July 10, 2013

Rights Management with NFC Smartphones and Electronic ID Cards: A Proof of Concept for Modern Car Sharing

Timo Kasper, Alexander Kühn, David Oswald,
Christian Zenger, Christof Paar

Chair for Embedded Security (EMSEC)
HGI, Ruhr-Universität Bochum, Germany

RFIDsec 2013
9th Workshop on RFID Security, Graz, Austria

Contactless Smartcards (and NFC)

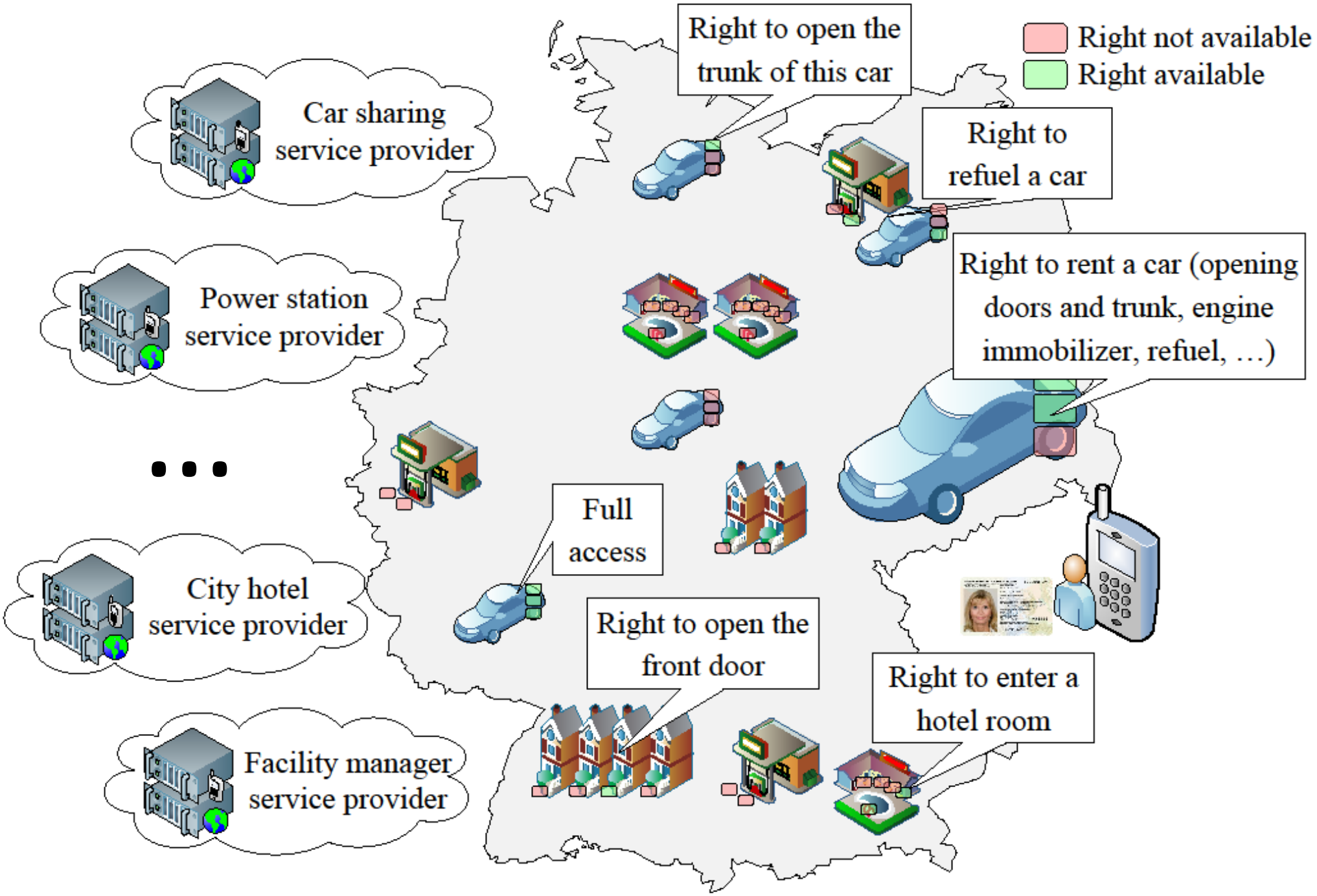
- defined in **ISO/IEC 14443** standard
- large scale applications:
  - access control systems
  - electronic passports
  - payment systems
  - ticketing / public transport
- Near Field Communication (NFC) is compatible to ISO/IEC 14443

NFC

The infrastructure (cards, readers, …) is out there

→ **Let's use it!**

Motivation


Right to open the trunk of this car
Right not available
Right available
Car sharing service provider
Right to refuel a car
Power station service provider
Right to rent a car (opening doors and trunk, engine immobilizer, refuel, …)
Full access
City hotel service provider
Right to open the front door
Right to enter a hotel room
Facility manager service provider

Goals of the Project

- on-line booking application
- correctly identify the customer (billing, …)

- transfer booked rights to phone

- access booked NFC objects with phone

(including scenarios *without* permanent Internet)

- enable alternatives based on contactless cards

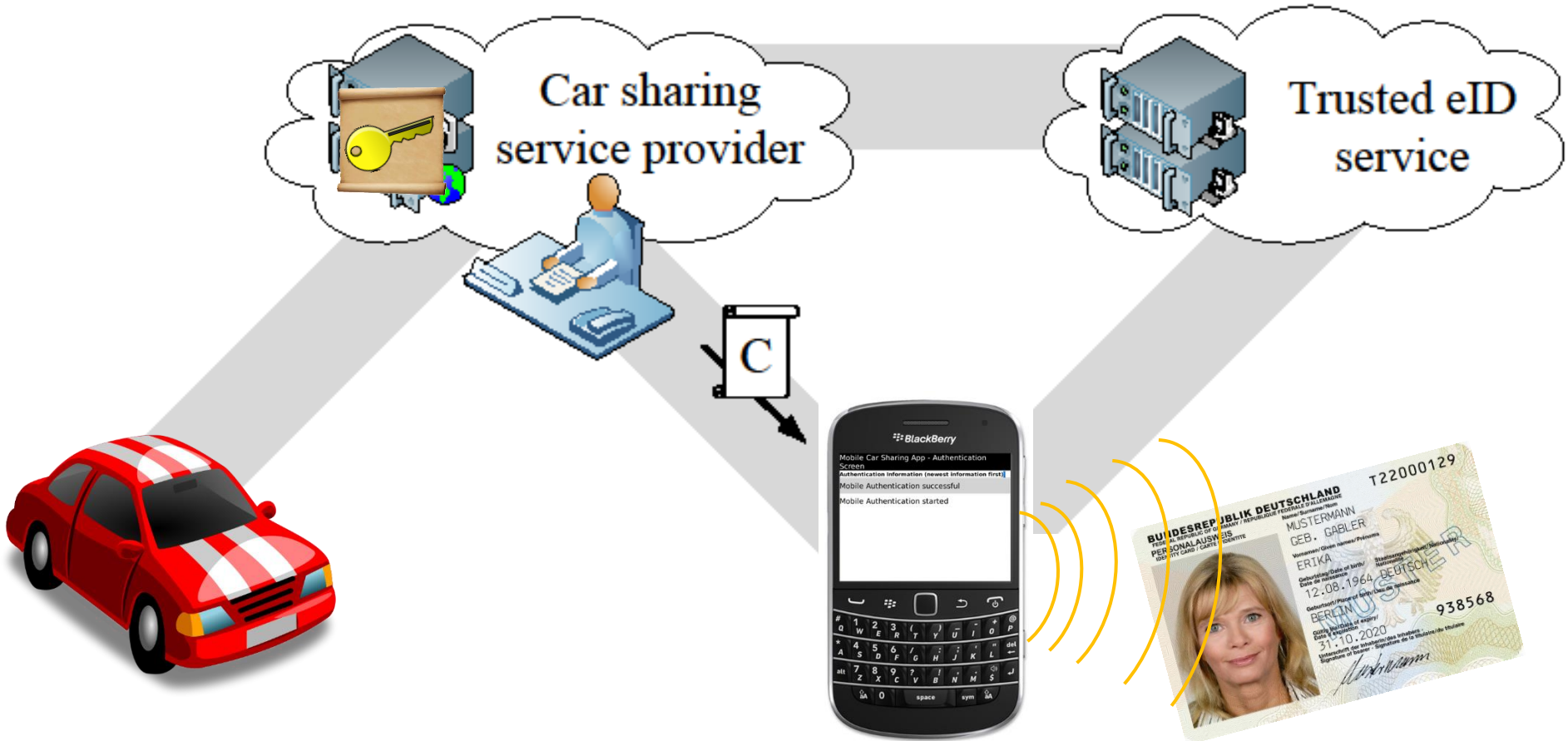
- **proof-of-concept implementation (!)**

Ingredients

1. **NFC-smartphone with Internet access (UMTS, GSM, …)**
   here: BlackBerry Bold 9900
2. **Contactless card with e-ID function**
   here: new German electronic identity card (nPA)
3. **NFC-enabled object(s)**
   here: red car with NFC interface

Phase 1: Booking (NFC phone acts as RFID reader)

- use e-ID card to prove customer's identity to service provider *(PACE with PIN and EAC)*
- credential is generated and *securely* transferred to the phone



Phase 2: Execute Booked Rights (NFC phone emulates Mifare DESfire)

- car acts as NFC reader, phone emulates Mifare DESfire card
- secure channel: 3DES-based mutual authentication scheme
- car obtains and checks credential
- if credential is valid, access is given

Thank you!

Questions?

timo.kasper@rub.de

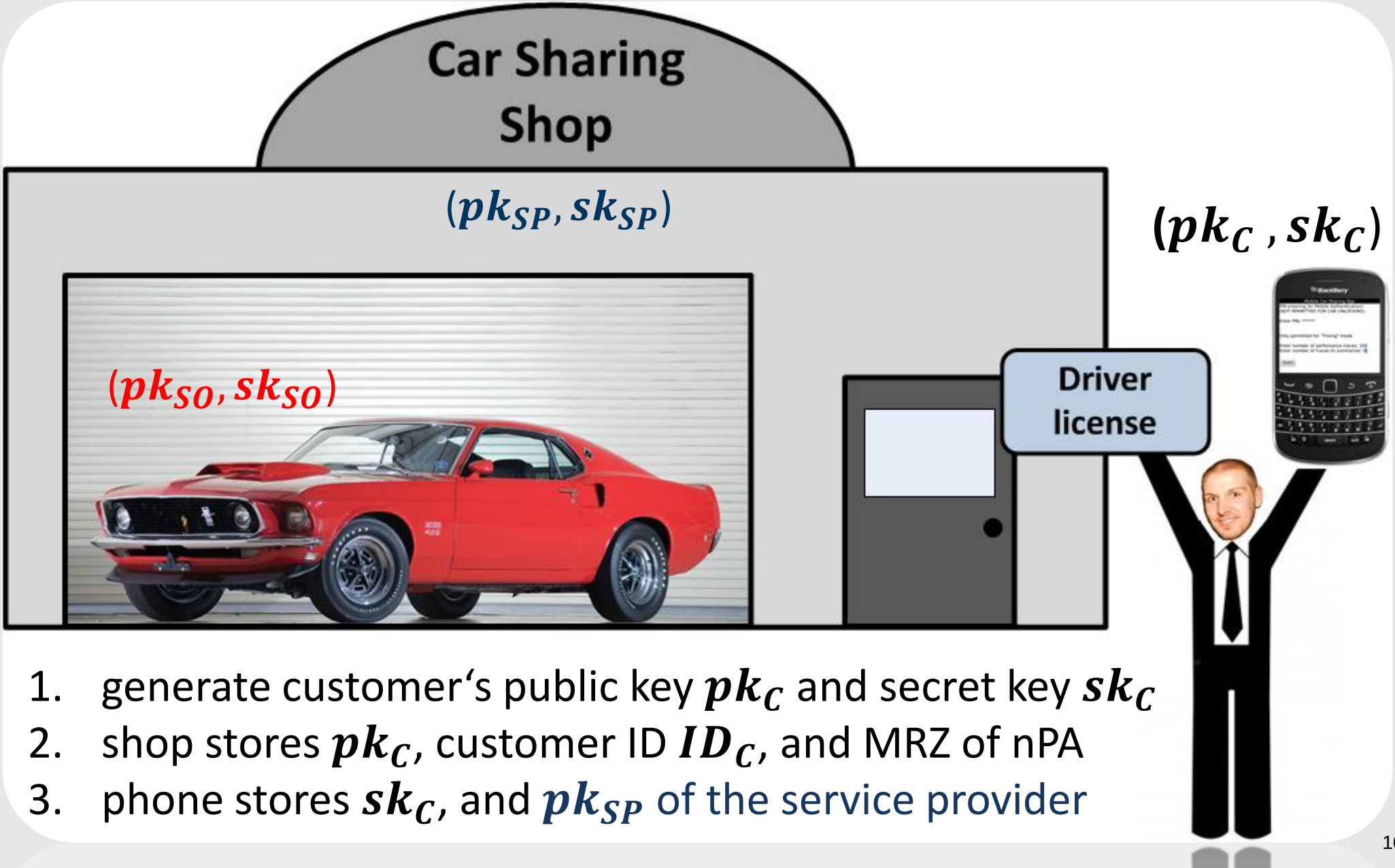
hgi EMSEC
RUHR-UNIVERSITÄT BOCHUM

Chair for Embedded Security (Prof. Christof Paar)

www.emsec.rub.de

OK, some more details ….

One-Time **Registration** at the Service Provider

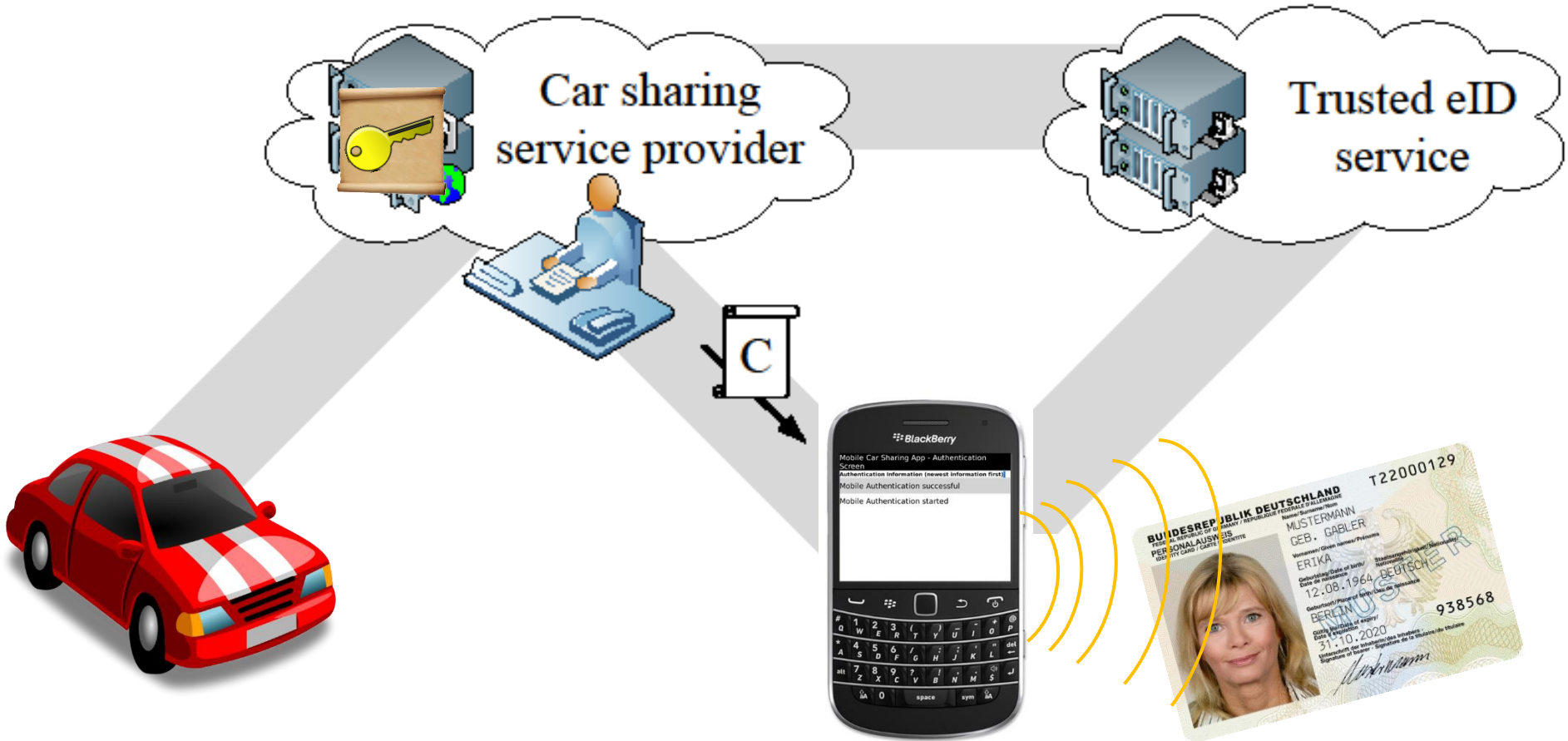


1. generate customer‘s public key $\boldsymbol{pk_C}$ and secret key $\boldsymbol{sk_C}$
2. shop stores $\boldsymbol{pk_C}$, customer ID $\boldsymbol{ID_C}$, and MRZ of nPA
3. phone stores $\boldsymbol{sk_C}$, and $\boldsymbol{pk_{SP}}$ of the service provider

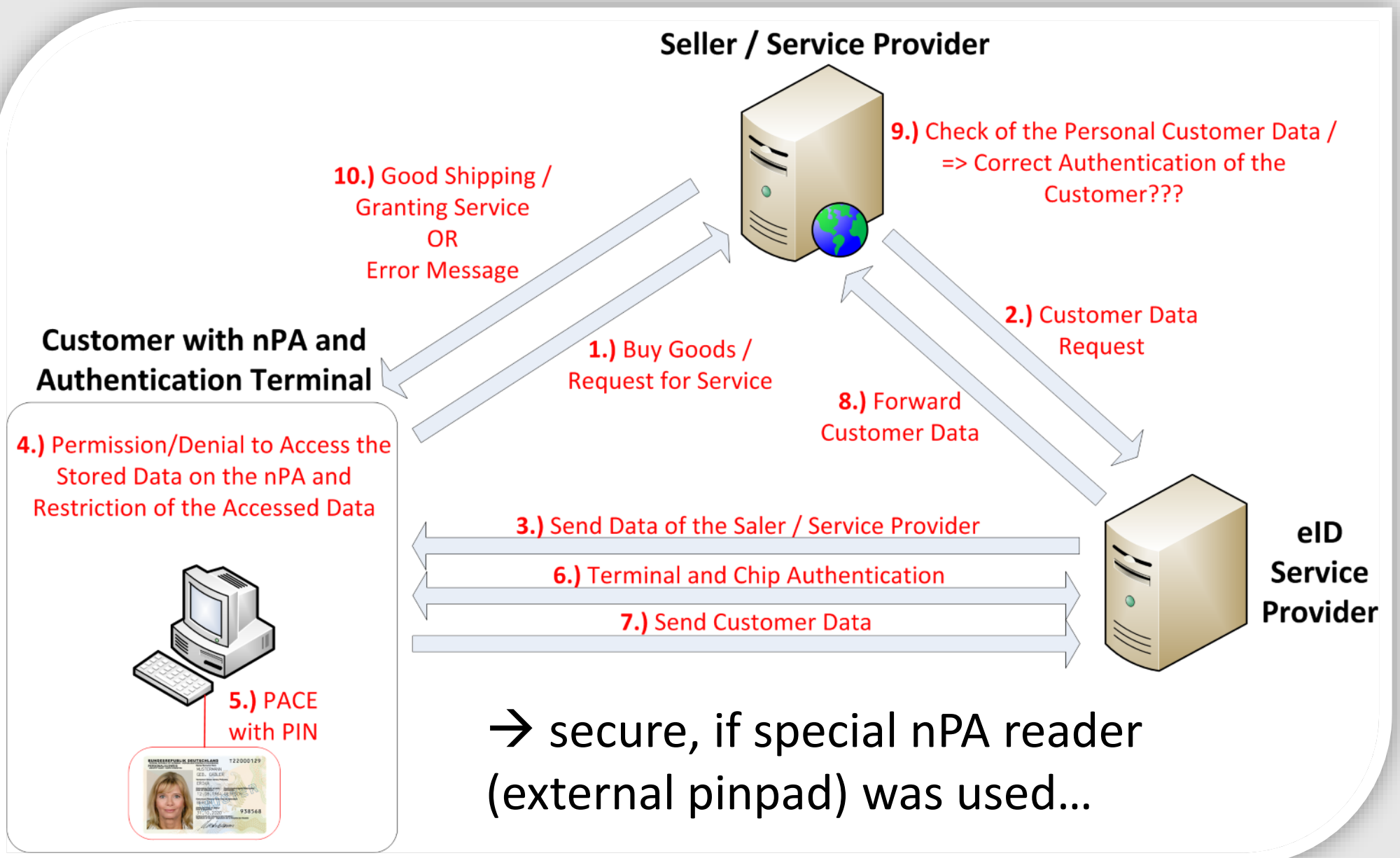
Phase 1: Booking (NFC phone acts as RFID reader)

Two steps:

1. customer identification
2. obtaining a right (credential)



Booking 1/2
Customer Identification

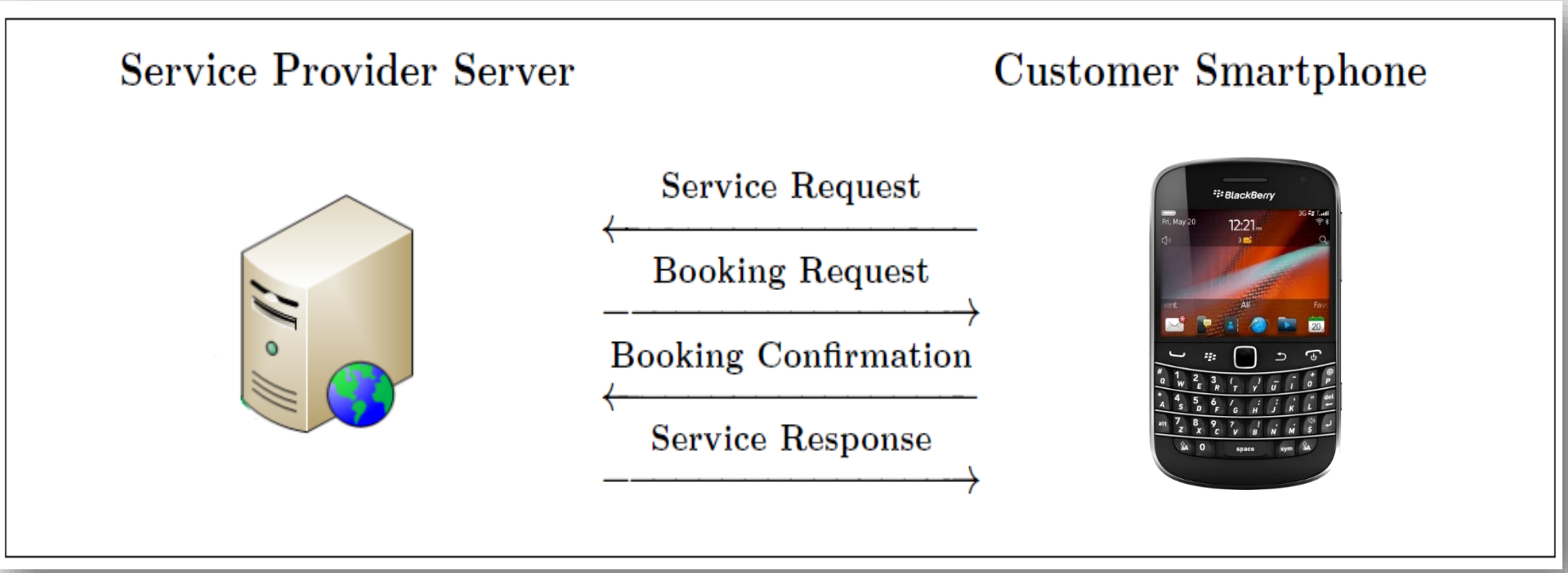


→ secure, if special nPA reader (external pinpad) was used…

Booking 2/2
Obtaining a Right (Credential)

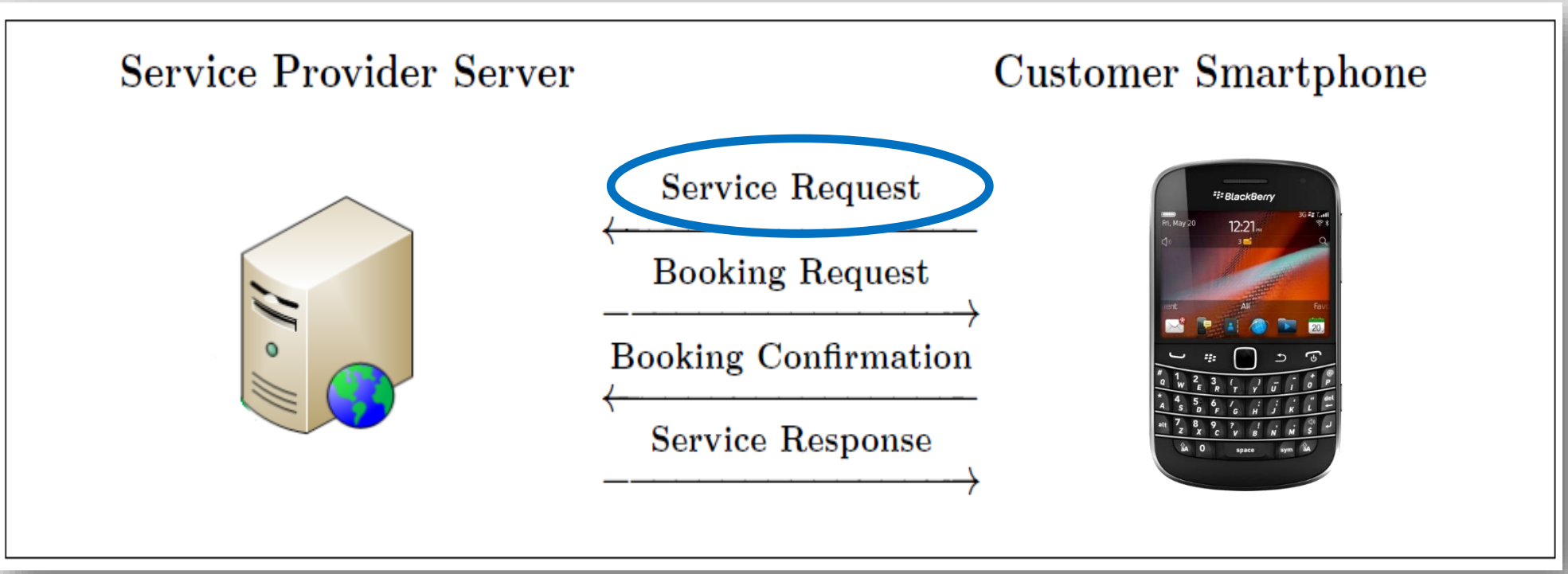
- customer is identified, let‘s book s.th. !
- communication secured with TLS (assumption: TLS is secure …)

- four steps:



Booking 2/2
Obtaining a Right (Credential)

- service information I_{SReq} (e.g., GPS position of phone)
- customer ID ID_C
- random nonce N_C
- time stamp ts_{SReq}



Booking 2/2
Obtaining a Right (Credential)

- service information I_{SReq} (e.g., GPS position of phone)
- customer ID ID_C
- random nonce N_C
- time stamp ts_{SReq}

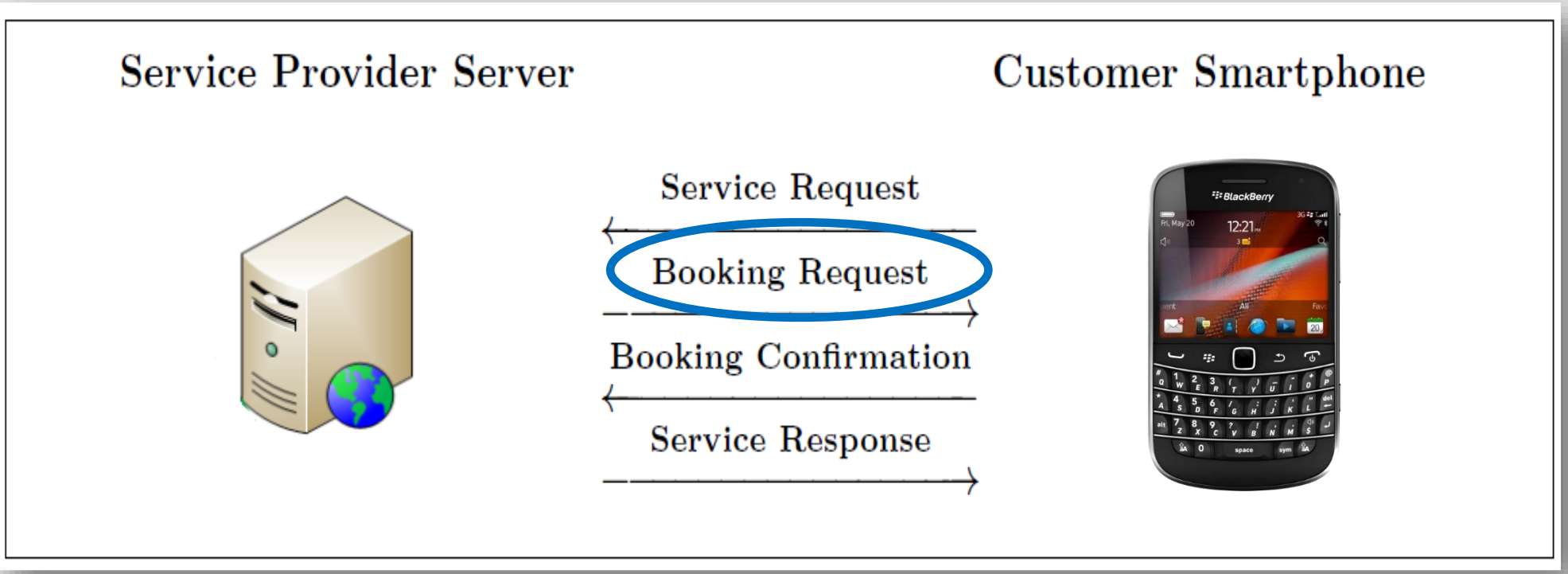
$$\mathrm{h_{SReq}} := \mathrm{hash}(\mathrm{I_{SReq}} \,||\, \mathrm{ID_C} \,||\, \mathrm{N_C} \,||\, \mathrm{ts_{SReq}})$$

$$\mathrm{t_{SReq}} := \mathrm{sign}_{\mathrm{sk_C}}(\mathrm{h_{SReq}})$$

$$\mathrm{p_{SReq}} := \mathrm{encrypt}_{\mathrm{pk_{SP}}}(\mathrm{I_{SReq}} \,||\, \mathrm{N_C} \,||\, \mathrm{ts_{SReq}} \,||\, \mathrm{t_{SReq}})$$

Booking 2/2
Obtaining a Right (Credential)

- service information I_{BReq} (e.g., GPS position of car …)
- unique service object information UI_{BReq} (e.g., car ID)
- modified nonce N_C‘
- time stamp ts_{BReq}



Booking 2/2
Obtaining a Right (Credential)

- service information I_{BReq} (e.g., GPS position of car …)
- unique service object information UI_{BReq} (e.g., car ID)
- modified nonce N_C‘
- time stamp ts_{BReq}

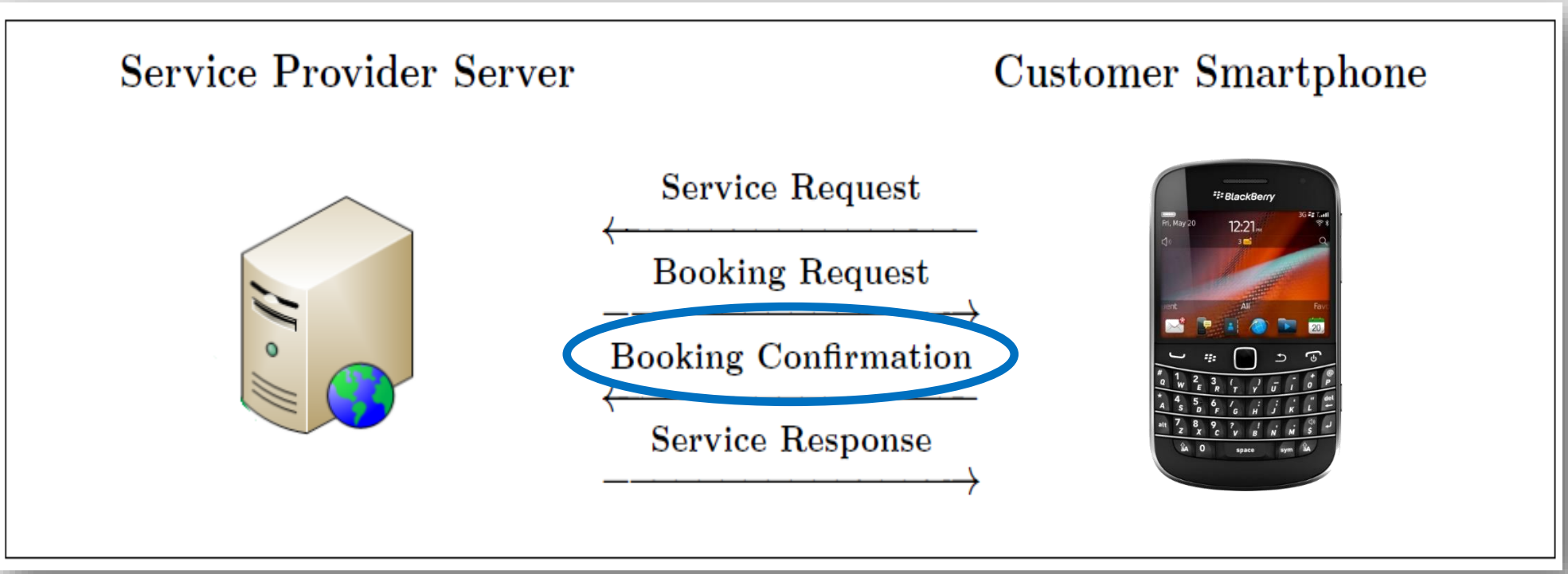
$$\mathrm{h_{BReq}} := \mathrm{hash}(\mathrm{I_{BReq}} \,||\, \mathrm{UI_{BReq}} \,||\, \mathrm{N_C'} \,||\, \mathrm{ts_{BReq}})$$

$$\mathrm{t_{BReq}} := \mathrm{sign}_{\mathrm{sk_{SP}}}(\mathrm{h_{BReq}})$$

$$\mathrm{p_{BReq}} := \mathrm{encrypt}_{\mathrm{pk_C}}(\mathrm{I_{BReq}} \,||\, \mathrm{UI_{BReq}} \,||\, \mathrm{N_C'} \,||\, \mathrm{ts_{BReq}} \,||\, \mathrm{t_{BReq}})$$

Booking 2/2
Obtaining a Right (Credential)

- service information I_{BReq}
- unique service object information UI_{BReq}
- (more) modified nonce N_C“
- time stamp ts_{BCon}



Booking 2/2
Obtaining a Right (Credential)

- service information I_{BReq}
- unique service object information UI_{BReq}
- (more) modified nonce N_C“
- time stamp ts_{BCon}

$$\mathrm{h_{BCon}} := \mathrm{hash}(\mathrm{I_{BReq}} \,||\, \mathrm{UI_{BReq}} \,||\, \mathrm{N_C"} \,||\, \mathrm{ts_{BCon}})$$

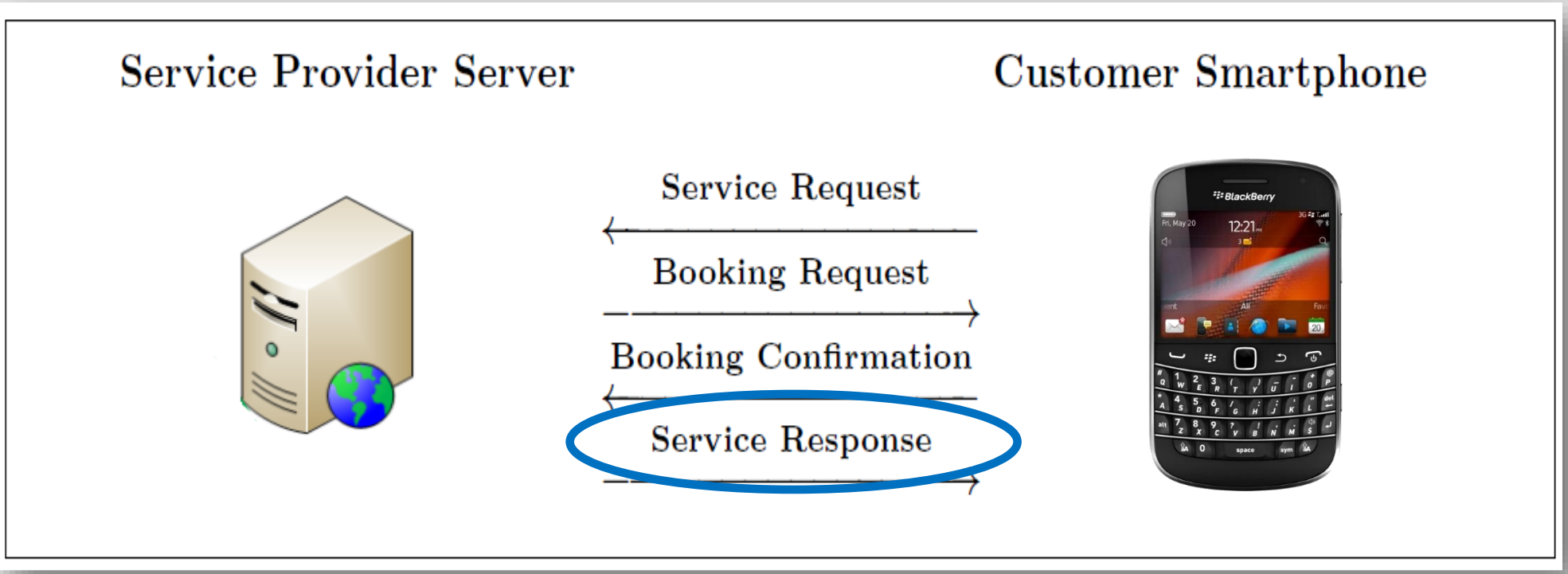
$$\mathrm{t_{BCon}} := \mathrm{sign}_{\mathrm{sk_C}}(\mathrm{h_{BCon}})$$

$$\mathrm{p_{BCon}} := \mathrm{encrypt}_{\mathrm{pk_{SP}}}(\mathrm{I_{BReq}} \,||\, \mathrm{UI_{BReq}} \,||\, \mathrm{N_C"} \,||\, \mathrm{ts_{BCon}} \,||\, \mathrm{t_{BCon}})$$

Booking 2/2
Obtaining a Right (Credential)

- Create **service credential** from:

information I_{SC}, (even more) modified nonce N_C‘‘, unique service object information UI_{SC}, time stamp ts_{SC}, *Authentication Key, and encrypted user rights credential*



Booking 2/2
Obtaining a Right (Credential)

- Create **service credential** from:

information I_{SC}, (even more) modified nonce N_C‘‘, unique service object information UI_{SC}, time stamp ts_{SC}, *Authentication Key, and encrypted User Rights Credential*

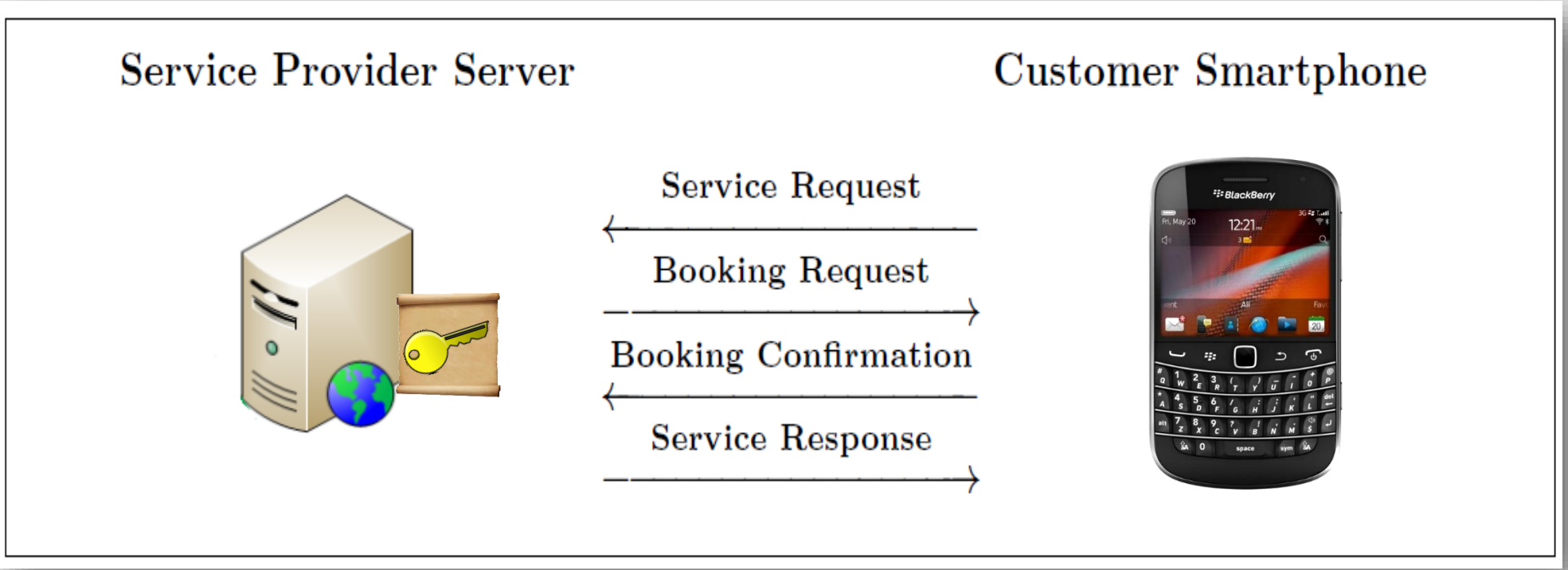
$$\mathrm{h_{SC}} := \mathrm{hash}(\texttt{Service Credential})$$

$$\mathrm{t_{SC}} := \mathrm{sign}_{\mathrm{sk_{SP}}}(\mathrm{h_{SC}})$$

$$\mathrm{p_{SC}} := \mathrm{encrypt}_{\mathrm{pk_C}}(\texttt{Service Credential} \,||\, \mathrm{t_{SC}})$$

Booking 2/2
Obtaining a Right (Credential)

very easy!



Phase 2: Execute Booked Rights (NFC phone emulates Mifare DESfire)

- *Authentication Key* from service credential is used to secure wireless link (DESfire mutual authentication)
- Decrypt *User Rights Credential* with $\boldsymbol{sk_{SO}}$ and verify its signature with $\boldsymbol{pk_{SP}}$

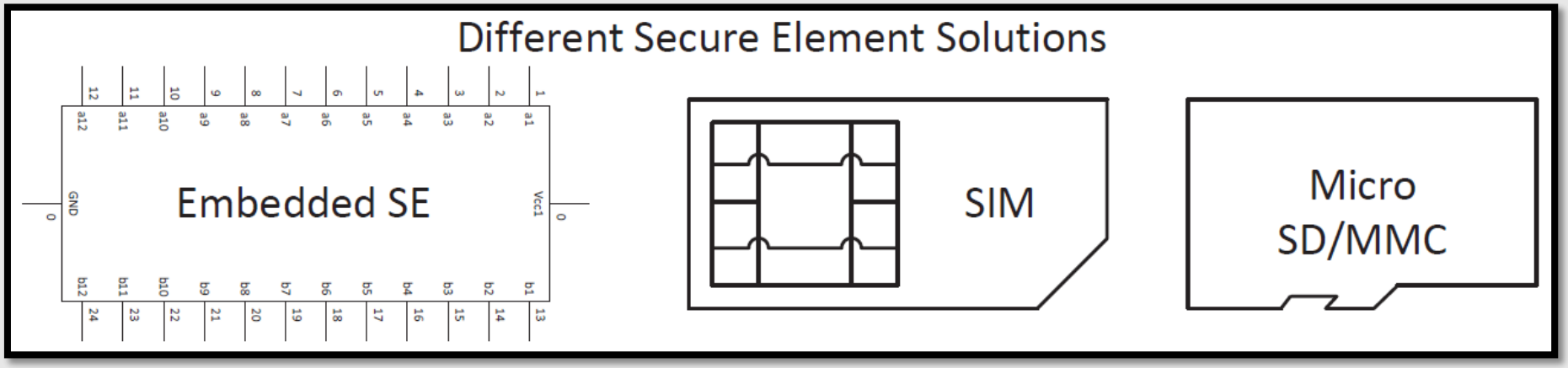
Homework:

Read our paper and find out how the Authentication Key is generated and updated in case of no Internet.

Secure Elements

In Theory: Several options

- Embedded Secure Element (eSE)
- SIM card issued by communication provider
- SE integrated in a (Micro) SD card



In Practice:

- slow (8-bit) and Java
- no access granted ☹

Implementation Obstacles and Security Issues

Software on Smartphone:

- no access to SE → no secure storage
- program main CPU in Java (☹ !!)
- RIM API doesn‘t support nPA elliptic curve (brainpoolP256r1)

nPA:

- No certificate for Terminal Authentication (TA)
- No external pinpad / secure nPA reader

→ Trojan in smartphone OS poses a security threat

Run-Time of PACE

PACE Step / Time	Minimum	Maximum	Average
Communication buildup & MSE:Set AT	124 ms	408 ms	262.11 ms
Encrypt Nonce	68 ms	138 ms	105.17 ms
Map Nonce	1558 ms	1763 ms	1695.32 ms
Perform Key Agreement	1185 ms	1396 ms	1291.57 ms
Mutual Authentication	118 ms	189 ms	147.32 ms
Total PACE	**3268 ms**	**3712 ms**	**3501.49 ms**

Summary

- Concept for secure rights management with NFC
- Smartphone application for booking via TLS

- NFC phone as RFID reader realizes eID function of nPA
  (ECDHKE *in Java …)*

- NFC phone emulates Mifare DESfire card to open car

- some remaining security issues discussed

Thank you!

Questions?

timo.kasper@rub.de

hgi EMSEC
RUHR-UNIVERSITÄT BOCHUM
Chair for Embedded Security (Prof. Christof Paar)

www.emsec.rub.de

KASPER OSWALD
Ingenieure für innovative Sicherheitslösungen

www.kasper-oswald.de

secmobil

RUHR-UNIVERSITÄT BOCHUM

RUB

Security for eMobility: Project SecMobil

secmobil Partners

RUB

escrypt Embedded Security

DAIMLER

smartlab

if(is) internet-sicherheit.

RUHR UNIVERSITÄT BOCHUM RUB

Associated Partners

BUNDESDRUCKEREI

Bundesamt für Sicherheit in der Informationstechnik

e·on

T··Systems···

·····T··

KASPER OSWALD

Gefördert durch:

Bundesministerium für Wirtschaft und Technologie

aufgrund eines Beschlusses des Deutschen Bundestages

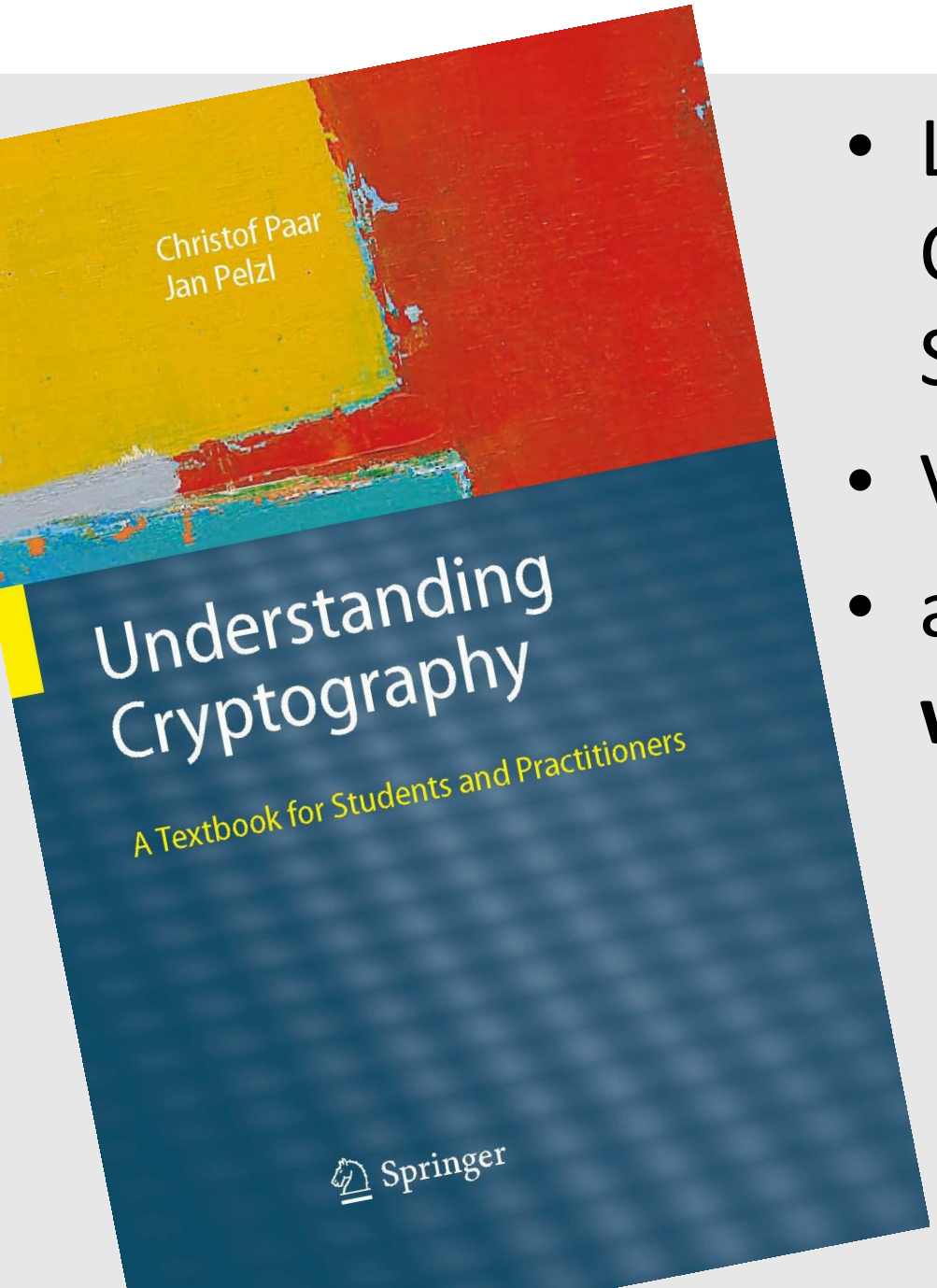
secmobil Goals

- development of a secure energy sensor
- tamper-proof smart metering

- standardized security architecture for electric cars

- privacy and data security
  for end-users and suppliers

Introduction to Cryptography and Data Security



- Lecture „Introduction to Cryptography and Data Security“
- Videos of 2 semesters
- all online: **www.crypto-textbook.com**