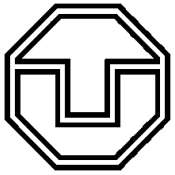
Developing Privacy-respecting E-ticketing Systems

Ivan Gudymenko



TECHNISCHE UNIVERSITÄT DRESDEN

Klausurtagung II/2012

Outline

- E-ticketing Systems Under Concern:
  - E-ticketing: A General Application Scenario
  - Fare Collection Approaches
  - Underlying Technology and Standards
  - Main Use Cases

What to protect

- Security Issues Affecting Privacy
- Specific Privacy Threats
- Dissertation Goals and Their Achievement
- Privacy Preservation
- Challenges

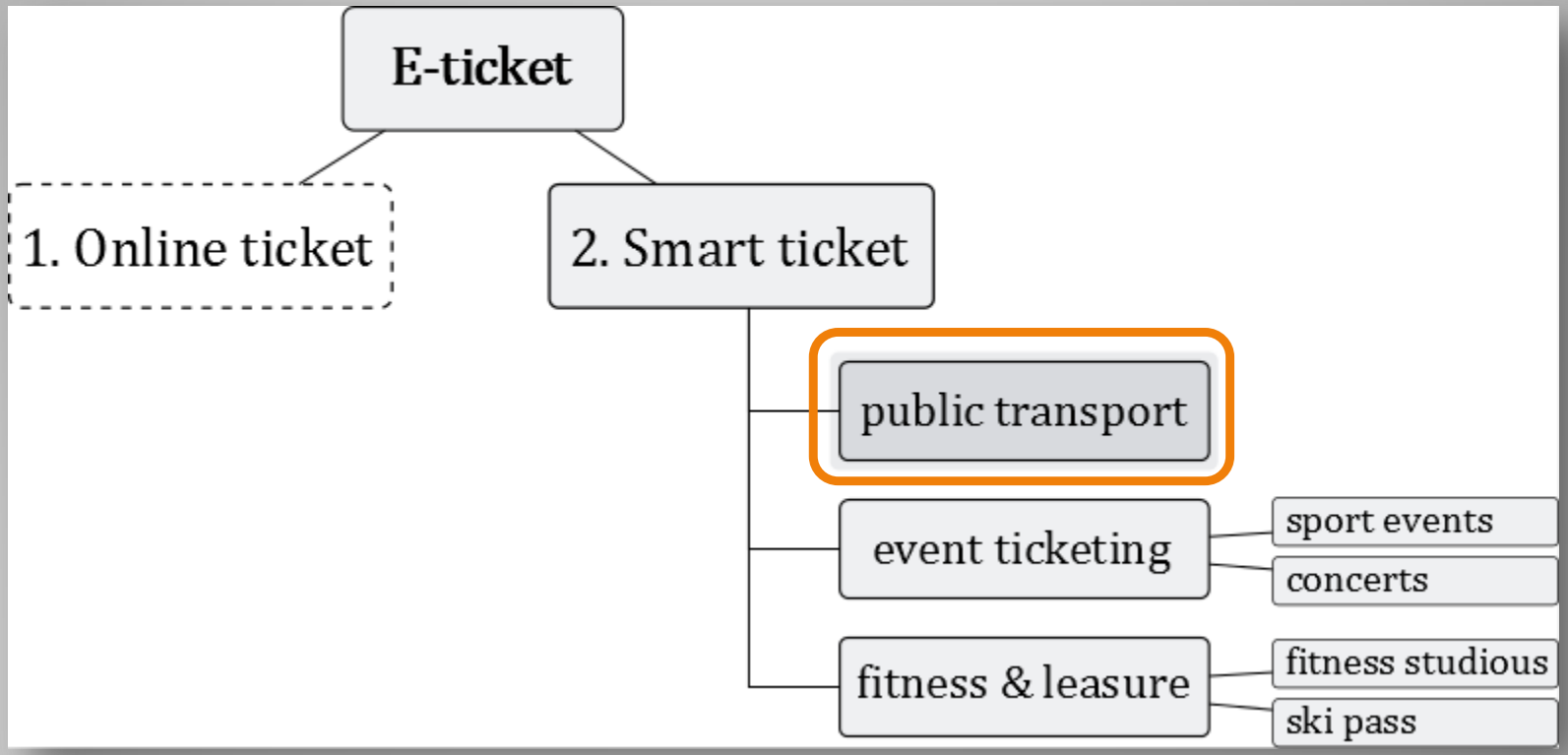
Dis. Focus

What Should Be Protected

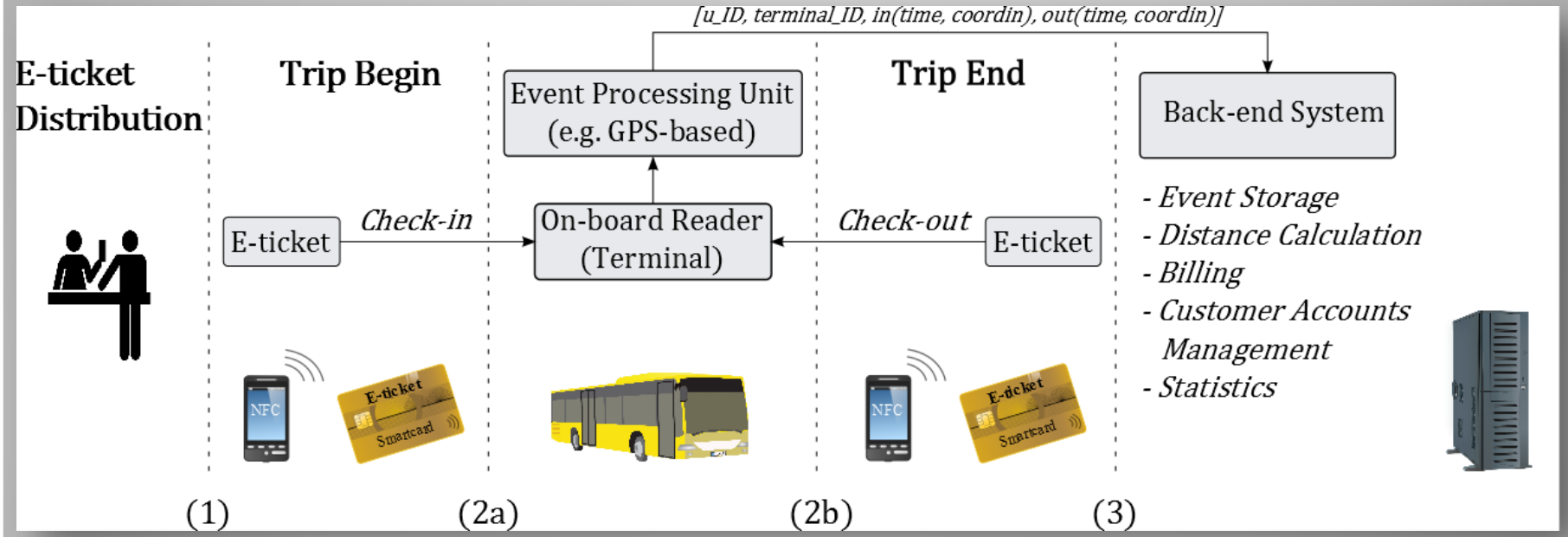
E-ticketing Systems Under Concern

- Part of UbiComp
- Focus on E-ticketing in Public Transport
- E-ticketing Systems [1]:
  - Account-based
  - Card-based
- E-ticket:
  - Online-based
  - "Smart ticket"

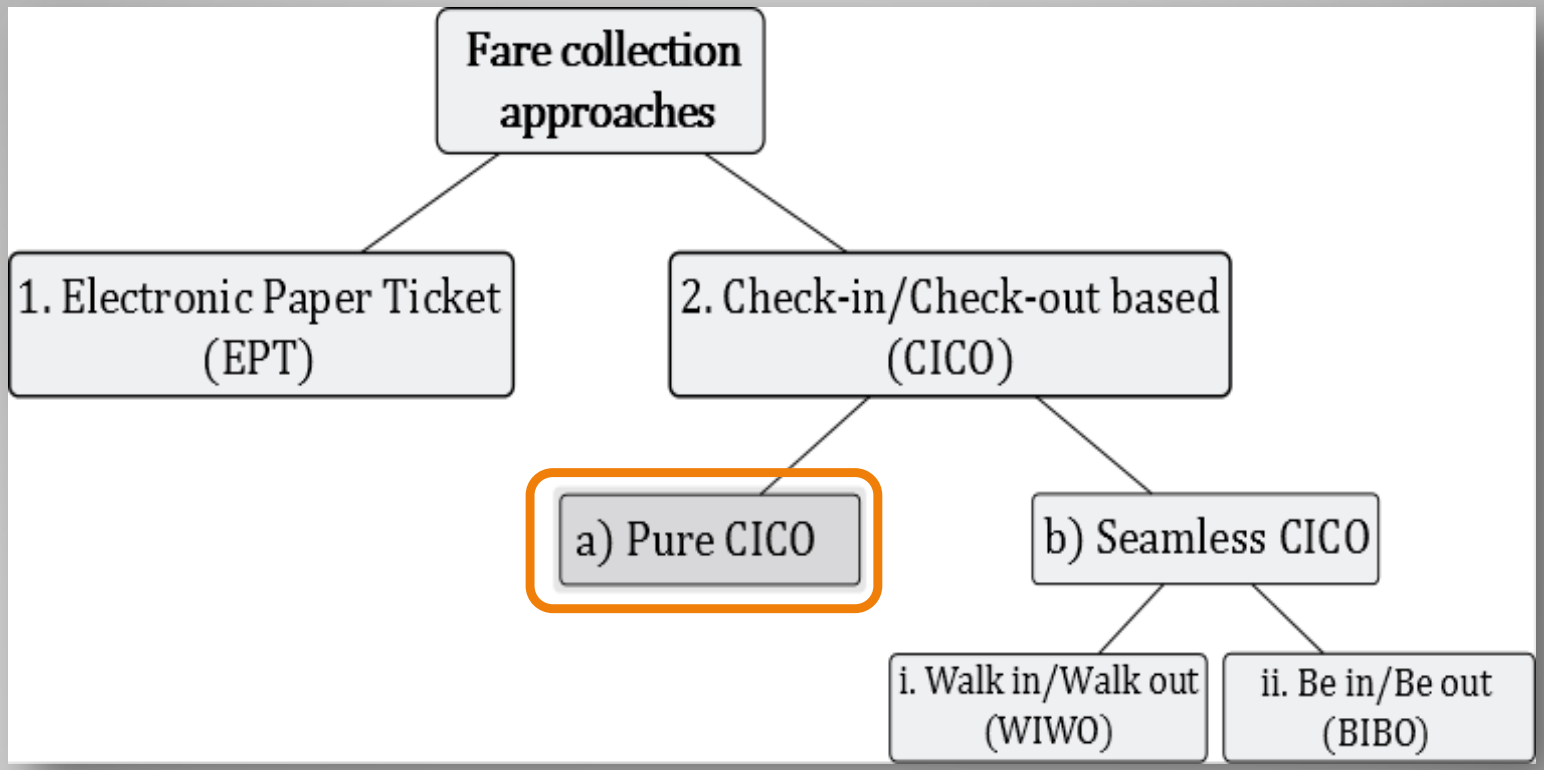
E-ticketing Systems Under Concern (2)



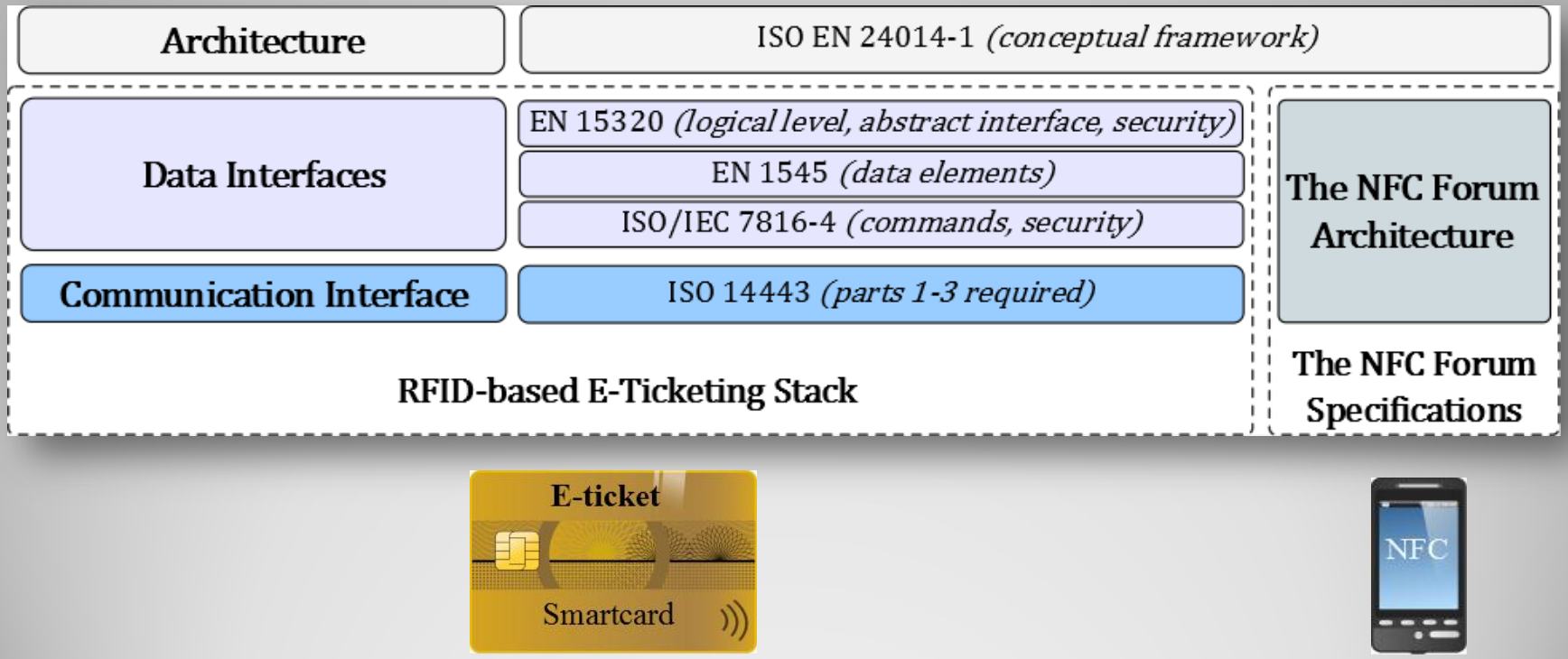
E-ticketing: A General Application Scenario



Fare Collection Approaches



Underlying Technology and Standards



Main Use Cases (Front-end)

- Java Cards
- NFC Smart Phones

Main Use Cases: Java Cards

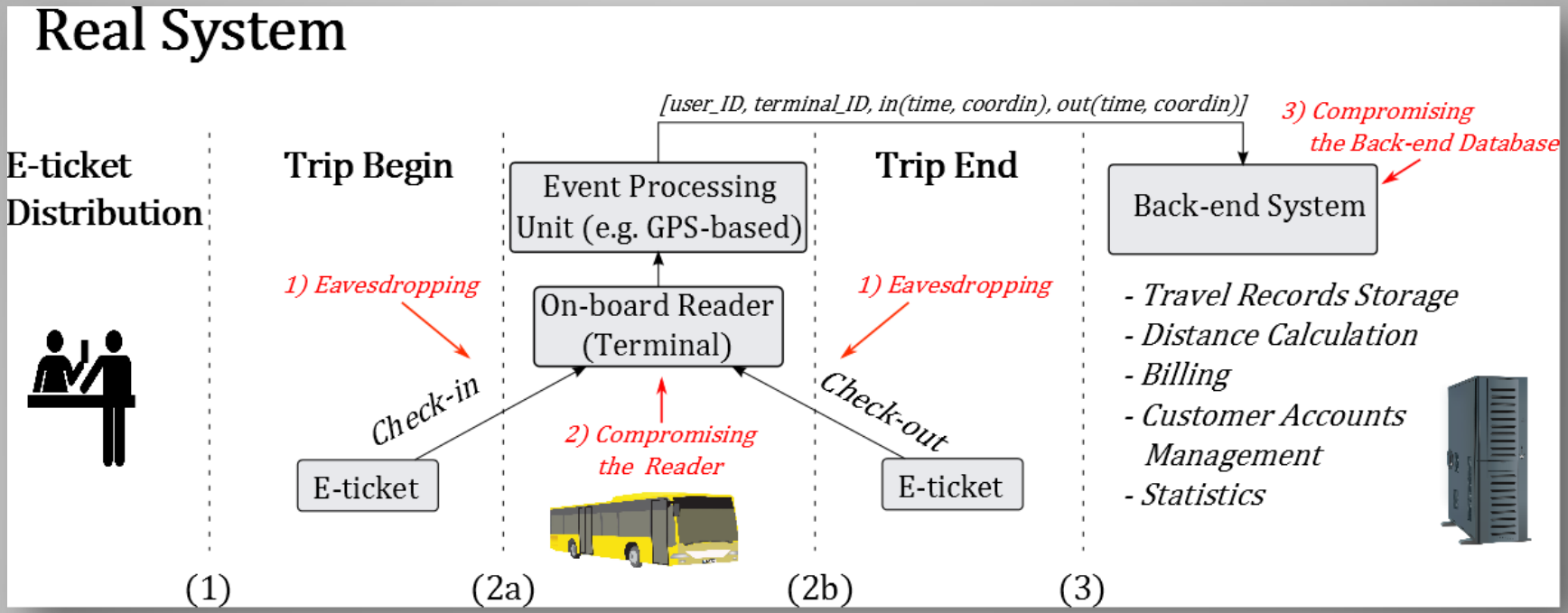
- "Secure by design and tamper-resistant" [2]
- Java Card Platform
  - Response-based communication (C/R-APDUs)
  - Two component JCVM (off-card, on-card)
  - Memory: ROM, RAM, EEPROM
  - Constrained resources
    - reused exception objects
    - optional Garbage Collection, *etc.*

Main Use Cases: NFC Smart Phones

- An extremely promising concept
- *P2P* and *Card Emulation* modes for e-ticketing
- Trusted execution environment provided by the SE (*e.g.* a SIM card)
- SE ←→ NFC front-end: via SWP or S^2P
- No need for phone battery (card emulation, SWP)
- Secure updates through OTA possible (flexibility)

Further Focus: User Privacy

Security Issues Affecting Privacy



Specific Privacy Threats

Threats	Countermeasures
1. Unintended customer identification:	
a) *Exposure of the customer ID:*	
i. Personal ID exposure (direct)	Privacy-respecting authentication; ID encryption/randomization; access-control functions [6]
ii. Indirect identification	ID encryption
b) *Unencrypted ID during anti-collision*	Randomized bit encoding [7]; bit collision masking [8, 9] (protocol dependent)
c) *PHY-layer identification*	Shielding; switchable antennas [10]
2. Information linkage	Anonymization (in front-end and back-end): threat 1 countermeasures; privacy-respecting data processing
3. Illegal customer profiling	Privacy-respecting data storage (back-end); the same as in threat 1

Main Goal of the Dissertation

- Targeting the user privacy from the outset
- In a holistic way across the system components ↔
- A cross-layer approach is desirable ↕

Goal Achievement

- Clearly define the system architecture
  - Online/Off-line e-ticket authentication, *etc.*
- Assign trust levels to the system components
  - Honest, semi-honest, malicious **Oct-Nov ’12**
- State-of-the-art (against the defined architecture) **Nov-Jan ’12/13**
- Concept development **Feb-June ’13**
- Validation **July-Oct ’13**

Concept Validation

- Theoretical Evaluation
- Experiments (labor set up, equipment)
- Student assignments
  - Lightweight crypto (Hauptseminar Techn. Datensch., finished)
  - Kryptografische Methoden auf einer Javacard (Praktikum, finished)
  - Abgesicherte Kommunikation von Android-basierten Smartphones mit Hilfe der NFC-Schittstelle (KP, planned for WS 2012)
  - Nicht-triviale Kryptoverfahren auf einer Java-Karte (KP, planned for WS 2012)
  - Joint E-ticket Application for JCP and NFC (Master Thesis, WS ’12)
  - …

Privacy Preservation

- Privacy/performance trade-off
  - Full privacy preservation
    - Blind Bill Computation (*e.g.* our paper [3])
    - "Optimistic payment" [4]
  - Partial privacy preservation
    - One of the system components is fully trusted (typically, the back-end)
    - Based on the protocol of [5], for example
    - Secure Computations in the back-end

Full Privacy Preservation: Blind Bill Computation [3]

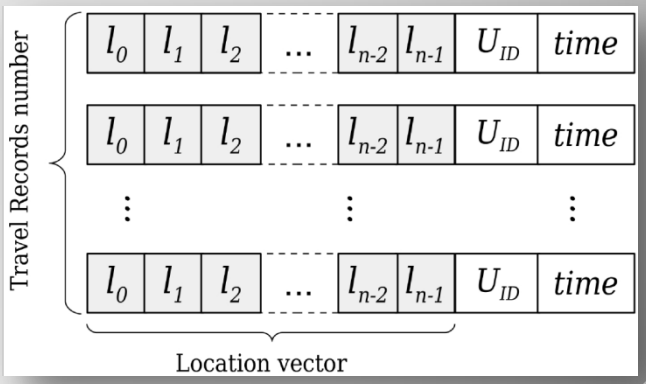
- Flexibility for a customer
- Requires bill processing in the back-end
- Based on partial homomorph. encr. (Paillier)
- Special bit encoding scheme

0	1
$E(r)$	$E(0)$

- Allows logical operations on ciphertexts: Λ, ==
- Additionally, Negation Service required: ¬
  - Full functional basis in the end (Λ, ¬)

Full Privacy Preservation (2)

- Two parts:
  - E-ticket authentication on Entry/Exit
    - ZKP of ID possession due to Schnorr
    - Database look up
    - Additional k-anonymous ID for search speed up
  - Bill Computation in the back-end
    - Travel Records creation
    - Travel Records Processing
      - Using the homomorph. properties and encryption scheme



Challenges (Blind Bill Comp.)

- Efficiency
  - Back-end
  - Front-end (proprietary encryption)
  - Processing cost can be prohibitive…
- Necessity to have a TTP for key mgmnt.

General Challenges

- Non-trivial Crypto on Java Card:
  - Running arithmetic ops at the app. layer is a significant performance limiting factor
  - The necessity to tunnel computations the cryptographic co-processor
- Securing the NFC communication interface
- Back-end efficiency
  - During the look up for blind bill computation
  - General look up

Plan For The Near Future

- Focus on the specified systems
- Define and stick to a certain system architecture (mobile/fixed terminals, *etc.*)
- Devise a privacy-preserving concept
- A paper for a doctoral symposium
  - Concept discussion

Thank You Very Much For Your Attention!

Questions? Comments? Suggestions?

References

[1] Khan *et al.* A Secure and Flexible Electronic-Ticket System. Computer Software and Applications Conference, Annual International, 1:421-426, 2009.

[2] C. Enrique Ortiz. An Introduction to Java Card Technology - Part 1. Oracle. 2003

[3] Florian Kerschbaum, Lim Hoon Wei, Ivan Gudymenko. Privacy-Preserving e-Ticketing for Transport Systems. Submitted to ACSAC-2012, Orlando, Florida, USA.

[4] Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, Christophe Geuens. PrETP: Privacy-Preserving Electronic Toll Pricing. 19th USENIX Security Symposium, 2010.

[5] B. Song and C.J. Mitchell. Scalable RFID security protocols supporting tag ownership transfer. Computer Communications, 34(4):556–566, Apr 2011.

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

[7] 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, '08, pages 40-49, Washington, DC, USA, 2008. IEEE Computer Society.

[8] 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 Laganá, 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.

[9] 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.

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