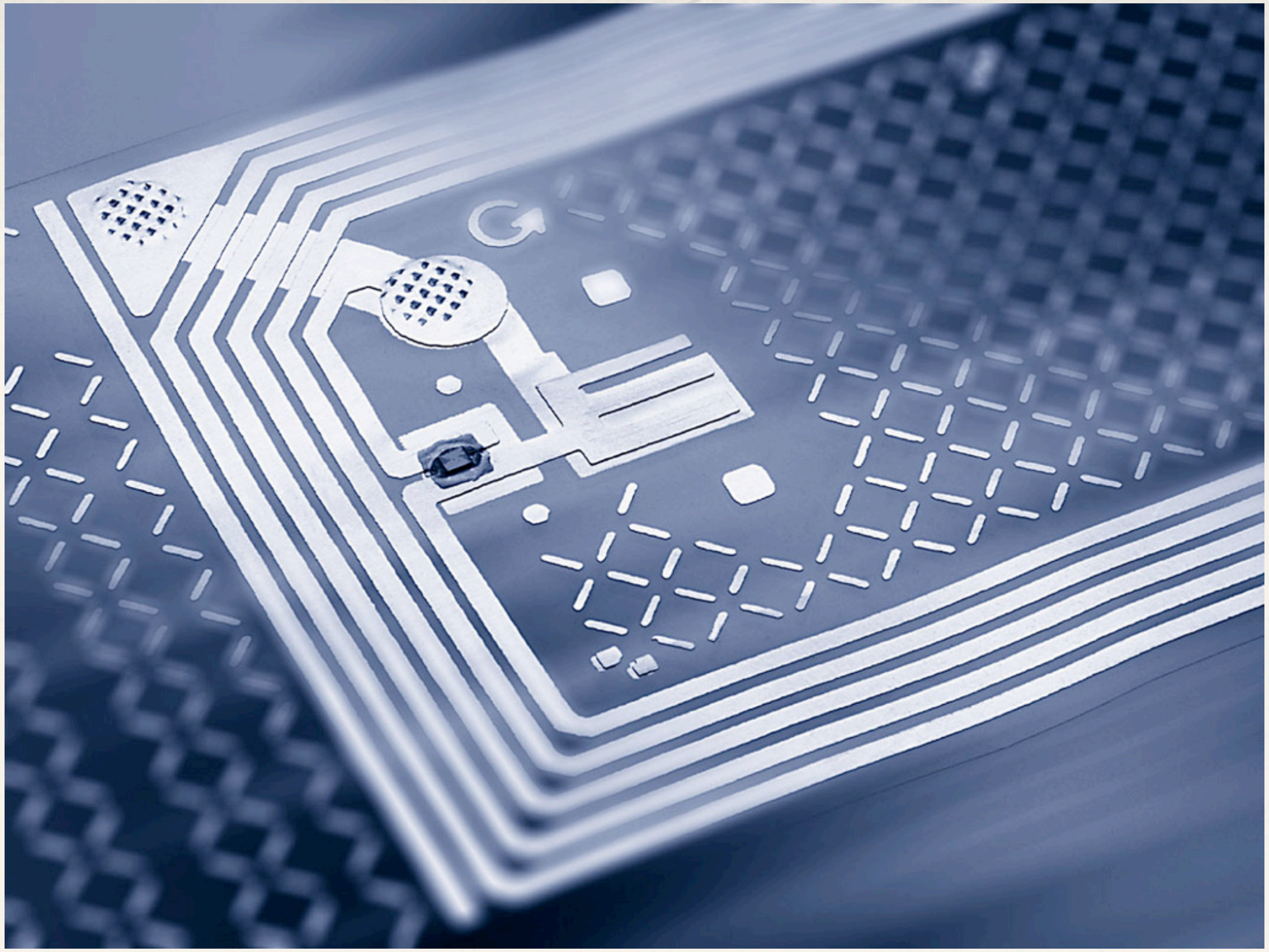


Protection of the Users' Privacy in Ubiquitous RFID-based Systems

Ivan Gudymenko

24.04.2012 *Hauptseminar "Technischer Datenschutz"*

Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work

Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work

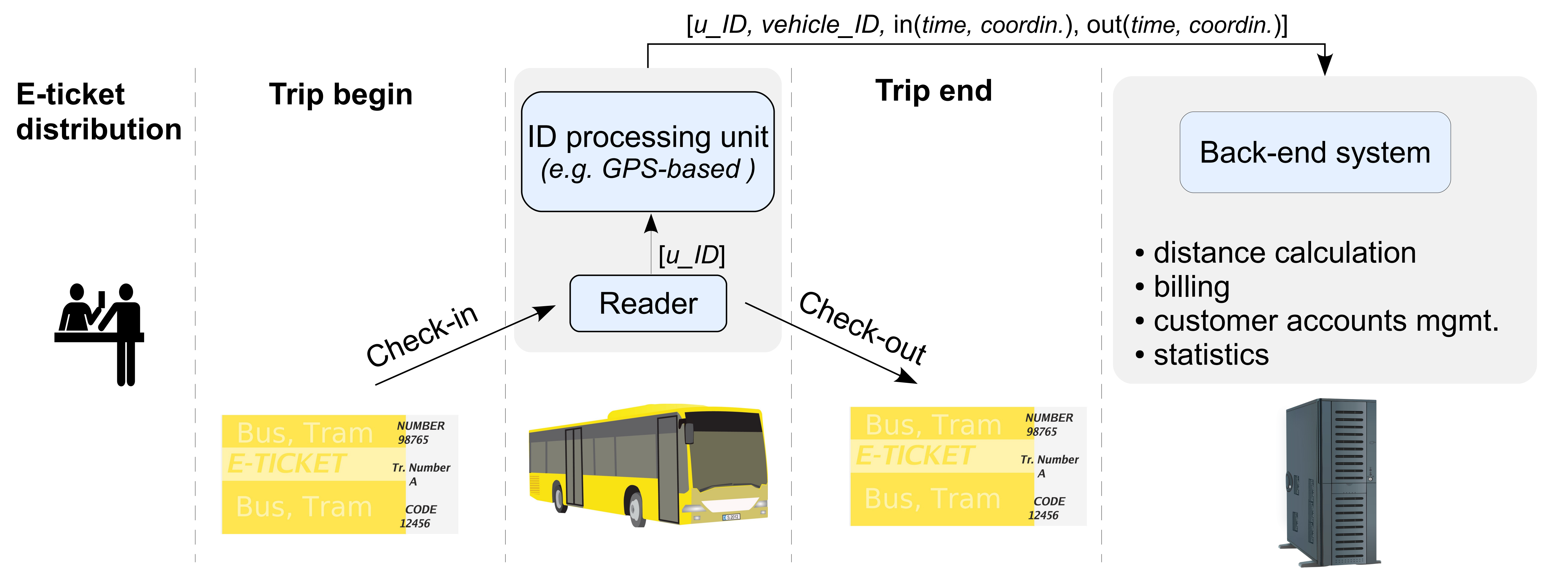
Intro

- UbiComp systems based on RFID
- Privacy issues address serious concerns
- Motivation: making UbiComp privacy-respecting
- Two use cases:
  - E-ticketing
  - Personal Belongings Management

Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work

E-ticketing: A General Scenario



[*u_ID*, *vehicle_ID*, in(*time*, *coordin.*), out(*time*, *coordin.*)]

E-ticket distribution

Trip begin

Trip end

ID processing unit
(e.g. GPS-based)

[*u_ID*]

Reader

Check-in

Check-out

Back-end system

- distance calculation
- billing
- customer accounts mgmt.
- statistics

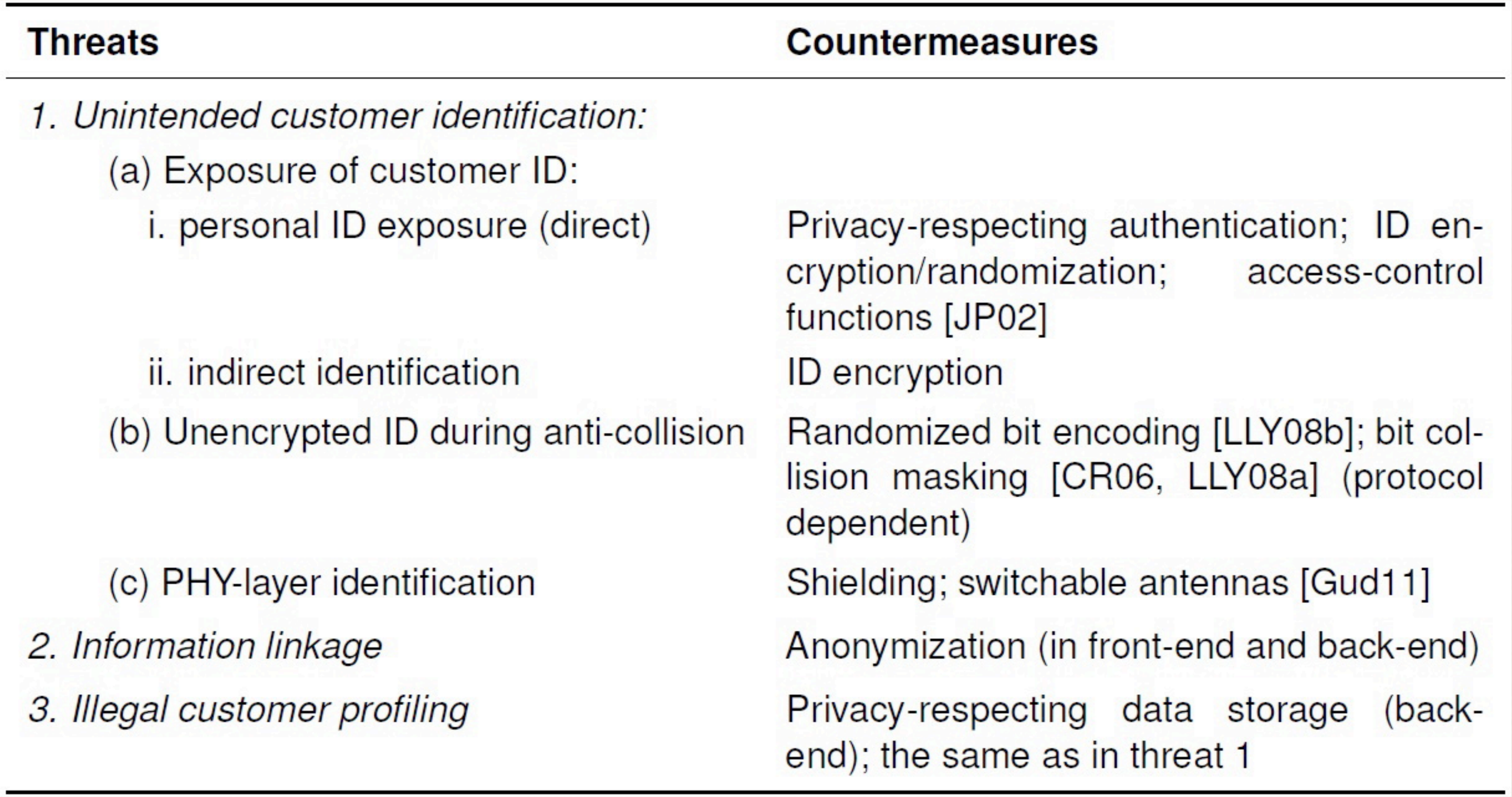
Privacy Concerns in E-ticketing

- Unintended customer identification
  - exposure of customer ID (direct and indirect)
  - unencrypted ID during the anti-collision session
  - physical layer identification (RFID fingerprinting)
- Information linkage
- Illegal customer profiling

Privacy Protection Goals:

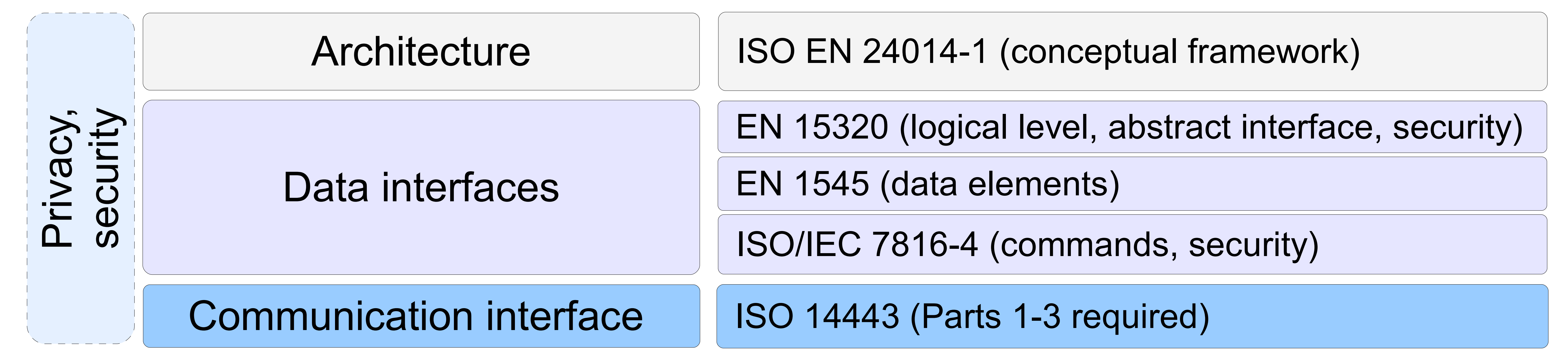
1. Anonymity
2. Confidentiality
3. Unlinkability
4. Unobservability

Privacy Concerns in E-ticketing: Countermeasures



Threats	Countermeasures
1. Unintended customer identification:	
(a) Exposure of customer ID:	
i. personal ID exposure (direct)	Privacy-respecting authentication; ID encryption/randomization; access-control functions [JP02]
ii. indirect identification	ID encryption
(b) Unencrypted ID during anti-collision	Randomized bit encoding [LLY08b]; bit collision masking [CR06, LLY08a] (protocol dependent)
(c) PHY-layer identification	Shielding; switchable antennas [Gud11]
2. Information linkage	Anonymization (in front-end and back-end)
3. Illegal customer profiling	Privacy-respecting data storage (back-end); the same as in threat 1

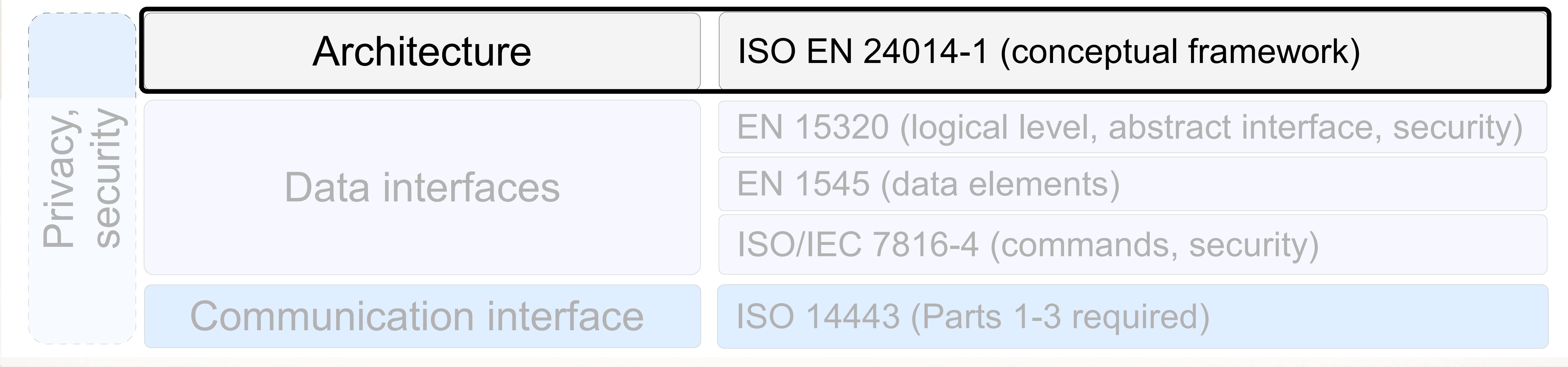
E-ticketing: Standards Stack



Privacy, security	Architecture	ISO EN 24014-1 (conceptual framework)
	Data interfaces	EN 15320 (logical level, abstract interface, security)
		EN 1545 (data elements)
		ISO/IEC 7816-4 (commands, security)
	Communication interface	ISO 14443 (Parts 1-3 required)

- Aimed at providing interoperability
- Many existent solutions are still proprietary, though

Privacy-related Issues: Architecture Level – ISO EN 24014-1



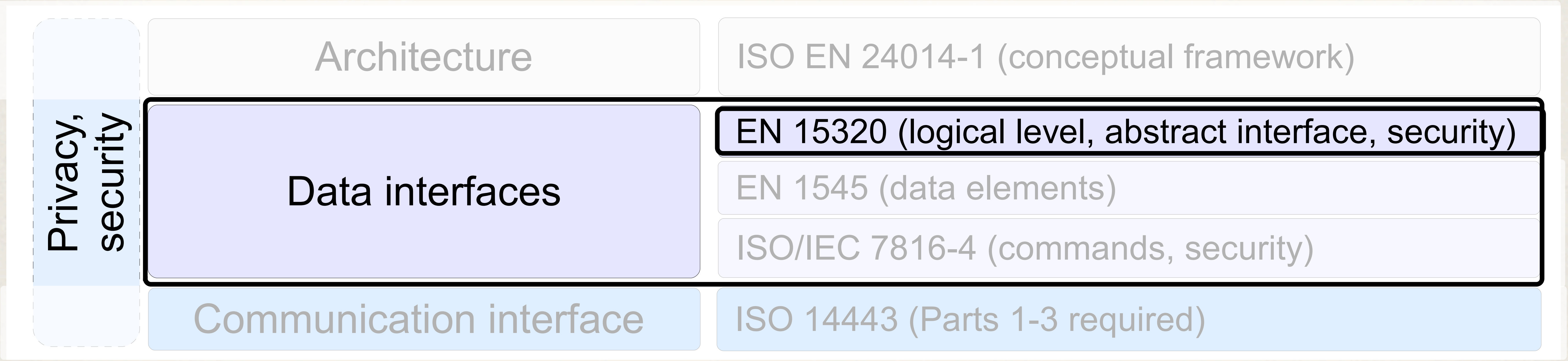
Privacy, security	Architecture	ISO EN 24014-1 (conceptual framework)
	Data interfaces	EN 15320 (logical level, abstract interface, security) EN 1545 (data elements) ISO/IEC 7816-4 (commands, security)
	Communication interface	ISO 14443 (Parts 1-3 required)

- Coarsely-specified, general privacy requirements:
  - data minimization
  - user consent acquisition
  - customer confidentiality
- No recommendations for further implementation

Privacy-related Issues: Data Interfaces Level

Privacy, security	Architecture	ISO EN 24014-1 (conceptual framework)
	Data interfaces	EN 15320 (logical level, abstract interface, security)
		EN 1545 (data elements)
		ISO/IEC 7816-4 (commands, security)
	Communication interface	ISO 14443 (Parts 1-3 required)

Privacy-related Issues: Data Interfaces Level – EN 15320



Privacy, security

Architecture

ISO EN 24014-1 (conceptual framework)

Data interfaces

EN 15320 (logical level, abstract interface, security)

EN 1545 (data elements)

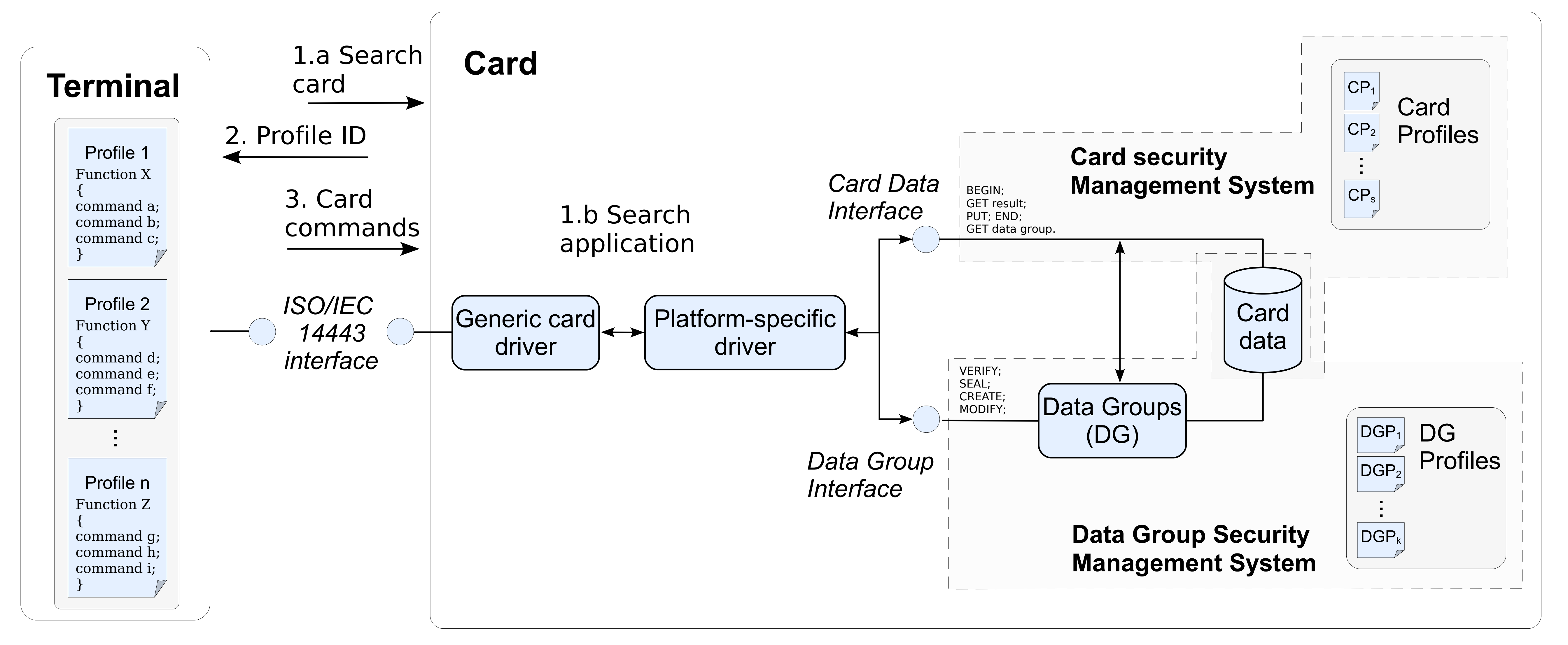
ISO/IEC 7816-4 (commands, security)

Communication interface

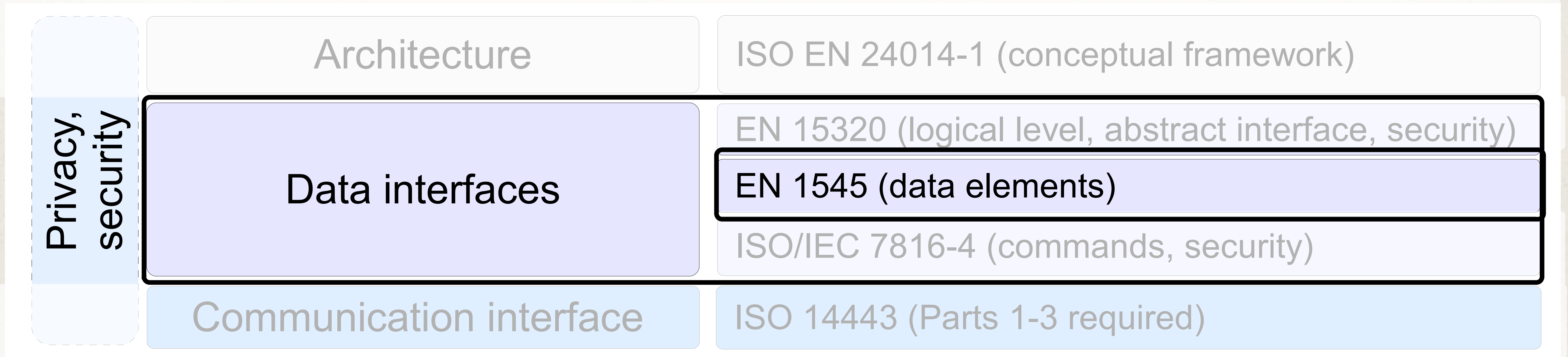
ISO 14443 (Parts 1-3 required)

- Specification of a generic Security Subsystem
- Access control to privacy-relevant fields further defined in EN 1545

Security Subsystem in EN 15320



Privacy-related Issues: Data Interfaces Level – EN 1545



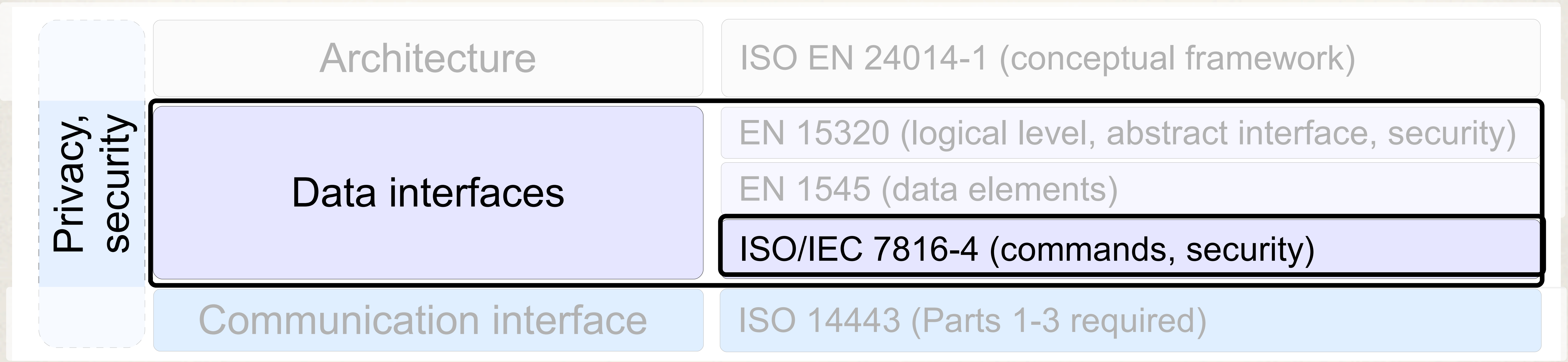
	Architecture	ISO EN 24014-1 (conceptual framework)
Privacy, security	Data interfaces	EN 15320 (logical level, abstract interface, security) EN 1545 (data elements) ISO/IEC 7816-4 (commands, security)
	Communication interface	ISO 14443 (Parts 1-3 required)

- Privacy-relevant data fields (*customer number, birth date, etc.*)
- Access control and encryption for protection

Privacy-relevant Fields in EN 1545-1

Privacy-relevant field	**Description**
birth date	-
birth name	-
birth place	-
customer number	*customer reference number*
device ID	*can be linked to a particular customer*
e-mail address	-
telephone number	-
postal address	-
location ID	-
customer profile ID	*e.g. student, military, resident, etc.*
user data	*additional information about a customer*

Privacy-related Issues: Data Interfaces Level – ISO 7816-4



Privacy, security	Architecture	ISO EN 24014-1 (conceptual framework)
	Data interfaces	EN 15320 (logical level, abstract interface, security)
		EN 1545 (data elements)
		ISO/IEC 7816-4 (commands, security)
	Communication interface	ISO 14443 (Parts 1-3 required)

- Secure messaging mechanisms
- Can be used for protecting privacy-critical data

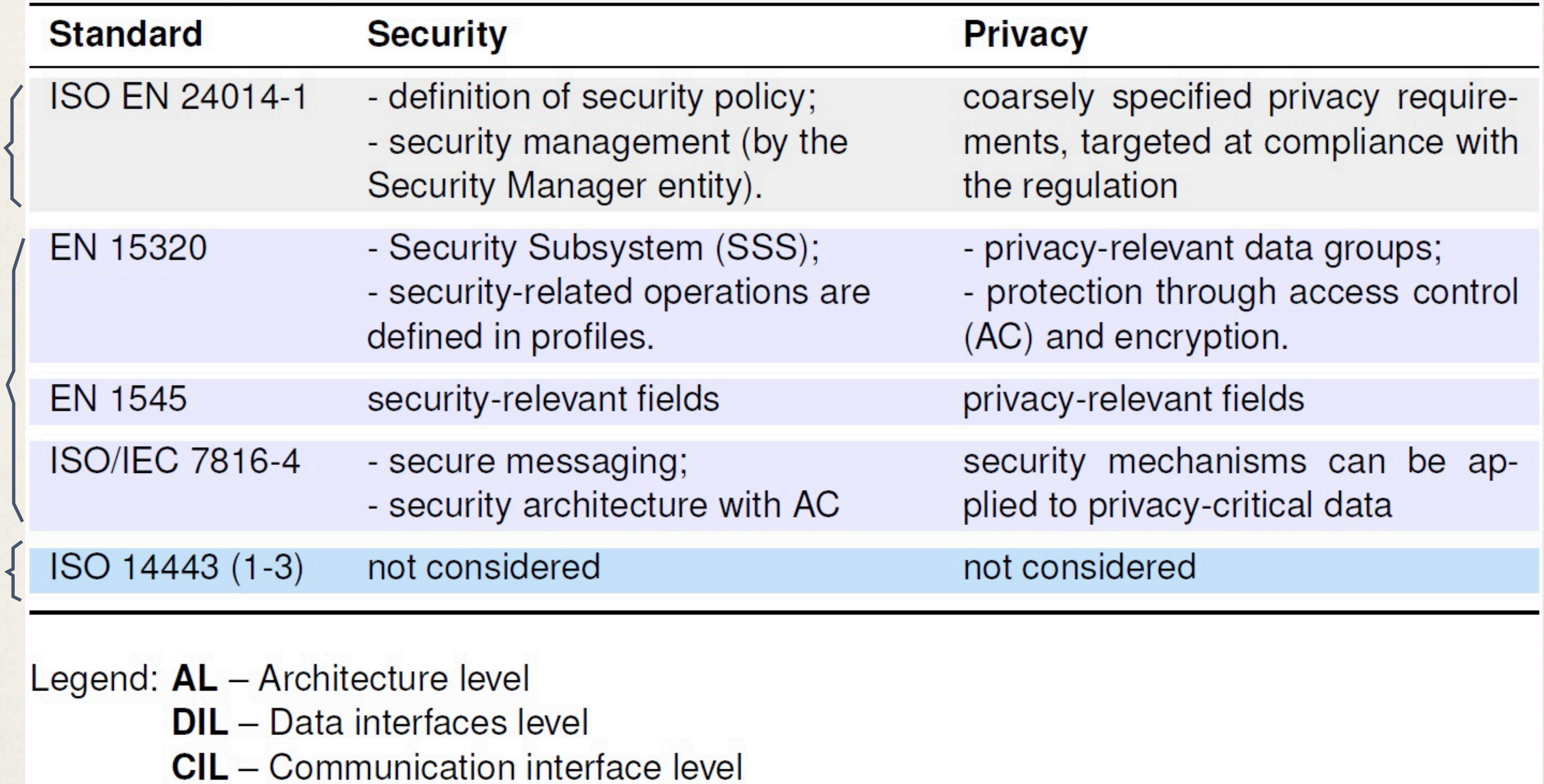
Privacy-related Issues: Communication Interface

Privacy, security	Architecture	ISO EN 24014-1 (conceptual framework)
	Data interfaces	EN 15320 (logical level, abstract interface, security)
		EN 1545 (data elements)
		ISO/IEC 7816-4 (commands, security)
	Communication interface	**ISO 14443 (Parts 1-3 required)**

- Solely functionality-oriented
- No security or privacy mechanisms considered

Customer ID exposure during the anti-collision session and **physical layer identification:** to be solved here

Privacy-related Issues: Summary



	Standard	Security	Privacy
AL	ISO EN 24014-1	- definition of security policy; - security management (by the Security Manager entity).	coarsely specified privacy requirements, targeted at compliance with the regulation
DIL	EN 15320	- Security Subsystem (SSS); - security-related operations are defined in profiles.	- privacy-relevant data groups; - protection through access control (AC) and encryption.
	EN 1545	security-relevant fields	privacy-relevant fields
	ISO/IEC 7816-4	- secure messaging; - security architecture with AC	security mechanisms can be applied to privacy-critical data
CIL	ISO 14443 (1-3)	not considered	not considered

Legend: **AL** – Architecture level
DIL – Data interfaces level
CIL – Communication interface level

Privacy-related Issues: Summary (2)

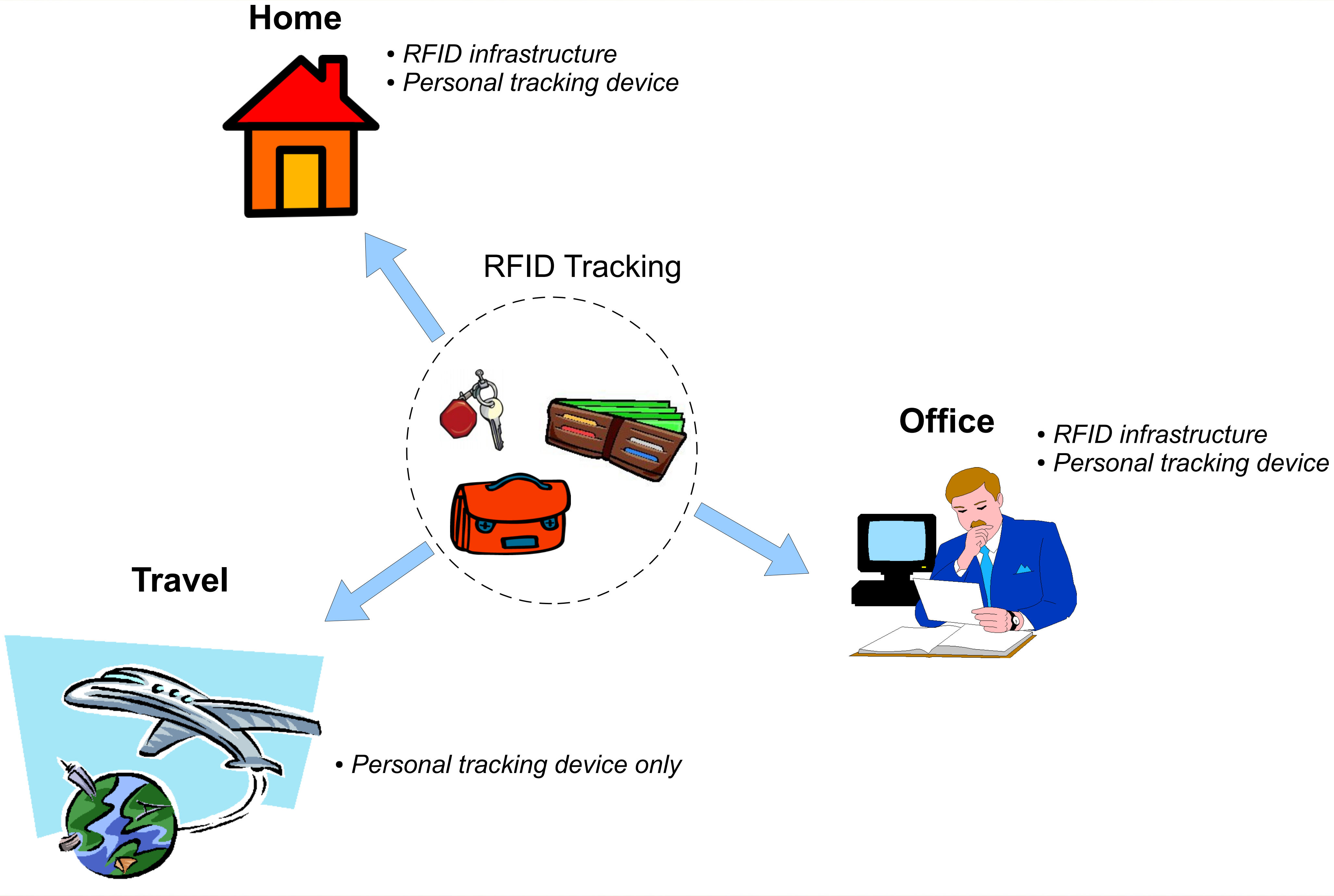
- Security mechanisms are considered in the first place
- Customer privacy more as a by-product
- Privacy issues are not explicitly addressed across the stack
- Proprietary solutions act in a similar way (ITSO, CALYPSO, MIFARE)

➡ *Develop an approach explicitly addressing privacy in a cross-layer fashion and across system components*

Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work

A General Scenario


Home
• *RFID infrastructure*
• *Personal tracking device*
RFID Tracking
Office
• *RFID infrastructure*
• *Personal tracking device*
Travel
• *Personal tracking device only*

Key Differences to E-ticketing

- The requirement to track items from a certain distance
- No validation step is required
- Anonymization is easier
- Only a few readers (e.g. a portable one, at work and at home)
- Compliance to the Standards Stack not required (weaker interoperability?)

➡ *Develop a privacy-respecting solution for personal belongings management*

Outline

- Intro
- E-ticketing
- Personal Belongings Management
- Conclusion and future work

Conclusion

- Two use cases for the PhD dissertation have been discussed
- Focus on user privacy
- No decent cross-layer, cross-component solution with respect to privacy has been developed so far

Future Work

- Further research on partial solutions developed so far
- Identify what can be done for a decent cross-layer, cross-component solution
- Focus on the issues representing a particular interest for a research community and industry

Time Plan: Near Future

May 2012	• Finish State-of-the-Art: - proprietary solutions - focus papers • Privacy-preserving protocol evaluation
June 2012	• Specific tasks determination • Core concept development
July / August 2012	• Requirements paper for doctoral symposium

References

[JP02] Ari Juels and Ravikanth Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In Financial Cryptography '03, pages 103–121. Springer-Verlag, 2002.

[LLY08-a] Tong-Lee Lim, Tieyan Li, and Sze-Ling Yeo. Randomized Bit Encoding for Stronger Backward Channel Protection in RFID Systems. In Proceedings of the 2008 Sixth Annual IEEE International Conference on Pervasive Computing and Communications, PERCOM '08, pages 40–49, Washington, DC, USA, 2008. IEEE Computer Society.

[LLY08-b] Tong-Lee Lim, Tieyan Li, and Sze-Ling Yeo. A Cross-layer Framework for Privacy Enhancement in RFID systems. Pervasive and Mobile Computing, 4(6):889 – 905, 2008.

[Gud11] Ivan Gudymenko. Protection of the Users' Privacy in Ubiquitous RFID Systems. Master's thesis, Technische Universität Dresden, Faculty of Computer Science, December 2011.

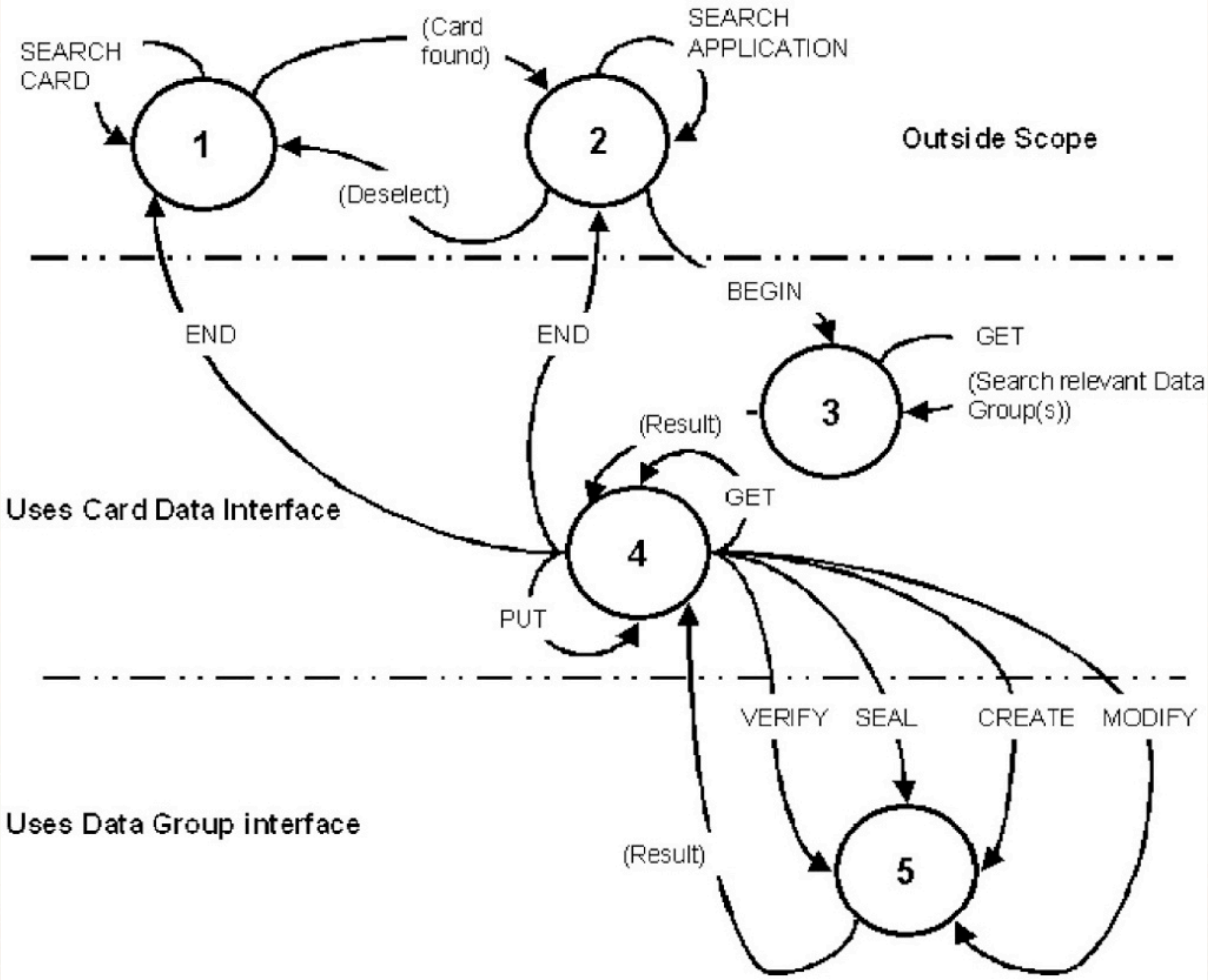
[CR06] Wonjoon Choi and Byeong-hee Roh. Backward Channel Protection Method for RFID Security Schemes Based on Tree-Walking Algorithms. In Marina Gavrilova, Osvaldo Gervasi, Vipin Kumar, C. Tan, David Taniar, Antonio Lagan´ a, Youngsong Mun, and Hyunseung Choo, editors, Computational Science and Its Applications - ICCSA 2006, volume 3983 of Lecture Notes in Computer Science, pages 279–287. Springer Berlin / Heidelberg, 2006.

Thank you very much for your attention!

Questions?
Comments?
Suggestions?

Back-up Slides

Logical Interfaces in EN 15320: States Transitional Diagram


SEARCH CARD
(Card found)
SEARCH APPLICATION
1
2
Outside Scope
(Deselect)
BEGIN
END
END
GET
3
(Search relevant Data Group(s))
(Result)
GET
Uses Card Data Interface
4
PUT
VERIFY
SEAL
CREATE
MODIFY
Uses Data Group interface
(Result)
5