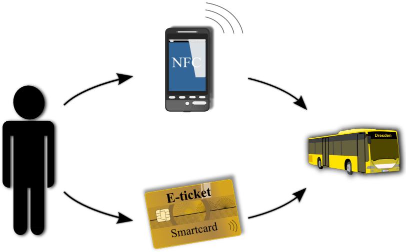
A Privacy-Preserving E-Ticketing System for Public Transportation Supporting Fine-Granular Billing and Local Validation

Ivan Gudymenko
ivan.gudymenko@mailbox.tu-dresden.de
`http://wwwpub.zih.tu-dresden.de/~igudym/`

Chair of Privacy and Data Security
Faculty of Computer Science, TU Dresden

11th of September, 2014



OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution

OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution

E-TICKETING IN PUBLIC TRANSPORT

[Courtesy of MünstercheZeitung.de]

WHAT AN E-TICKET IS

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an "e-ticket" at a user device:
  - Smart Card
  - NFC-enabled smart phone

WHAT AN E-TICKET IS

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
    - Smart Card
    - NFC-enabled smart phone

WHAT AN E-TICKET IS

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
  - Smart Card
  - NFC-enabled smart phone

WHAT AN E-TICKET IS

- A digitalized version of a travel permission (or a proof thereof)
- Stored as an "e-ticket" at a user device:
  - Smart Card
  - NFC-enabled smart phone

WHAT AN E-TICKET IS

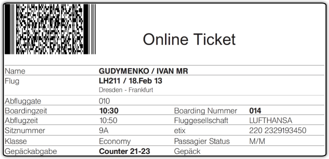
- A digitalized version of a travel permission (or a proof thereof)
- Stored as an “e-ticket” at a user device:
  - Smart Card
  - NFC-enabled smart phone

WHAT AN E-TICKET IS NOT

- A widely used "online ticket" (air transport, etc.)
- Pointing to the respective entry in the back-end DB

WHAT AN E-TICKET IS NOT

- A widely used “online ticket” (air transport, etc.)
- Pointing to the respective entry in the back-end DB

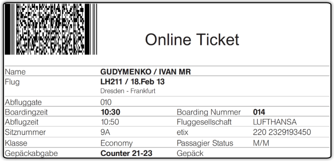


Online Ticket

Name	**GUDYMENKO / IVAN MR**		
Flug	**LH211 / 18.Feb 13** Dresden - Frankfurt		
Abfluggate	010		
Boardingzeit	**10:30**	Boarding Nummer	**014**
Abflugzeit	10:50	Fluggesellschaft	LUFTHANSA
Sitznummer	9A	etix	220 2329193450
Klasse	Economy	Passagier Status	M/M
Gepäckabgabe	**Counter 21-23**	Gepäck	

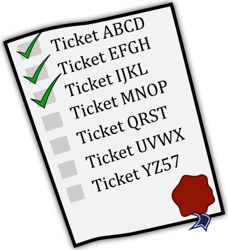
WHAT AN E-TICKET IS NOT

- A widely used “online ticket” (air transport, etc.)
- Pointing to the respective entry in the back-end DB



Online Ticket

Name	**GUDYMENKO / IVAN MR**		
Flug	**LH211 / 18.Feb 13** Dresden - Frankfurt		
Abfluggate	010		
Boardingzeit	**10:30**	Boarding Nummer	**014**
Abflugzeit	10:50	Fluggesellschaft	LUFTHANSA
Sitznummer	9A	etix	220 2329193450
Klasse	Economy	Passagier Status	M/M
Gepäckabgabe	**Counter 21-23**	Gepäck	



NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive

- Interaction-based
  - enable fine-granular billing.

NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive


TECHNISCHE UNIVERSITÄT DRESDEN

Studentenausweis
Student Identity Card

gültig vom 01.04.2011 bis 30.09.2011

Mustermann, Max

geb. am 17.07.1777 Matrikel-Nr. 08154711

TUD

Nur gültig in Verbindung mit Pass oder Personalausweis

- Interaction-based
  - enable fine-granular billing.

NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive

- Interaction-based
  - enable fine-granular billing.

NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive

Studentenausweis
Student Identity Card
gültig vom 01.04.2011 bis 30.09.2011
Mustermann, Max
geb. am 17.07.1777 Matrikel-Nr. 08154711
Nur gültig in Verbindung mit Pass oder Personalausweis

- Interaction-based
  - enable fine-granular billing.

NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive


TECHNISCHE UNIVERSITÄT DRESDEN
Studentenausweis
Student Identity Card
gültig vom 01.04.2011 bis 30.09.2011
Mustermann, Max
geb. am 17.07.1777 Matrikel-Nr. 08154711
TUD
Nur gültig in Verbindung mit Pass oder Personalausweis

- Interaction-based
  - enable fine-granular billing.

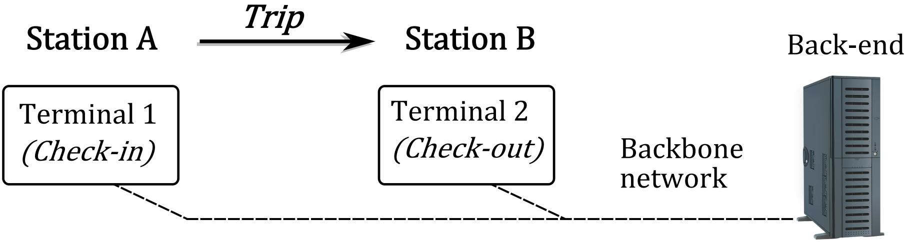
NON-INTERACTIVE VS. INTERACTION-BASED

- Non-interactive


TECHNISCHE UNIVERSITÄT DRESDEN
Studentenausweis
Student Identity Card
gültig vom 01.04.2011 bis 30.09.2011
Mustermann, Max
geb. am 17.07.1777 Matrikel-Nr. 08154711
TUD
Nur gültig in Verbindung mit Pass oder Personalausweis

- Interaction-based
  - enable fine-granular billing.

E-TICKETING: A GENERAL APPLICATION SCENARIO



Trip

Station A

Station B

Back-end

Terminal 1
(Check-in)

Terminal 2
(Check-out)

Backbone network

OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution

CONVENTIONAL E-TICKETING SYSTEMS: PRIVACY

- Primary focus on functionality (and security)
- Privacy is often not directly considered

CONVENTIONAL E-TICKETING SYSTEMS: PRIVACY

- Primary focus on functionality (and security)
- Privacy is often not directly considered

CONVENTIONAL E-TICKETING SYSTEMS: PRIVACY

- Primary focus on functionality (and security)
- Privacy is often not directly considered

PRIVACY CONSIDERATIONS

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification

PRIVACY CONSIDERATIONS

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification

PRIVACY CONSIDERATIONS

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification

PRIVACY CONSIDERATIONS

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification

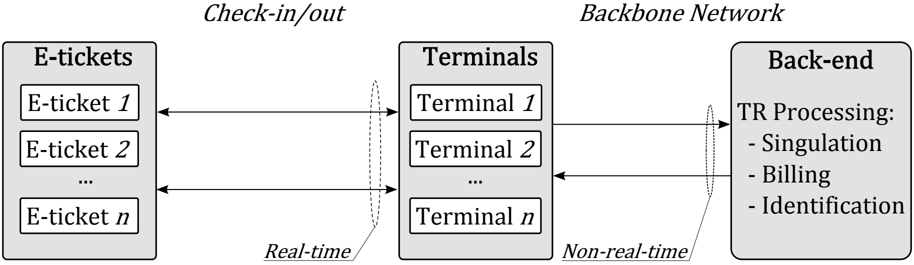
PRIVACY CONSIDERATIONS

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification

PRIVACY CONSIDERATIONS

- Traceability
- Transactions linkability
- Customer profiling
- Ubiquitous identification

A GENERAL SYSTEM ARCHITECTURE



A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

(1) **Privacy**

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

(1) **Privacy**

(a) **Against terminals**

Identification:	*no*
Correlation:	*no*

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

(1) **Privacy**

(a) **Against terminals**	Identification:	*no*
	Correlation:	*no*
(b) **Against back-end**	Identification:	*no*
	Correlation:	*yes*

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

(1) **Privacy**

(a) **Against terminals**	Identification:	*no*
	Correlation:	*no*
(b) **Against back-end**	Identification:	*no*
	Correlation:	*yes*
(c) **Against observers**	PII Derivation:	*no*

A Privacy-preserving E-ticketing System: Core Requirements

(1) **Privacy**

(a) **Against terminals**	Identification:	*no*
	Correlation:	*no*
(b) **Against back-end**	Identification:	*no*
	Correlation:	*yes*
(c) **Against observers**	PII Derivation:	*no*

(2) **Fine-granular billing support**

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

(1) **Privacy**

(a) **Against terminals**	Identification: Correlation:	*no* *no*
(b) **Against back-end**	Identification: Correlation:	*no* *yes*
(c) **Against observers**	PII Derivation:	*no*

(2) **Fine-granular billing support**

(3) **Loose-coupling**

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

(1) **Privacy**

(a) **Against terminals**	Identification: Correlation:	*no* *no*
(b) **Against back-end**	Identification: Correlation:	*no* *yes*
(c) **Against observers**	PII Derivation:	*no*

(2) **Fine-granular billing support**

(3) **Loose-coupling**

(4) **Efficiency** Check-in/out events handling

A PRIVACY-PRESERVING E-TICKETING SYSTEM: CORE REQUIREMENTS

Requirement	Property	Value
(1) **Privacy**		
(a) **Against terminals**	Identification: Correlation:	*no* *no*
(b) **Against back-end**	Identification: Correlation:	*no* *yes*
(c) **Against observers**	PII Derivation:	*no*
(2) **Fine-granular billing support**		
(3) **Loose-coupling**		
(4) **Efficiency**	Check-in/out events handling	
(5) **Multilateral security**		

CORE SYSTEM REQUIREMENTS: INHERENT CONTRADICTIONS

(1) **Privacy**

(a) **Against terminals**
Identification: *no*
Correlation: *no*

(b) **Against back-end**
Identification: *no*
Correlation: *yes*

(c) **Against observers**
PII Derivation: *no*

(2) **Fine-granular billing support**

(3) **Loose-coupling**

(4) **Efficiency**
Check-in/out events handling

(5) **Multilateral security**

OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution

RELATED WORK/OTHER SOLUTIONS

- Academic solutions: not covering all requirements
- Industry: essentially not interested in privacy preservation

RELATED WORK/OTHER SOLUTIONS

- Academic solutions: not covering all requirements
- Industry: essentially not interested in privacy preservation

RELATED WORK/OTHER SOLUTIONS

- Academic solutions: not covering all requirements
- Industry: essentially not interested in privacy preservation

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
    - valid e-tickets remain anonymous to the terminal;
    - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
    - fine-granular billing for the registered tickets is possible;
    - direct identification of customers is prevented.

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
  - valid e-tickets remain anonymous to the terminal;
  - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
  - fine-granular billing for the registered tickets is possible;
  - direct identification of customers is prevented.

CORE CHALLENGES

- How to provide for a privacy-preserving local validation at the terminal side such that:
    - valid e-tickets remain anonymous to the terminal;
    - invalid e-tickets are rejected.
- How to allow for privacy-preserving travel records processing in the back-end such that:
    - fine-granular billing for the registered tickets is possible;
    - direct identification of customers is prevented.

OUTLINE

Introduction

Privacy Issues

State-of-the Art and Core Challenges

Our Solution

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)
   → no PII derivation
2. *(Insider)* **Terminals** can analyse the logs, may leak information.
   → No tracking and identification of valid e-tickets
3. *(Insider)* **Back-end** can process all information pieces under its control
   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

ADVERSARY MODEL

1. *(Outsider)* **External observers** can observe the communication between terminals and e-tickets (front-end)

   → no PII derivation

2. *(Insider)* **Terminals** can analyse the logs, may leak information.

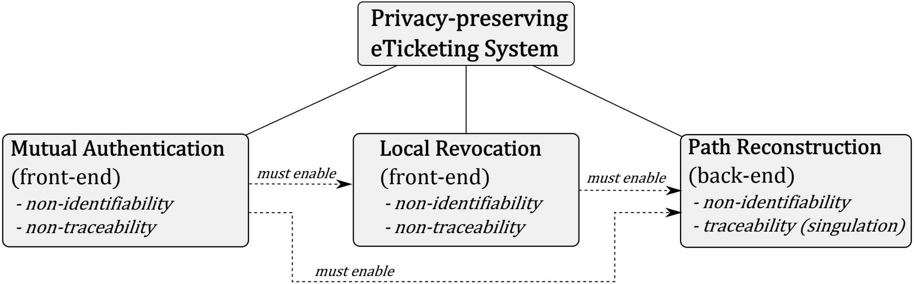
   → No tracking and identification of valid e-tickets

3. *(Insider)* **Back-end** can process all information pieces under its control

   → No direct identification of any e-ticket

→ *Insider/outsider* with respect to the involvement into the system flow.

SOLUTION BUILDING BLOCKS



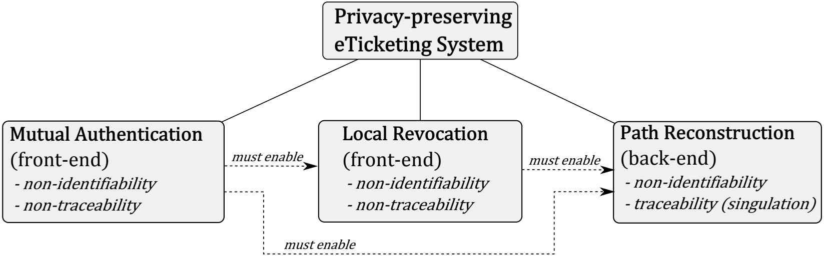
Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- *non-identifiability*
- *non-traceability*

Local Revocation (front-end)
- *non-identifiability*
- *non-traceability*

Path Reconstruction (back-end)
- *non-identifiability*
- *traceability (singulation)*

SOLUTION BUILDING BLOCKS (2)



Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- *non-identifiability*
- *non-traceability*

Local Revocation (front-end)
- *non-identifiability*
- *non-traceability*

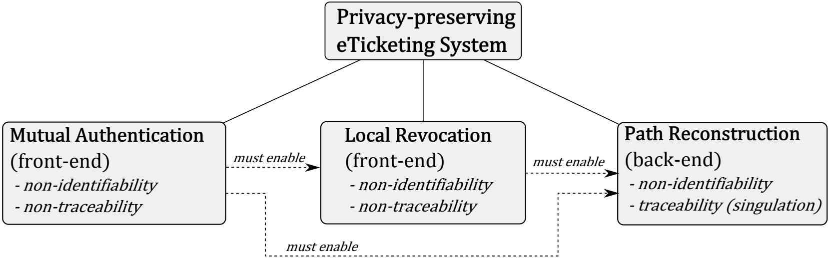
Path Reconstruction (back-end)
- *non-identifiability*
- *traceability (singulation)*

Tools available:
- Group Signatures
- ZKP of possession of a valid credential

Tools available:
- Dynamic Accumulators
- Homomorphic encryption and ZKP of correctness

Tools available:
- Predefined Matrix-based
- Private Information Retrieval?

SOLUTION BUILDING BLOCKS: SUMMARY



Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- *non-identifiability*
- *non-traceability*

Local Revocation (front-end)
- *non-identifiability*
- *non-traceability*

Path Reconstruction (back-end)
- *non-identifiability*
- *traceability (singulation)*

Tools available:
- Group Signatures
- ZKP of possession of a valid credential

Tools available:
- Dynamic Accumulators
- Homomorphic encryption and ZKP of correctness

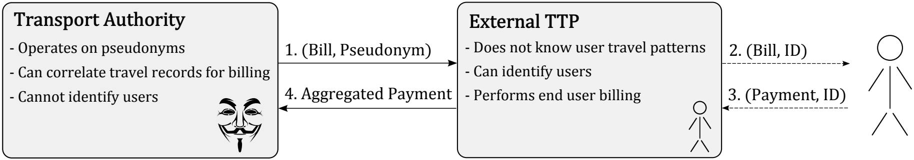
Tools available:
- Predefined Matrix-based
- Other approaches?

Chosen approach:
- **A slightly modified certificate-based authentication**

Chosen approach:
- **A custom blacklisting scheme**

Chosen approach:
- **A custom pseudonymisation scheme**

SOLUTION OUTLINE



Transport Authority

- Operates on pseudonyms
- Can correlate travel records for billing
- Cannot identify users

1. (Bill, Pseudonym)

4. Aggregated Payment

External TTP

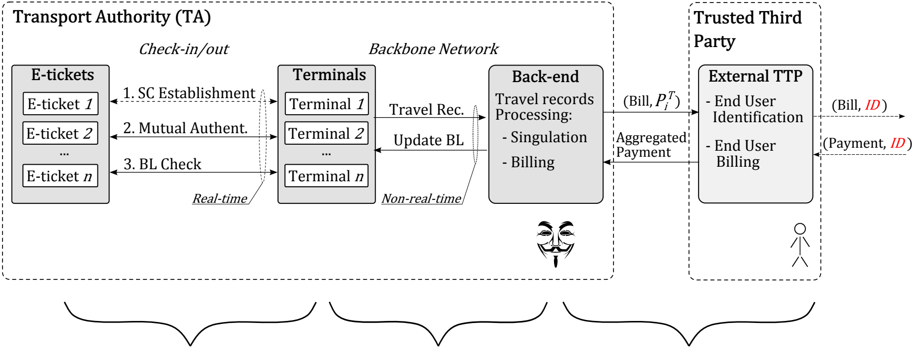
- Does not know user travel patterns
- Can identify users
- Performs end user billing

2. (Bill, ID)

3. (Payment, ID)

- Information minimization
- Separation of concerns

THE SUGGESTED PRIVACY-PRESERVING FRAMEWORK

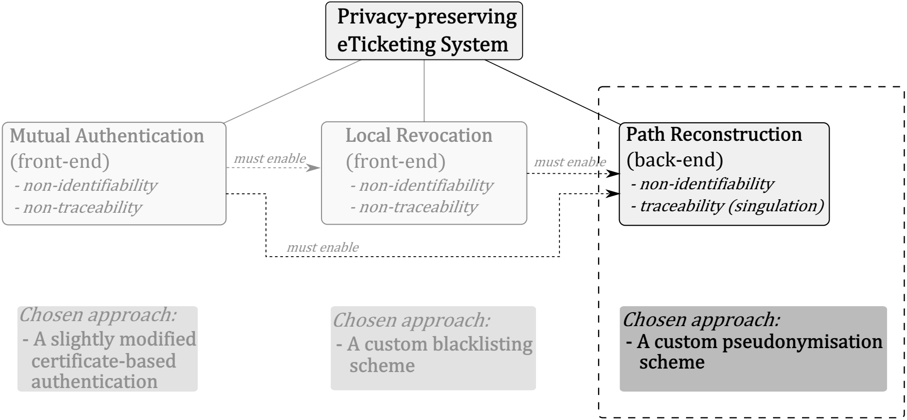


Front-end Interaction
(time critical)

Back-end Processing

Distributed Billing

PATH RECONSTRUCTION: PSEUDONYMISATION



Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- *non-identifiability*
- *non-traceability*

Local Revocation (front-end)
- *non-identifiability*
- *non-traceability*

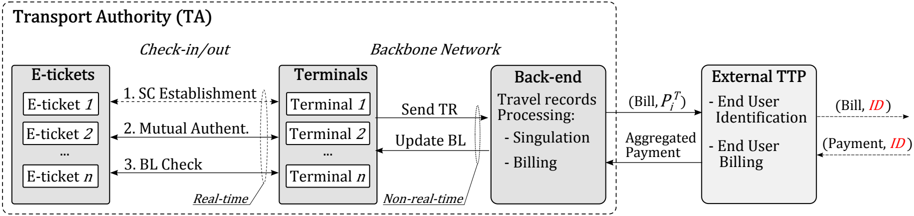
Path Reconstruction (back-end)
- *non-identifiability*
- *traceability (singulation)*

Chosen approach:
- A slightly modified certificate-based authentication

Chosen approach:
- A custom blacklisting scheme

Chosen approach:
- A custom pseudonymisation scheme

PATH RECONSTRUCTION: PSEUDONYMISATION



Transport Authority (TA)

Check-in/out

Backbone Network

E-tickets

E-ticket *1*

E-ticket *2*

...

E-ticket *n*

1. SC Establishment
2. Mutual Authent.
3. BL Check

Real-time

Terminals

Terminal *1*

Terminal *2*

...

Terminal *n*

Send TR

Update BL

Non-real-time

Back-end

Travel records Processing:

- Singulation
- Billing

(Bill, P_i^T)

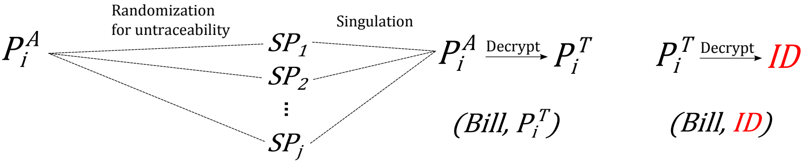
Aggregated Payment

External TTP

- End User Identification
- End User Billing

(Bill, *ID*)

(Payment, *ID*)



Randomization for untraceability

Singulation

P_i^A

SP_1

SP_2

$\vdots$

SP_j

$P_i^A \xrightarrow{\text{Decrypt}} P_i^T$

$P_i^T \xrightarrow{\text{Decrypt}} ID$

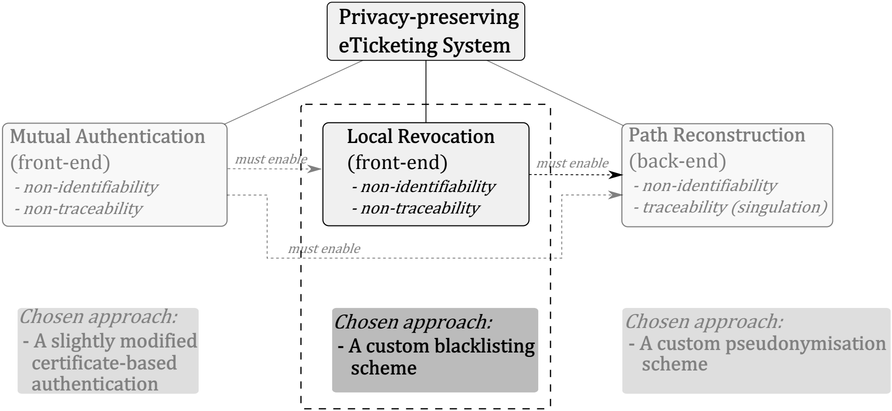
(Bill, P_i^T)

(Bill, ID)

$$SP_j = E_{k^+_{ta}}\left(P_i^A \cdot r_j\right)$$

r_j is a session-specific, random nonce

LOCAL REVOCATION BASED ON BLACKLISTS



Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- *non-identifiability*
- *non-traceability*

must enable

Local Revocation (front-end)
- *non-identifiability*
- *non-traceability*

must enable

Path Reconstruction (back-end)
- *non-identifiability*
- *traceability (singulation)*

must enable

Chosen approach:
- A slightly modified certificate-based authentication

Chosen approach:
- A custom blacklisting scheme

Chosen approach:
- A custom pseudonymisation scheme

LOCAL REVOCATION BASED ON BLACKLISTS

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right)$;
- Homomorphic property: $E(x \cdot r) = E(x)^r$;
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big)$;
- Black list: $\{y : y \in BL\}$;
- Check SP_j against the BL: $\forall y \in BL, E(r) \in SPT : \; c \leftarrow E(r)^y$ $c \overset{?}{=} E(x \cdot r) \; \forall c \in C$.

LOCAL REVOCATION BASED ON BLACKLISTS

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right)$;
- Homomorphic property: $E(x \cdot r) = E(x)^r$;
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big)$;
- Black list: $\{y : y \in BL\}$;
- Check SP_j against the BL: $\forall y \in BL, E(r) \in SPT: \; c \leftarrow E(r)^y$ $c \overset{?}{=} E(x \cdot r) \;\; \forall c \in C$.

LOCAL REVOCATION BASED ON BLACKLISTS

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right)$;
- Homomorphic property: $E(x \cdot r) = E(x)^r$;
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big)$;
- Black list: $\{y : y \in BL\}$;
- Check SP_j against the BL: $\forall y \in BL, E(r) \in SPT : \; c \leftarrow E(r)^y$ $c \stackrel{?}{=} E(x \cdot r) \;\; \forall c \in C$.

LOCAL REVOCATION BASED ON BLACKLISTS

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right)$;
- Homomorphic property: $E(x \cdot r) = E(x)^r$;
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big)$;
- Black list: $\{y : y \in BL\}$;
- Check SP_j against the BL: $\forall y \in BL, E(r) \in SPT : \ c \leftarrow E(r)^y$ $c \overset{?}{=} E(x \cdot r) \ \ \forall c \in C$.

LOCAL REVOCATION BASED ON BLACKLISTS

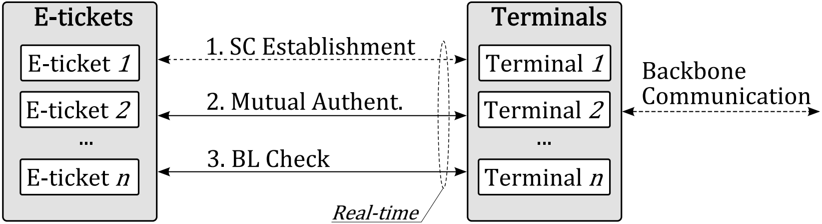
- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right)$;
- Homomorphic property: $E(x \cdot r) = E(x)^r$;
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big)$;
- Black list: $\{y : y \in BL\}$;
- Check SP_j against the BL: $\forall y \in BL, E(r) \in SPT :\; c \leftarrow E(r)^y$ $c \overset{?}{=} E(x \cdot r) \;\; \forall c \in C$.

LOCAL REVOCATION BASED ON BLACKLISTS

- Based on the inherent homomorphism of an encryption scheme in use: $P_i^A = E_{k_{ta}^+}\left(P_i^T\right);$
- Homomorphic property: $E(x \cdot r) = E(x)^r;$
- On validation, an e-ticket presents a tuple to a terminal: $SPT \leftarrow \big(E(x \cdot r), E(r)\big);$
- Black list: $\{y : y \in BL\};$
- Check SP_j against the BL: $\forall y \in BL, E(r) \in SPT : \; c \leftarrow E(r)^y$ $c \overset{?}{=} E(x \cdot r) \;\; \forall c \in C.$

LOCAL REVOCATION BASED ON BLACKLISTS (2)

Check-in/Check-out



E-tickets

E-ticket *1*

E-ticket *2*

...

E-ticket *n*

1. SC Establishment
2. Mutual Authent.
3. BL Check

Real-time

Terminals

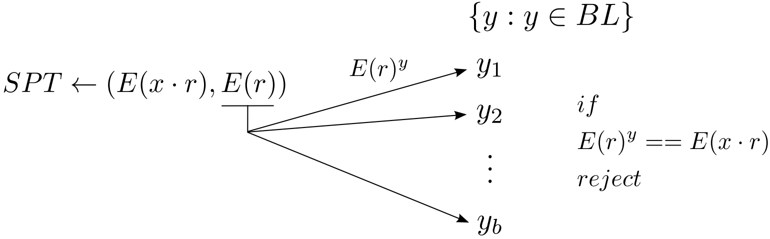
Terminal *1*

Terminal *2*

...

Terminal *n*

Backbone Communication



$$\{y : y \in BL\}$$

$$SPT \leftarrow (E(x \cdot r), \underline{E(r)})$$

$$E(r)^y \rightarrow y_1, y_2, \ldots, y_b$$

if

$E(r)^y == E(x \cdot r)$

$reject$

LOCAL REVOCATION: BOOSTING PERFORMANCE

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional k-anonymous identifier
- Results in partitioned blacklist and $\mathcal{O}(1)$ in the number of blacklisted elements

LOCAL REVOCATION: BOOSTING PERFORMANCE

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional k-anonymous identifier
- Results in partitioned blacklist and $\mathcal{O}(1)$ in the number of blacklisted elements

LOCAL REVOCATION: BOOSTING PERFORMANCE

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional k-anonymous identifier
- Results in partitioned blacklist and $\mathcal{O}(1)$ in the number of blacklisted elements

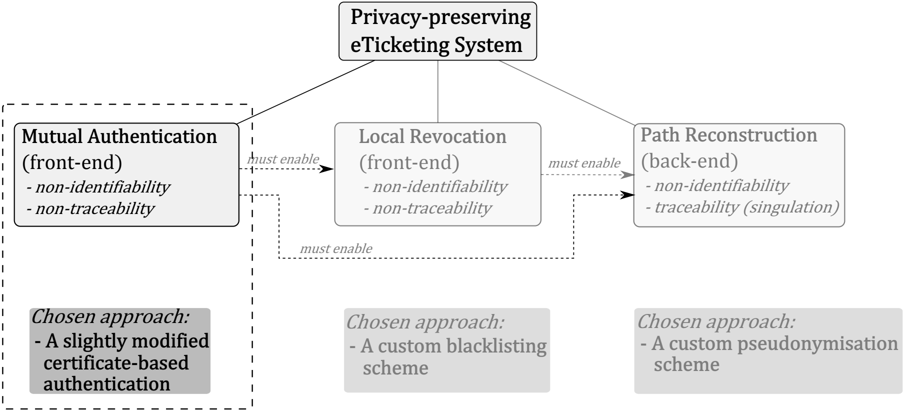
LOCAL REVOCATION: BOOSTING PERFORMANCE

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional k-anonymous identifier
- Results in partitioned blacklist and $\mathcal{O}(1)$ in the number of blacklisted elements

LOCAL REVOCATION: BOOSTING PERFORMANCE

- Basic version has linear complexity in the number of blacklisted elements
- The anonymity set of each session pseudonym can be reduced in a controllable way
- Additional *k*-anonymous identifier
- Results in partitioned blacklist and $\mathcal{O}(1)$ in the number of blacklisted elements

PRIVACY-PRESERVING MUTUAL AUTHENTICATION



Privacy-preserving eTicketing System

Mutual Authentication (front-end)
- *non-identifiability*
- *non-traceability*

Local Revocation (front-end)
- *non-identifiability*
- *non-traceability*

Path Reconstruction (back-end)
- *non-identifiability*
- *traceability (singulation)*

Chosen approach:
- A slightly modified certificate-based authentication

Chosen approach:
- A custom blacklisting scheme

Chosen approach:
- A custom pseudonymisation scheme

PRIVACY-PRESERVING MUTUAL AUTHENTICATION

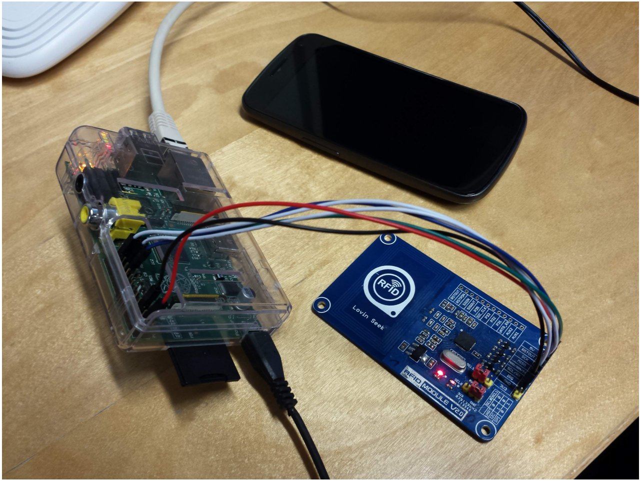
- A variation of the certificate-based authentication
- Alternatively, more profound group signatures can be used

Key	**Type**
$K_e \leftarrow (k_{gr}^{+}, k_{gr}^{-})$	group key pair of an e-ticket;
$K_t \leftarrow (k_t^{+}, k_t^{-})$	unique key pair of a terminal;
$K_{ta} \leftarrow (k_{ta}^{+}, k_{ta}^{-})$	unique key pair of a transport authority;

THE DEVELOPED PROTOTYPE

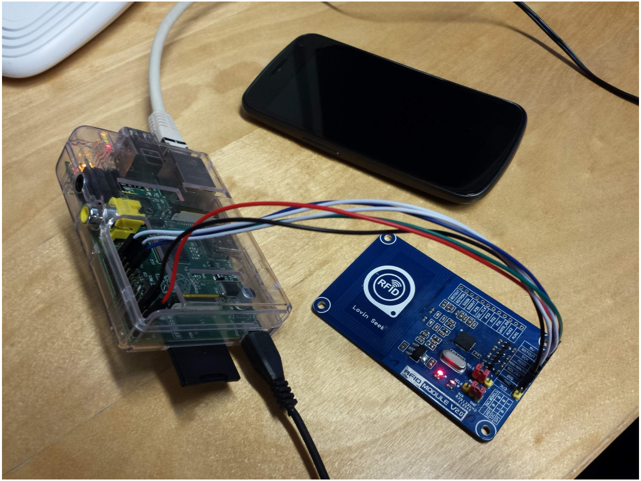
- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250

THE DEVELOPED PROTOTYPE



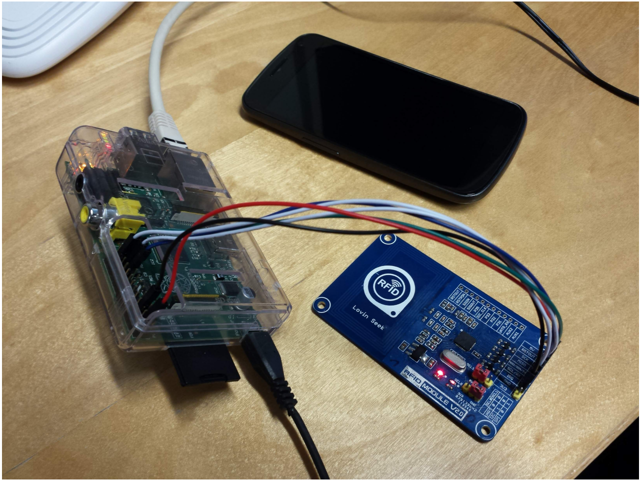
- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250

THE DEVELOPED PROTOTYPE



- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250

THE DEVELOPED PROTOTYPE

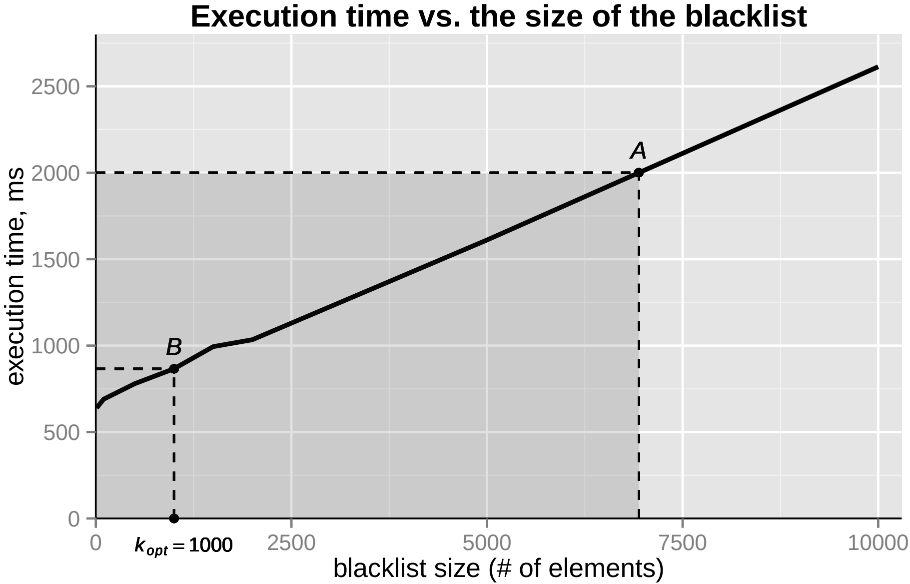


- PN532 NFC Breakout Board via SPI on
- Raspberry Pi Model B 256MB RAM
- NFC Smart phone: Samsung Galaxy Nexus GT-I9250

A SHORT DEMO

- Check-in/check-out session: a video demonstration

PROTOTYPE PERFORMANCE



INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:
- Our solution is based on loose-coupling
- Multi-entity environment (interoperability and separation of concerns):
    - The interfaces for accommodating TTP are already present
    - E.g., KVP in eTicket Germany (VDV-KA)
- Leveraging the cryptographic mechanisms supported by constrained devices
    - Smart card industry
    - Smart phone industry

INTEGRATION OF OUR SOLUTION INTO REAL-WORLD SYSTEMS

- Can be achieved at a relatively low cost, since:

- Our solution is based on loose-coupling

- Multi-entity environment (interoperability and separation of concerns):
  - The interfaces for accommodating TTP are already present
  - E.g., KVP in eTicket Germany (VDV-KA)

- Leveraging the cryptographic mechanisms supported by constrained devices
  - Smart card industry
  - Smart phone industry

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority's security domain
- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
    - without relying on device tamper-resistance and
    - on the security of transport authority's security domain
- More efficient local revocation:
    - advanced cryptographic tools impose additional restrictions (require further assumptions)
    - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
    - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority's security domain
- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority's security domain
- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority's security domain
- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
    - without relying on device tamper-resistance and
    - on the security of transport authority's security domain
- More efficient local revocation:
    - advanced cryptographic tools impose additional restrictions (require further assumptions)
    - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
    - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority's security domain
- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority’s security domain

- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.

- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: CONCEPT

- Secure proof of correctness and well-formedness of the tuple delivered to the terminal:
  - without relying on device tamper-resistance and
  - on the security of transport authority's security domain
- More efficient local revocation:
  - advanced cryptographic tools impose additional restrictions (require further assumptions)
  - efficiency considerations.
- Securing critical info on a smart phone (keys, etc.)
  - no tamper-resistant storage by default

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.
- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.
- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
    - resource constraints
    - supported cryptographic operations are tailored for specific use cases and standards.
- In case of NFC-enabled handsets:
    - interactive NFC interface (supporting challenge-response) turned out to be a problem
    - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
    - resource constraints
    - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
    - interactive NFC interface (supporting challenge-response) turned out to be a problem
    - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.
- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
  - resource constraints
  - supported cryptographic operations are tailored for specific use cases and standards.

- In case of NFC-enabled handsets:
  - interactive NFC interface (supporting challenge-response) turned out to be a problem
  - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

CURRENT CHALLENGES: IMPLEMENTATION

- For off-the-shelf smart cards:
    - resource constraints
    - supported cryptographic operations are tailored for specific use cases and standards.
- In case of NFC-enabled handsets:
    - interactive NFC interface (supporting challenge-response) turned out to be a problem
    - supported NFC reader types are relatively slow (UART-to-USB vs. SPI)

OUR SOLUTION: SUMMARY

- A privacy-preserving framework for e-ticketing systems
- Satisfies all the requirements
- Goes in line with the adopted attacker model

OUR SOLUTION: SUMMARY

- A privacy-preserving framework for e-ticketing systems
- Satisfies all the requirements
- Goes in line with the adopted attacker model

Thank you for your attention!
Questions? Comments?
Suggestions?

REFERENCES I

[1] F. Baldimtsi, G. Hinterwalder, A. Rupp, A. Lysyanskaya, C. Paar, and W. P. Burleson, “Pay as you go,” in *Workshop on hot topics in privacy enhancing technologies, HotPETSs 2012*, `http://petsymposium.org/2012/papers/hotpets12-8-pay.pdf`, 2012.

[2] T. S. Heydt-Benjamin, H.-J. Chae, B. Defend, and K. Fu, “Privacy for Public Transportation,” in *Proceedings of the 6th international conference on Privacy Enhancing Technologies*, PET’06, (Berlin, Heidelberg), pp. 1–19, Springer-Verlag, 2006.

[3] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, “User Privacy in Transport Systems Based on RFID E-Tickets,” in *Workshop on Privacy in Location-Based Applications (PILBA 2008)*, vol. 5283 of *Lecture Notes in Computer Sciences*, Springer-Verlag, October 2008.

[4] F. Garcia and P. Rossum, “Modeling Privacy for Off-Line RFID Systems,” in *Smart Card Research and Advanced Application* (D. Gollmann, J.-L. Lanet, and J. Iguchi-Cartigny, eds.), vol. 6035 of *Lecture Notes in Computer Science*, pp. 194–208, Springer Berlin Heidelberg, 2010.

[5] G. Avoine, C. Lauradoux, and T. Martin, “When Compromised Readers Meet RFID,” in *Information Security Applications* (H. Y. Youm and M. Yung, eds.), vol. 5932 of *Lecture Notes in Computer Science*, pp. 36–50, Springer Berlin Heidelberg, 2009.

[6] M. Ohkubo, K. Suzuki, and S. Kinoshita, “Cryptographic Approach to ”Privacy-Friendly” Tags,” in *In RFID Privacy Workshop*, 2003.

[7] B. Song and C. J. Mitchell, “Scalable RFID security protocols supporting tag ownership transfer,” *Comput. Commun.*, vol. 34, pp. 556–566, apr 2011.

[8] A. Juels and R. Pappu, “Squealing Euros: Privacy Protection in RFID-Enabled Banknotes,” in *Financial Cryptography 03*, pp. 103–121, Springer-Verlag, 2002.

[9] T.-L. Lim, T. Li, and S.-L. 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, (Washington, DC, USA), pp. 40–49, IEEE Computer Society, 2008.

REFERENCES II

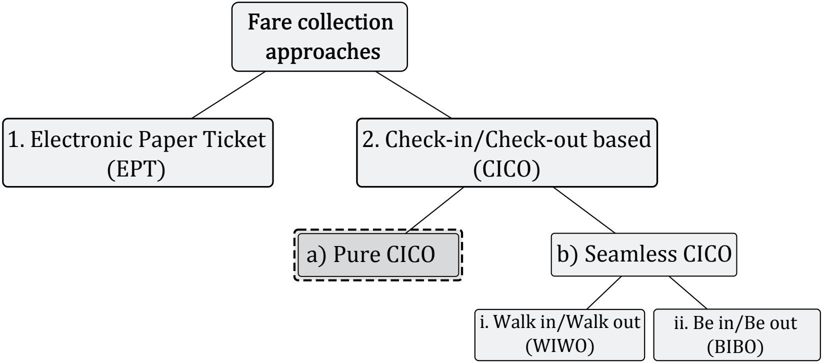
[10] W. Choi and B.-h. Roh, “Backward Channel Protection Method for RFID Security Schemes Based on Tree-Walking Algorithms,” in *Computational Science and Its Applications - ICCSA 2006* (M. Gavrilova, O. Gervasi, V. Kumar, C. Tan, D. Taniar, A. Lagan, Y. Mun, and H. Choo, eds.), vol. 3983 of *Lecture Notes in Computer Science*, pp. 279–287, Springer Berlin / Heidelberg, 2006.

[11] T.-L. Lim, T. Li, and S.-L. Yeo, “A Cross-layer Framework for Privacy Enhancement in RFID systems,” *Pervasive and Mobile Computing*, vol. 4, no. 6, pp. 889 – 905, 2008.

[12] I. Gudymenko, “Protection of the Users Privacy in Ubiquitous RFID Systems,” Master’s thesis, Technische Universitt Dresden, Faculty of Computer Science, December 2011.

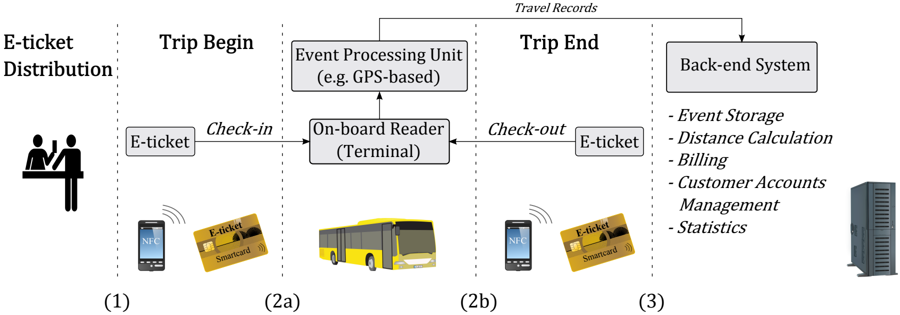
BACKUP SLIDES

FARE COLLECTION APPROACHES IN E-TICKETING



- Focus on CICO-based systems

A GENERAL APPLICATION SCENARIO: DETAILED



Travel Records

E-ticket Distribution

Trip Begin

Event Processing Unit (e.g. GPS-based)

Trip End

Back-end System

E-ticket

Check-in

On-board Reader (Terminal)

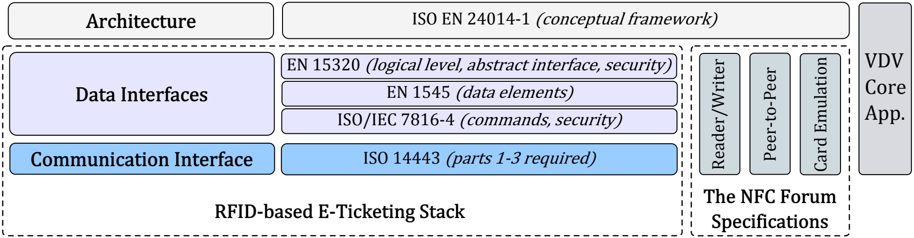
Check-out

E-ticket

- *Event Storage*
- *Distance Calculation*
- *Billing*
- *Customer Accounts Management*
- *Statistics*

E-TICKETING: TECHNOLOGIES AND STANDARDS

- RFID-based stack (proximity cards);
- NFC stack (NFC-enabled devices);
- E-ticket Germany: “Core Application” (VDV-KA)



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)*

RFID-based E-Ticketing Stack

Reader/Writer; Peer-to-Peer; Card Emulation

The NFC Forum Specifications

VDV Core App.

WHY FINE-GRANULAR BILLING?

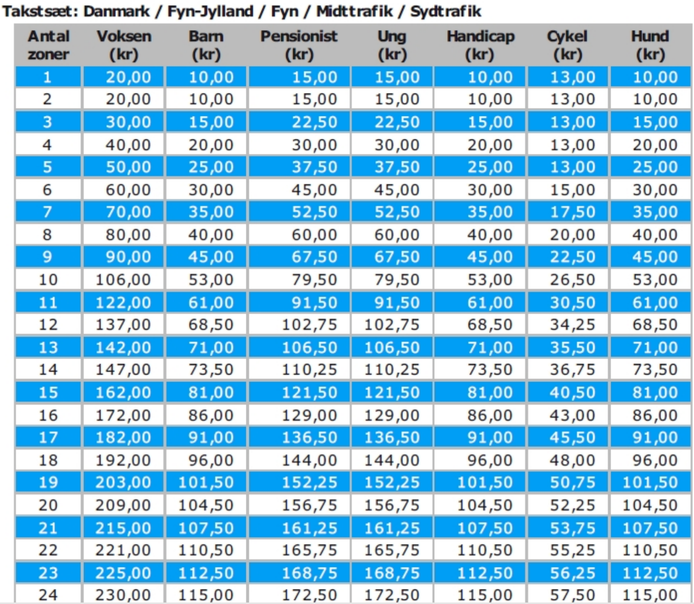
- An important feature (with high potential)
- Enables highly flexible fare polices (loyalty programs, individual discounts, etc.):
    - Essential for a modern public transport market
    - Personalized cards are often a preferred choice due to more services they provide [de Panizza *et al.*, 2010];
- Several real-world systems are already supporting regular billing (Hannover, Phoenix).

E-TICKETING: MAIN ADVANTAGES

- **For transport companies**
  - decrease in system maintenance costs;
  - significant reduction of payment handling costs;
  - fare dodgers rate improvement;
  - better support of flexible pricing schemes;
  - support of multiapplication/nontransit scenarios;
  - a high interoperability potential.

- **For customers**
  - faster verification of an e-ticket;
  - ”pay as you go”;
  - flexible pricing schemes;
  - increased usability.

Fare System in Danemark



Takstsæt: Danmark / Fyn-Jylland / Fyn / Midttrafik / Sydtrafik

Antal zoner	Voksen (kr)	Barn (kr)	Pensionist (kr)	Ung (kr)	Handicap (kr)	Cykel (kr)	Hund (kr)
1	20,00	10,00	15,00	15,00	10,00	13,00	10,00
2	20,00	10,00	15,00	15,00	10,00	13,00	10,00
3	30,00	15,00	22,50	22,50	15,00	13,00	15,00
4	40,00	20,00	30,00	30,00	20,00	13,00	20,00
5	50,00	25,00	37,50	37,50	25,00	13,00	25,00
6	60,00	30,00	45,00	45,00	30,00	15,00	30,00
7	70,00	35,00	52,50	52,50	35,00	17,50	35,00
8	80,00	40,00	60,00	60,00	40,00	20,00	40,00
9	90,00	45,00	67,50	67,50	45,00	22,50	45,00
10	106,00	53,00	79,50	79,50	53,00	26,50	53,00
11	122,00	61,00	91,50	91,50	61,00	30,50	61,00
12	137,00	68,50	102,75	102,75	68,50	34,25	68,50
13	142,00	71,00	106,50	106,50	71,00	35,50	71,00
14	147,00	73,50	110,25	110,25	73,50	36,75	73,50
15	162,00	81,00	121,50	121,50	81,00	40,50	81,00
16	172,00	86,00	129,00	129,00	86,00	43,00	86,00
17	182,00	91,00	136,50	136,50	91,00	45,50	91,00
18	192,00	96,00	144,00	144,00	96,00	48,00	96,00
19	203,00	101,50	152,25	152,25	101,50	50,75	101,50
20	209,00	104,50	156,75	156,75	104,50	52,25	104,50
21	215,00	107,50	161,25	161,25	107,50	53,75	107,50
22	221,00	110,50	165,75	165,75	110,50	55,25	110,50
23	225,00	112,50	168,75	168,75	112,50	56,25	112,50
24	230,00	115,00	172,50	172,50	115,00	57,50	115,00

GENERIC PRIVACY THREATS IN E-TICKETING SYSTEMS

1. Unintended customer identification:
    a) Exposure of the customer ID:
        i. Personal ID exposure (direct identification);
        ii. Indirect identification through the relevant object's ID.
    b) Exposure of a non-encrypted identifier during the anti-collision session;
    c) Physical layer identification (RFID fingerprinting).
2. Information linkage;
3. Illegal customer profiling.

→ A **cross-layered** set of countermeasures required.

GENERIC COUNTERMEASURES

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 [8]
ii. Indirect identification	ID encryption
b) *Unencrypted ID during anti-collision*	Randomized bit encoding [9]; bit collision masking [10, 11] (protocol dependent)
c) *PHY-layer identification*	Shielding; switchable antennas [12]
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

- Difficult to apply in a **joint** fashion.

STATE OF THE ART

- Real-world systems
- Academic solutions

REAL-WORLD SYSTEMS

- Primary focus on:
  - direct functionality
  - system security
  - resource effectiveness (cost implications)

- Privacy is usually considered in the second place, if at all

- Frequently, privacy is **traded-off** for efficiency (as far as legislation allows)

- Examples: eTicket Germany (KA), Metrô São Paulo, ...

ACADEMIC SOLUTIONS

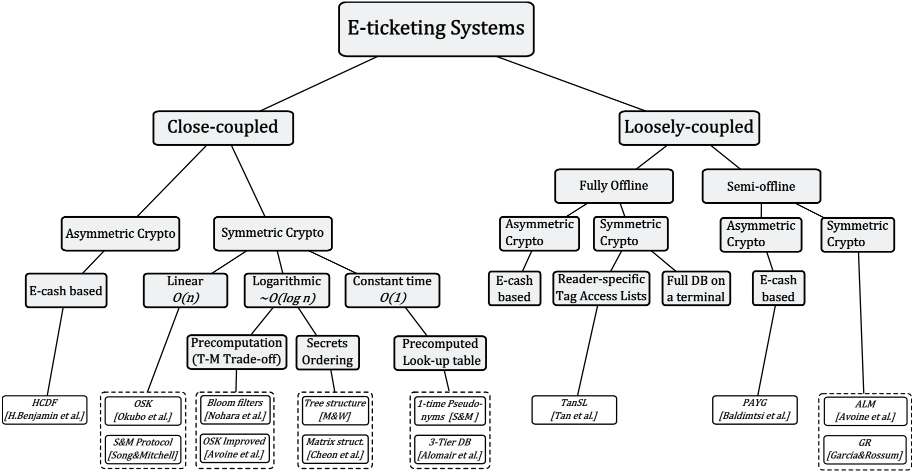
- Loosely-coupled architecture

- Tightly-coupled architecture

IMPORTANT EVALUATION CRITERIA

- Mutual authentication between terminals and e-ticket;
- E-ticket anonymity/untraceability against terminals;
- Trust assumptions (esp. concerning terminals);
- Back-end coupling;
- Regular billing support.

ACADEMTIC SOLUTIONS: TAXONOMY



- E-ticketing Systems
  - Close-coupled
    - Asymmetric Crypto
      - E-cash based
        - *HCDF [H.Benjamin et al.]*
    - Symmetric Crypto
      - Linear $O(n)$
        - *OSK [Okubo et al.]*
        - *S&M Protocol [Song&Mitchell]*
      - Logarithmic $\sim O(\log n)$
        - Precomputation (T-M Trade-off)
          - *Bloom filters [Nohara et al.]*
          - *OSK Improved [Avoine et al.]*
        - Secrets Ordering
          - *Tree structure [M&W]*
          - *Matrix struct. [Cheon et al.]*
      - Constant time $O(1)$
        - Precomputed Look-up table
          - *1-time Pseudonyms [S&M]*
          - *3-Tier DB [Alomair et al.]*
  - Loosely-coupled
    - Fully Offline
      - Asymmetric Crypto
        - E-cash based
      - Symmetric Crypto
        - Reader-specific Tag Access Lists
          - *TanSL [Tan et al.]*
        - Full DB on a terminal
    - Semi-offline
      - Asymmetric Crypto
        - E-cash based
          - *PAYG [Baldimtsi et al.]*
      - Symmetric Crypto
        - *ALM [Avoine et al.]*
        - *GR [Garcia&Rossum]*

ACADEMIC SOULUTIONS: ASSESSMENT

Criteria	**The most relevant approaches Reviewed**						
	PAYG[1]	HCDF[2]	SVW[3]	GR[4]	ALM[5]	OSK[6]	RSMP[7]
Anonymity terminals	yes	yes	p	no	no	yes	yes
Untraceability terminals	yes	yes	p	no	no	yes	yes
Mutual authentication	no	no	no	no	yes	no	yes
Close-coupling	no	yes	no	no	no	yes	yes
Regular billing	no	no	no	∅	∅	∅	∅
BE is trusted	no	no	yes	yes	yes	yes	yes
ATs are trusted	no	no	yes	yes	yes	no	no

Legend:

∅	–	not considered;
p	–	partially provided;

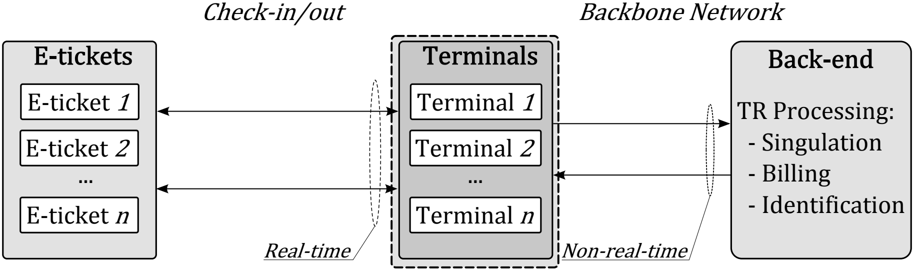
REQUIREMENTS: PRIVACY AGAINST TERMINALS

(1) **Privacy**

(a) **Against terminals**

Identification: *no*

Correlation: *no*



Check-in/out

Backbone Network

E-tickets

- E-ticket *1*
- E-ticket *2*
- ...
- E-ticket *n*

Terminals

- Terminal *1*
- Terminal *2*
- ...
- Terminal *n*

Back-end

TR Processing:
- Singulation
- Billing
- Identification

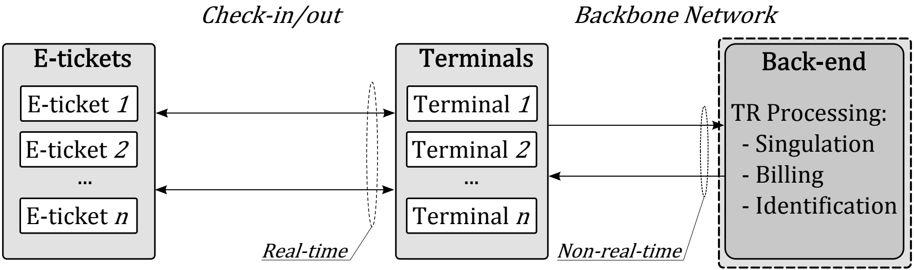
REQUIREMENTS: PRIVACY AGAINST THE BACK-END

(1) **Privacy**

(b) **Against back-end**

Identification: *no*

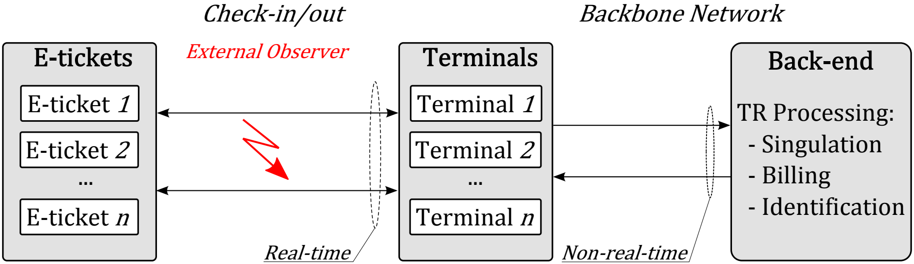
Correlation: *yes*



REQUIREMENTS AGAINST OBSERVERS

(1) **Privacy**

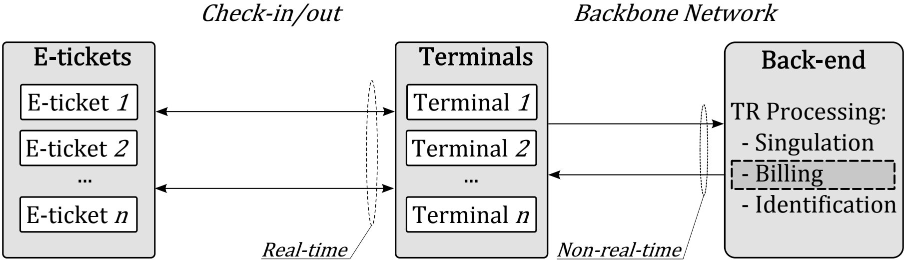
(c) **Against observers** PII Derivation: *no*



REQUIREMENTS: FINE-GRANULAR BILLING SUPPORT

(2) **Fine-granular billing support**

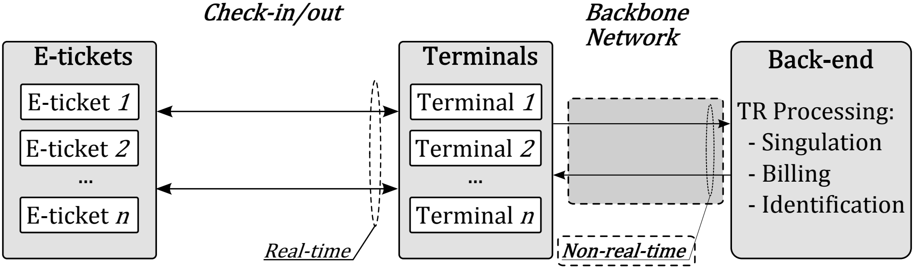
- Enabling best price calculation and discounts
- Tariff schemes must be separated from system architecture



REQUIREMENTS: LOOSE-COUPLING

(3) **Loose-coupling**

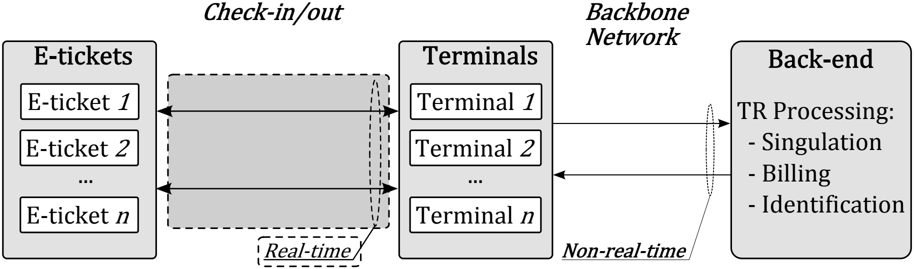
- Large-scale distribution;
- Compatibility to real-world systems (e.g., Metrô São Paulo, Dresdner Verskehrsbetriebe)



REQUIREMENTS: EFFICIENCY

(4) **Efficiency** Check-in/out events handling

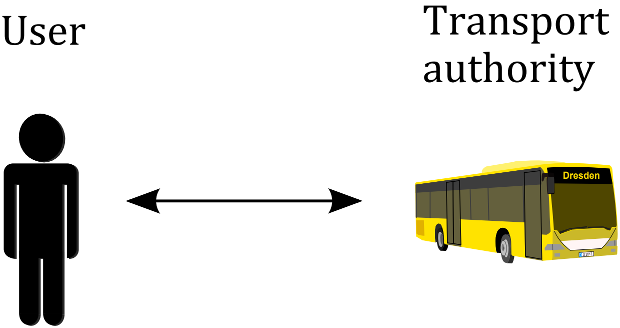
- Time-critical
- Directly affects customer experience



REQUIREMENTS: MULTILATERAL SECURITY

(5) **Multilateral security**

- Security goals of transport authority
- Security goals of users



User

Transport authority

CHALLENGES: MUTUAL AUTHENTICATION

1. *Dynamic extensibility.* Support for dynamic accommodation of new e-tickets is a must.
2. *Bootstrapping authentication.* Enabling authentication without tracking.
3. *Implications for path reconstruction.* Fully anonymous mutual authentication prohibits path reconstruction in the back-end
4. *Efficiency.* Advanced methods often have negative efficiency implications and can be resource prohibitive for constrained devices.

→ In our solution, a **slightly modified certificate-based approach** is chosen.

CHALLENGES: LOCAL REVOCATION

1. Determine (on the fly) if an e-ticket is valid or not
2. Without being able to track or identify e-tickets
3. Valid e-tickets must remain anonymous (to the terminal) and untraceable
4. Cryptographic tools like various cryptographic accumulators do not suit

→ Our solution considers **a custom blacklisting scheme**

CHALLENGES: PATH RECONSTRUCTION

1. The supported fare schemes need to be *flexible* and *extensible*
2. It should be possible to combine the rides to issue discounts
3. At the same time, in a privacy-preserving way
4. Simple fare schemes (e.g. matrix-based) allow for privacy-preserving billing with decent privacy properties
    - Efficiency is an issue, though [KHG13]

→ Our solution is based on a **special pseudonymisation scheme**

LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod \ p)$
- Homomorphic property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad (mod \quad p) \\ &= E(x)^r. \end{aligned}$$

- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.

LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod \ p)$
- Homomorphic property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad (mod \ \ p) \\ &= E(x)^r. \end{aligned}$$

- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.

LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod \ p)$
- Homomorphic property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad (mod \ \ p) \\ &= E(x)^r. \end{aligned}$$

- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.

LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod\ p)$
- Homomorphic property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad\qquad (mod\ \ p) \\ &= E(x)^r. \end{aligned}$$

- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.

LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod \ p)$
- Homomorphic property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad\qquad (mod \ \ p) \\ &= E(x)^r. \end{aligned}$$

- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.

LOCAL REVOCATION BASED ON BLACKLISTS: A CHOICE OF A SUITABLE ENCRYPTION SCHEME

- Based on the discrete exponentiation function
- $E(x) = g^x \ (mod\ p)$
- Homomorphic property:

$$\begin{aligned} E(x \cdot r) &= g^{(x \cdot r)} \\ &= \left(g^x\right)^r \qquad\qquad (mod\ \ p) \\ &= E(x)^r. \end{aligned}$$

- Okamoto-Uchiyama trapdoor as a private key
- Other inherently homomorphic deterministic schemes possible.

OTHER ACADEMIC SOLUTIONS AND OURS

Criteria	**The most relevant approaches Reviewed**							
	PAYG[1]	HCDF[2]	SVW[3]	GR[4]	ALM[5]	OSK[6]	RSMP[7]	**Our**
Anonymity terminals	yes	yes	p	no	no	yes	yes	**yes**
Untraceability terminals	yes	yes	p	no	no	yes	yes	**yes**
Mutual authentication	no	no	no	no	yes	no	yes	**yes**
Close-coupling	no	yes	no	no	no	yes	yes	**no**
Regular billing	no	no	no	∅	∅	∅	∅	**yes**
BE is trusted	no	no	yes	yes	yes	yes	yes	**no**
ATs are trusted	no	no	yes	yes	yes	no	no	**no**

Legend:

∅ – not considered;
p – partially provided;