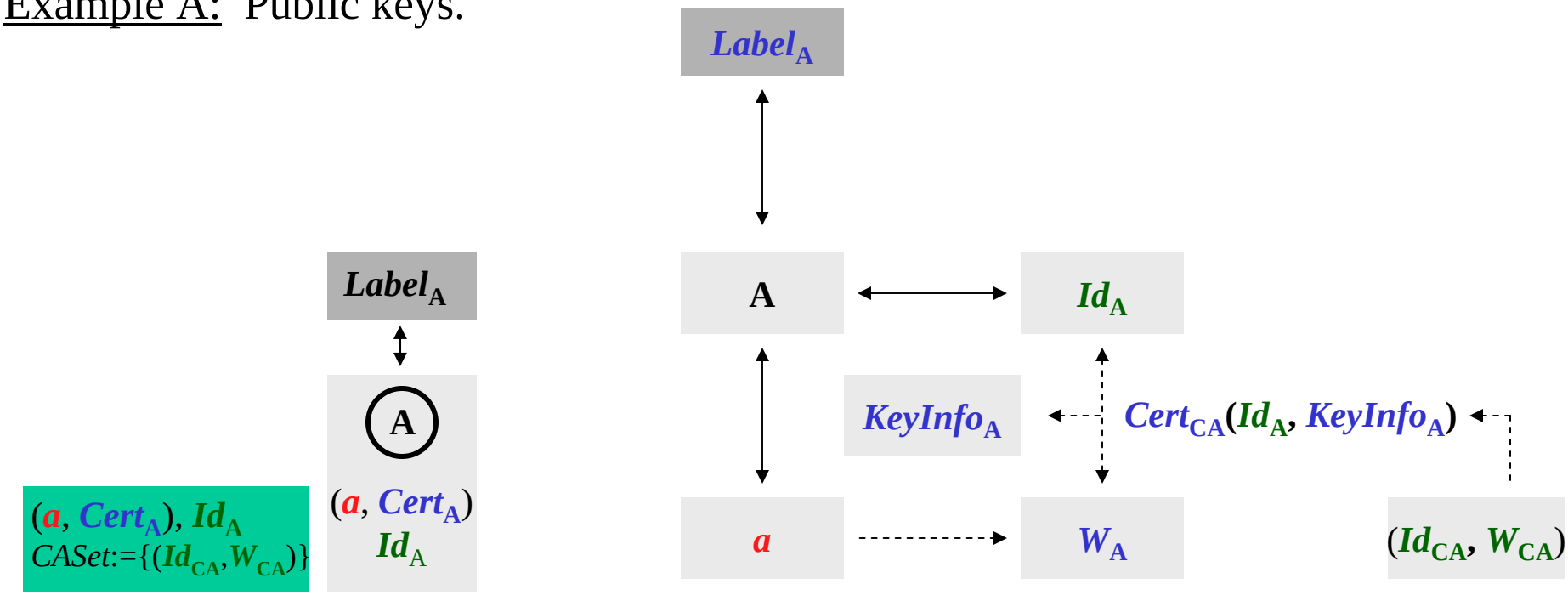
Certificate Generation (2)



Device roles		Keying information		Device information	
A	Ordinary device	(q_A, Q_A)	ephemeral private/public key A	Id_A	identifier of device A
RA	Registration authority	$(a, Cert_A)$	private key, resp. certificate A	Id_{CA}	identifier of CA
CA	Certificate authority	W_{CA}	public root key CA	Id_C	identifier of C
N	Name server	$sign_{CA}$	signature over certificate info		
C	Configuration manager	$KeyInfo_A$	keying information for device A		

Device relationships (1)

Example A: Public keys.



Device roles

A Ordinary device

CA Certificate authority

Type of binding

------- logical link

——— physical link

Keying information

$(a, Cert_A)$ private key, resp. certificate A

W_{CA} public root key CA

$KeyInfo_A$ keying information for device A

Device information

Id_A identifier of device A

Id_{CA} identifier of CA

$Label_A$ label of device A

Networks vs. ad-hoc wireless networks

Underlying network technology (varying details)

Communication technology

- Transmission technology (e.g., frequency band for radio transmissions if wireless)
- Anticipated data rates (including, e.g., breakdown depending on device type)
- Hearing range (i.e., range over which direct communication between static and moving devices may be possible without routing)
- Cost factors (e.g., low power, low cost, low complexity devices)
- Special communication types (e.g., beacon and beacon-less communication)

Devices

- Anticipated application area of devices, networks

Network Characteristics

- Network topology (e.g., star network, mesh networks)
- Communication patterns (e.g., peer-to-peer, multicast, broadcast)
- Devices and their roles and capabilities (e.g., ordinary device, network coordinator)
- *Intra*-network behavior and *inter*-network behavior (roaming)

Interaction with outside world

- Gateway to other networks (e.g, node that communicates MAC service data units back and forth)
- Access to infrastructure (e.g., no online access to external infrastructure (external to network))

NOTE: Presentation relies on concepts only, but assumes distinct network coordinator role

Network security objectives

Access control to the network itself

Restriction of access to scarce network resources to authorized devices only, to ensure objectives including the following:

- proper bandwidth allocation;
- protection of commands (e.g., those regulating network membership);
- power drain savings.

Control of access to message traffic between network devices

Restriction of access to information secured between members of a group of network devices to precisely these group members. This includes any of the following objectives:

- Confidentiality:
  Prevent external parties from learning the content of exchanged messages.
- Data integrity/message authentication:
  Prevent external parties from modifying or injecting messages in undetected way.

- **Other** …

Wireless networking standards

Wireless Local Area Networks (WLAN)
- IEEE 802.11 family (11-55 Mbps and much higher)
- WiFi Alliance

Wireless Personal Area Networks (WPAN)

Medium-rate WPAN
- Bluetooth: 1 Mbps
- Bluetooth Lite

High-Rate WPAN
- IEEE 802.15.3: 11-55 Mbps
- WiMedia Alliance, UWB Forum: up to 450 Mbps (using UWB)

Low-Rate WPAN
- IEEE 802.15.4: 20, 40, 250 kbps
- IEEE 802.15.4a
- ZigBee Alliance

Fixed/mobile broadband access standards (802.16, 802.20), 4G, 3GPP, etc.

Ubiquitous computing standards, DRM, etc.

Applications (sensor and control networks)

- Toys and games
- Consumer electronics
- PC peripherals
- Home automation
- Building automation (HVAC)
- Healthcare
- Factory automation
- Industrial control
- Supply chain management
- Asset tracking & localization
- Homeland security
- Smart dust …

Potential of wireless sensors for industry [US Dept of Energy (Dec 2002)]
- efficiency improvement: 25%; emission reduction: 10%
- significant reduction of ‘wiring cost’; current range: from $50-100 to $2,000 per foot (if hazardous environment)

2001 figure: ‘wiring cost’ of $100B with $11B sensor market [WINA (2003)]

Constraints (1)

Constraints for sensor networks

High throughput is not essential, but rather

- Low energy consumption:
  Lifetime of 1 year with 2 AAA batteries (@750 mAh, 2V) yields 85μA average power consumption, thus forcing 'sleepy' devices (802.15.4 uses 40-60 mW for Tx/Rx)
- Low manufacturing cost:
  Low cost devices force small memory, limited computing capabilities
  (clock frequency: 4-16 Mhz; 10-32 kbytes ROM, 1-4 kbytes RAM, possibly no flash)

Constraints for adhoc networks

- No centralized management:
  No online availability of fixed infrastructure (so, decentralized key management)
- Promiscuous behavior:
  Short-lived communications between devices that may never have met before
  (so, trust establishment and maintenance difficult)
- Unreliability:
  Devices are cheap consumer-style devices, without physical protection
  (so, no trusted platform on device)

Constraints (2)

Security constraints for adhoc networks

- Decentralized key management:
  Due to no online availability fixed infrastructure, but also very ‘sleepy’ nodes
- Flexible configuration and trust management:
  Due to promiscuous, adhoc behavior, but also survivability requirements.
- Low impact of key compromise:
  Due to unavailability of trusted platform (tamper-proofing, etc.)
- Automatic lifecycle management:
  Due to virtual absence of human factor, after initialization

Security constraints for sensor networks

- Implementation efficiency: protocols should use similar cryptographic building blocks
- Parallelism: design protocols have the similar message flows
- Low communication overhead: protocols must avoid message expansion if possible

Constraints (3)

Chip cost considerations

Hardware vs. software cost (in USD)[1]

- Cost metrics of 0.33μ CMOS technology:
  1k gates ≈ 0.5¢
  1 pin ≈ 0.5¢
  RAM = 8 ROM
  1 kbytes ROM ≈ ½ mm^2
  15k gates ≈ 1 mm^2

- Cost *x* kbytes flash memory ≈ $a + b\,x$, where *a* is big constant (4-5 extra processes)

Note: Cost mainly determined by chip area (if mass produced)

- Cost ratios:
  (1 kgates : 1kROM : 1 kRAM) = (1 : 7.5 : 60)
- Impact process technology:
  Change from 0.33μ → 0.18μ CMOS technology yields *area* → 0.3 *area*.

[1]Figures indicative only, courtesy Melexis Telecom (June 2003)

Constraints (4)

Cryptographic building blocks

- Symmetric: all based on fixed block cipher, e.g., AES-128
- Public-key: all based on fixed elliptic curve, e.g., binary Koblitz curve K-163

	Block Cipher (AES)	ECC (K-163)
Software	ROM: 800-2,300 bytes RAM: 60 bytes	ROM: 3-5 Kbytes[1] RAM: 300 bytes
Hardware	≈ 6-7,000 gates	≈ 3,500 gates ROM: 1-2 Kbytes

[1]Figures on ATMel ATMega 128L processor, 16 MHz, 128K RAM

Hardware implementation cost

- AES-128. Cost: 3.5¢ → 1¢ (0.33μ → 0.18μ)
- K-163 curve. Cost: 2¢ → ½ - ¾¢ (0.33μ → 0.18μ) {Note: for K-283: 3¢ → 1¢}

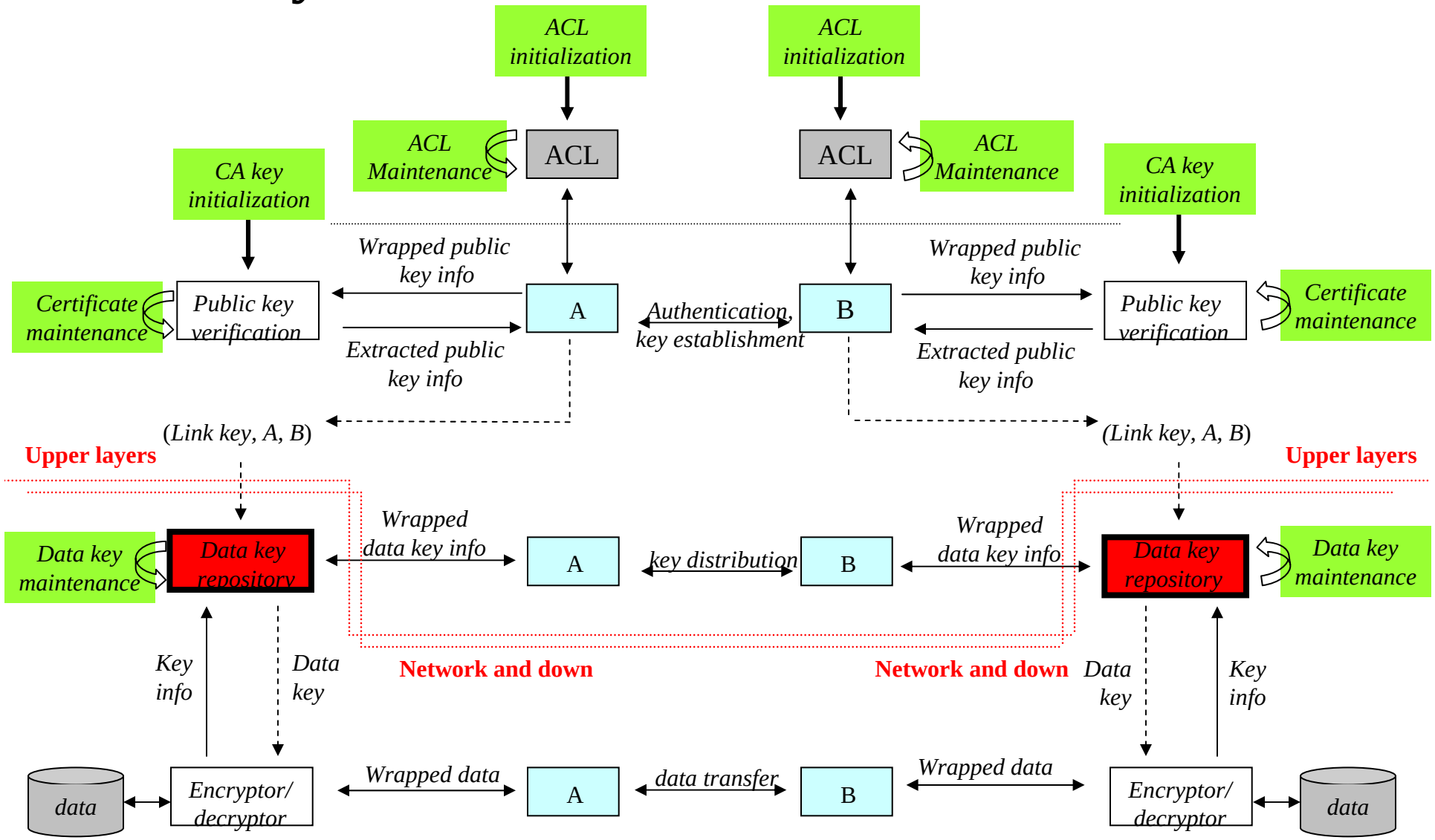
Software implementation cost

- AES-128. Cost: 3 – 8.5¢ → 1 – 3¢ (0.33μ → 0.18μ)
- K-163 curve. Cost: 11 – 19 → 3.5 – 6¢ (0.33μ → 0.18μ)

Hardware: significantly lower power consumption

Security Architectural Framework

Security Architectural Framework: Overview



Security Architectural Elements

Security Architectural Framework: Data transport (1)

Cryptographic services:
data confidentiality, data authentication, non repudiation, replay protection, timeliness.

Problems:
• Cryptographic frame protection generally leads to data expansion, due to data authenticity tag (e.g., up to 16 octets per secured frame).
• Security overhead is substantial (security control info, key identifier, nonce).
• Overhead substantial, esp. if multiple layers of encryption).

Impact:
Energy consumption, bandwidth, time latency.

Observations:
• Do not send information in full if this information can be reconstructed from info in the frame and locally maintained side information
• Take cross layer issues into account (multiple layers of encryption)
• Consider purpose of protection (e.g., infrastructure security, content security)
• Exploit open trust model within device

Frame security dreams (1)

	2	1	4 to 20	1	0, 1, 5, or 9	0-4	n	0, 4, 8, or 16	2
D1	Frame Control	Sequence Number	Addressing fields	Security Control Field	Explicit Key Identifier	Frame Counter	Data Payload (encrypted)	Integrity code (encrypted)	FCS
	MHR			Auxiliary security frame header			Payload field	Integrity code	
	New MHR						MAC payload		MFR

No crypto expansion

	2	1	4 to 20	1	0, 1, 5, or 9	0-4	n	0, 4, 8, or 16	2
D1	Frame Control	Sequence Number	Addressing fields	Security Control Field	Explicit Key Identifier	Frame Counter	Data Payload (encrypted)	Integrity code (encrypted)	FCS
	MHR			Auxiliary security frame header			Payload field	Integrity code	
	New MHR						MAC payload		MFR

No crypto expansion

	1	1	4 to 20	1	0, 1, 5, or 9	0-4	n	0, 4, 8, or 16	2
D1	Frame Control	Sequence Number	Addressing fields	Security Control Field	Explicit Key Identifier	Frame Counter	Data Payload (encrypted)	Integrity code (encrypted)	FCS
	MHR			Auxiliary security frame header			Payload field	Integrity code	
	New MHR						MAC payload		MFR

Reduce MAC header overhead

Reduce Security overhead

	Fields are part of 'a' data only
	Fields are part of 'a' data and 'm' data
	Fields are not included in 'a' or 'm' data

Frame security dreams (2)

Example: with ZigBee, one may have the following overhead across layers:
(ZigBee does not use MAC layer security right now)
NWK layer: 22 octets of security overhead
APL layer: 12 octets of security overhead

Total security overhead: 34 = 22 + 12 octets

(this excludes header overhead across layers!)

With overhead reduction techniques:

– Reduce security and crypto overhead to at most 8 octets in total only
– Reduce header overhead significantly

Potential gain: much more payload data left for application data (≈50% more)
Caveats: This requires augmentation CCM* mode of operation by other construct

Examples

	2	1	4 to 20	1	0, 1, 5, or 9	0-4	n	0, 4, 8, or 16	2
D1	Frame Control	Sequence Number	Addressing fields	Security Control Field	Explicit Key Identifier	Frame Counter	Data Payload (encrypted)	Integrity code (encrypted)	FCS
	MHR			Auxiliary security frame header			Payload field	Integrity code	
	New MHR						MAC payload		MFR

	1	1	~~4 to 20~~	~~1~~	~~0, 1, 5, or 9~~	~~0-4~~	n	~~0, 4, 8, or 16~~	2
D1	Frame Control	Sequence Number	~~Addressing fields~~	Security Control Field	~~Explicit Key Identifier~~	Frame Counter	Data Payload (encrypted)	~~Integrity code (encrypted)~~	~~FCS~~
	MHR			~~Auxiliary security frame header~~			Payload field	~~Integrity code~~	
	New MHR						MAC payload		MFR

Reduce MAC header overhead

Reduce Security overhead

No frame check sequence

MAC payload	small	+CRC	+authenticity
5	7	9	13
6	8	10	14
7	9	11	15
8	10	12	16
9	11	13	17

[1] with typical payloads

	Fields are part of 'a' data only
	Fields are part of 'a' data and 'm' data
	Fields are not included in 'a' or 'm' data

Summary of issues (1)

Data transport (combined encryption and authentication mode)

Use algorithm with parameterize services offered (e.g., decrease penalty of Securing, e.g., small ACKs; distinguish infrastructure security and content security)

Allow reuse of keying material across different layers

Key transport (key wrap)

Provides implicit key authentication and authenticity

Is data expansion really necessary? (Authenticity often provided by data transport)

Use cases: switch key and wrapped key in same storage (“disk encryption mode”)

Entity authentication, public-key key agreement, symmetric-key key agreement

Exploit commonalities in protocol flows, state machines, etc.

Public-key infrastructure vs. symmetric-key infrastructure

Public-key infrastructure often covers “everything under the sun”, but symmetric-key infrastructure is often localized (single trust domain, no CRL, etc.)

Summary of issues (2)

Trust models

Need for distributed trust models, dynamic "device role models", and security invariants

Certificates

- Certificate request with inclusion of "key possession" makes mass production of public keys difficult (e.g., production during chip manufacturing)

Symmetric-key keying material

- Key usage, policy, etc. aspects often ignored

Specialized issues

Current specifications do sometimes thwart efficiency gains:

Example #1: ECDSA signature speed-ups with (R,s) value, rather than (r, s) value (Also allows batch verification, combined verification and computations)

Example #2: Use of block-cipher based unkeyed hash for key derivation currently not allowed

Security and Ease of Use – Concluding remarks

Recall our challenge:

Bridge the gap between state-of-the-art security that is known and security that is actually being used.

Lots of techniques known to address security architectural and trust lifecycle management challenges in *all but most mundane* environments.

Still, hurdles remain:

- support for semi-autonomous lifecycle management (no expensive IT personnel)
- specification of common crypto mechanisms, such as entity authentication, incomplete
- need to take into account constraints of "internet of things"
- need for more involvement crypto/security experts with sensor and control standards

Adhoc networks	**Security constraints**
• No centralized management	• Decentralized key management
• Promiscuous behavior	• Flexible configuration and trust model
• Unreliability	• Low impact key compromise
Sensor networks	• Automatic lifecycle management
• Low energy consumption	• Low communication overhead
• Low manufacturing cost	• Low implementation cost

(Certicom Research)

Contact info

René Struik
Certicom Research

Phone: +1 (905) 501-6083
Email: rstruik@certicom.com

Research interests

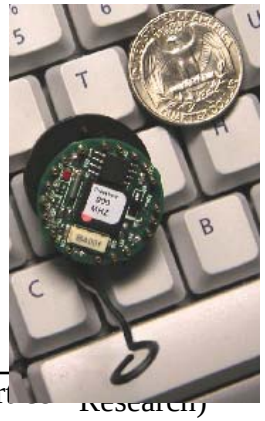
Core crypto

- ECDSA signatures: speed-up verification (single, batch)
- ECDH key agreement: unbalanced and assisted computations
- Low power crypto, others…

Adhoc sensor networks

- Security models and trust management
- Semi-automatic lifecycle management
- Configuration and installation
- Low implementation cost
  - Protocols: re-use building blocks, parallelism flows, etc.
  - Keying material: key identification, key usage, key size

Adhoc networks
- No centralized management
- Promiscuous behavior
- Unreliability

Sensor networks
- Low energy consumption
- Low manufacturing cost

Security constraints
- Decentralized key management
- Flexible configuration and trust model
- Low impact key compromise
- Automatic lifecycle management
- Low communication overhead
- Low implementation cost