Smartphones as Practical and Secure Location Verification Tokens for Payments

Claudio Marforio, Nikolaos Karapanos, Claudio Soriente,
Kari Kostiainen and Srdjan Čapkun

Institute of Information Security, ETH Zurich
{firstname.lastname}@inf.ethz.ch

NDSS'14
San Diego, CA
Feb 24th, 2014

www.technorati.com

money.usnews.com

- **Frauds** for **1.2 billion** Euro in the Single Euro Payments Area [1]
- Counterfeit or stolen cards
- Chip-n-Pin brings better security, but attacks have been found [2]
- 1/4 frauds outside of SEPA targeting **old(er)** terminals

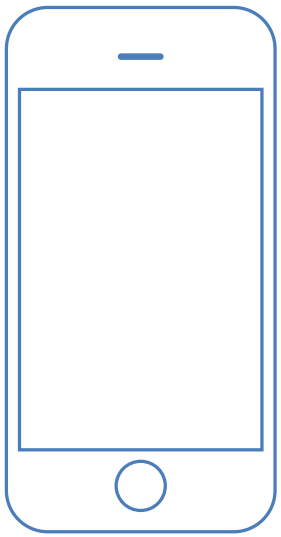
[1] European Central Bank: Report on Card Fraud (2012)
http://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201207en.pdf
[2] M. Bond et al., Chip and Skim: cloning EMV cards with the pre-play attack http://arxiv.org/abs/1209.2531

Goals

Second Factor Authentication for payments at PoS

- **No** need for dedicated hardware tokens (impractical)
- **No** changes to user experience (impractical)
- **No** changes hardware/software changes to the PoS infrastructure (slow/expensive)

Location-based Second Factor Authentication



[1] F. S. Park, C. Gangakhedkar, and P. Traynor, "Leveraging cellular infrastructure to improve fraud prevention", ACSAC'09

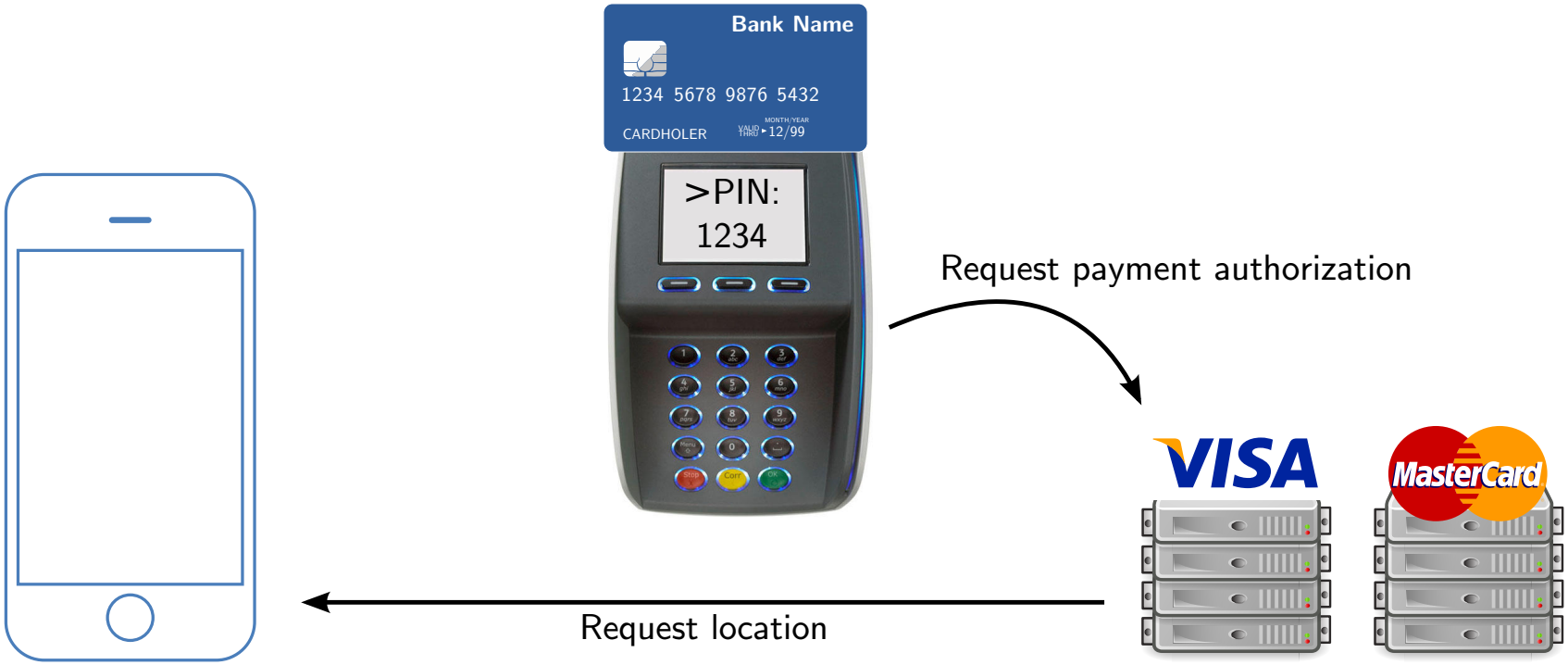
[2] P. Fourez and Mastercard International Inc., "Location controls on payment card transactions", Patent No. WO/2011/022062, 2011.

Location-based Second Factor Authentication

[1] F. S. Park, C. Gangakhedkar, and P. Traynor, "Leveraging cellular infrastructure to improve fraud prevention", ACSAC'09

[2] P. Fourez and Mastercard International Inc., "Location controls on payment card transactions", Patent No. WO/2011/022062, 2011.

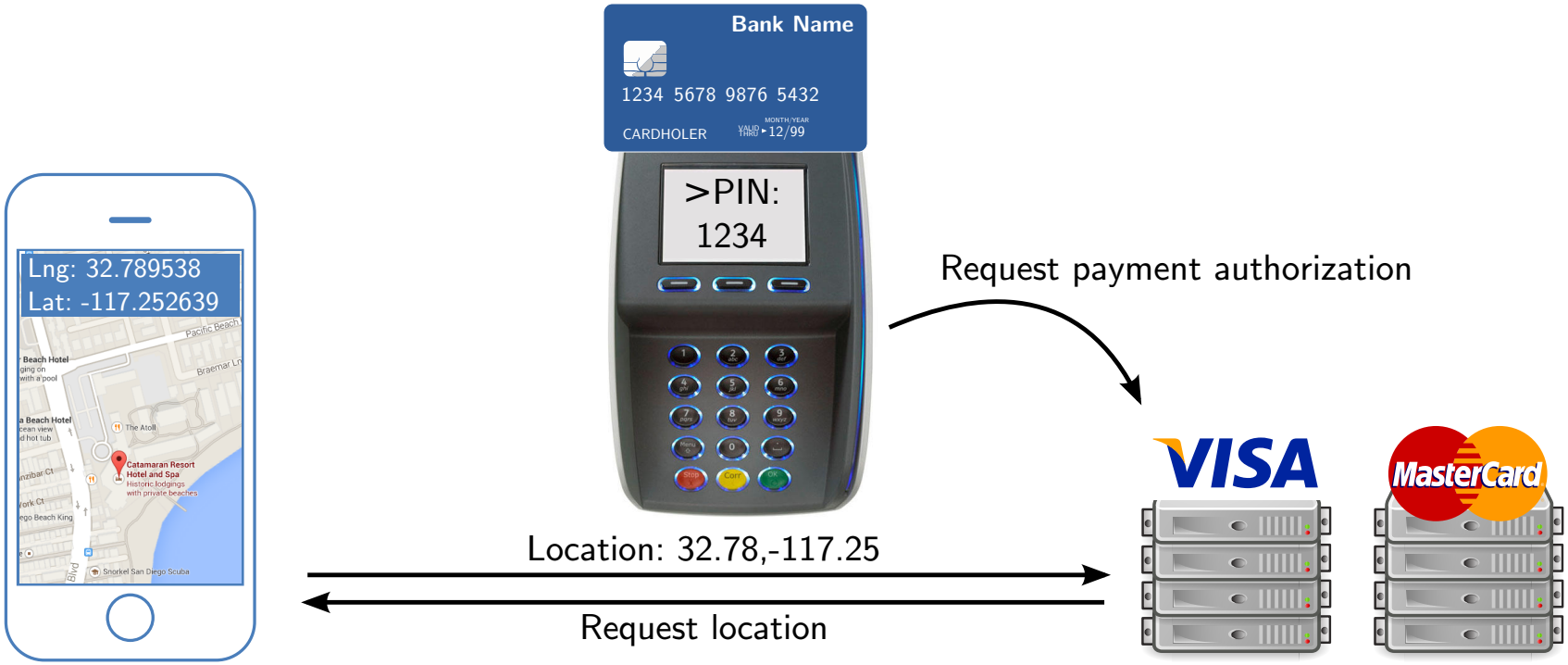
Location-based Second Factor Authentication



[1] F. S. Park, C. Gangakhedkar, and P. Traynor, "Leveraging cellular infrastructure to improve fraud prevention", ACSAC'09

[2] P. Fourez and Mastercard International Inc., "Location controls on payment card transactions", Patent No. WO/2011/022062, 2011.

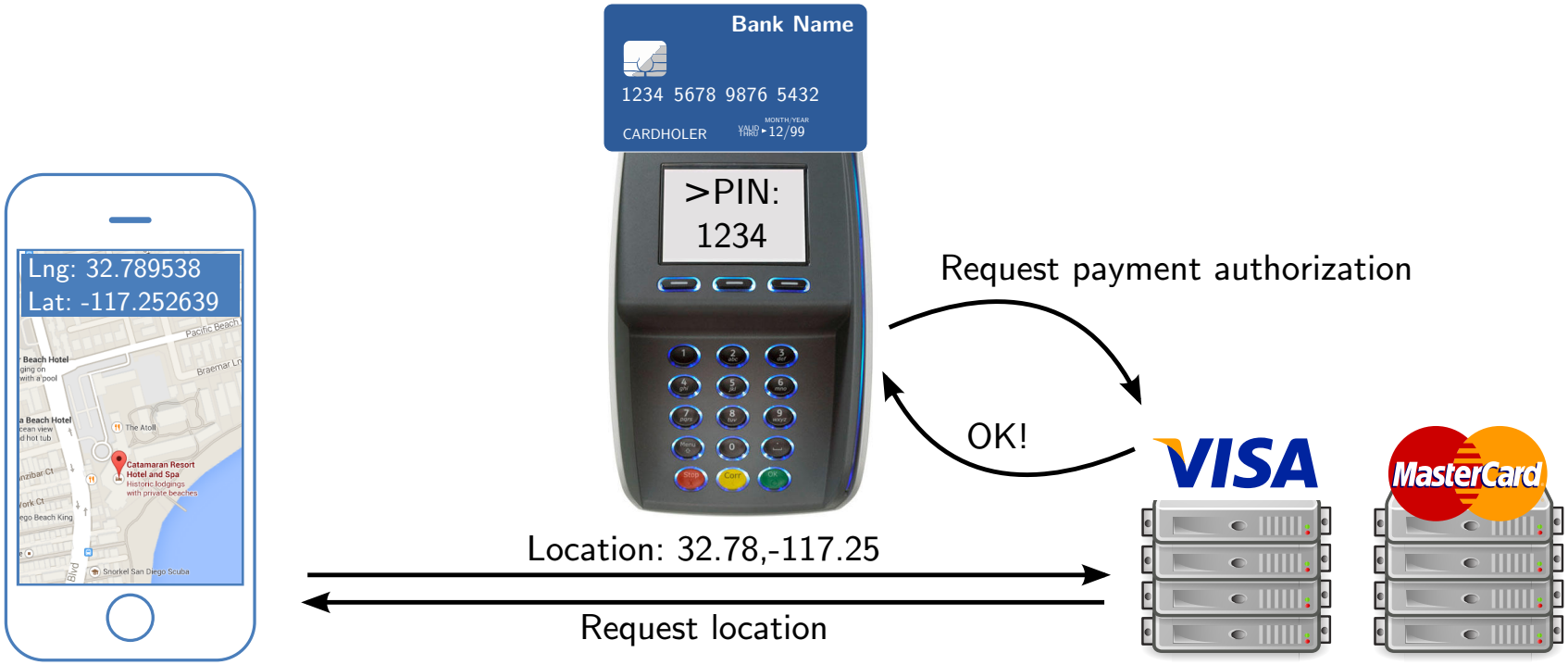
Location-based Second Factor Authentication



[1] F. S. Park, C. Gangakhedkar, and P. Traynor, "Leveraging cellular infrastructure to improve fraud prevention", ACSAC'09

[2] P. Fourez and Mastercard International Inc., "Location controls on payment card transactions", Patent No. WO/2011/022062, 2011.

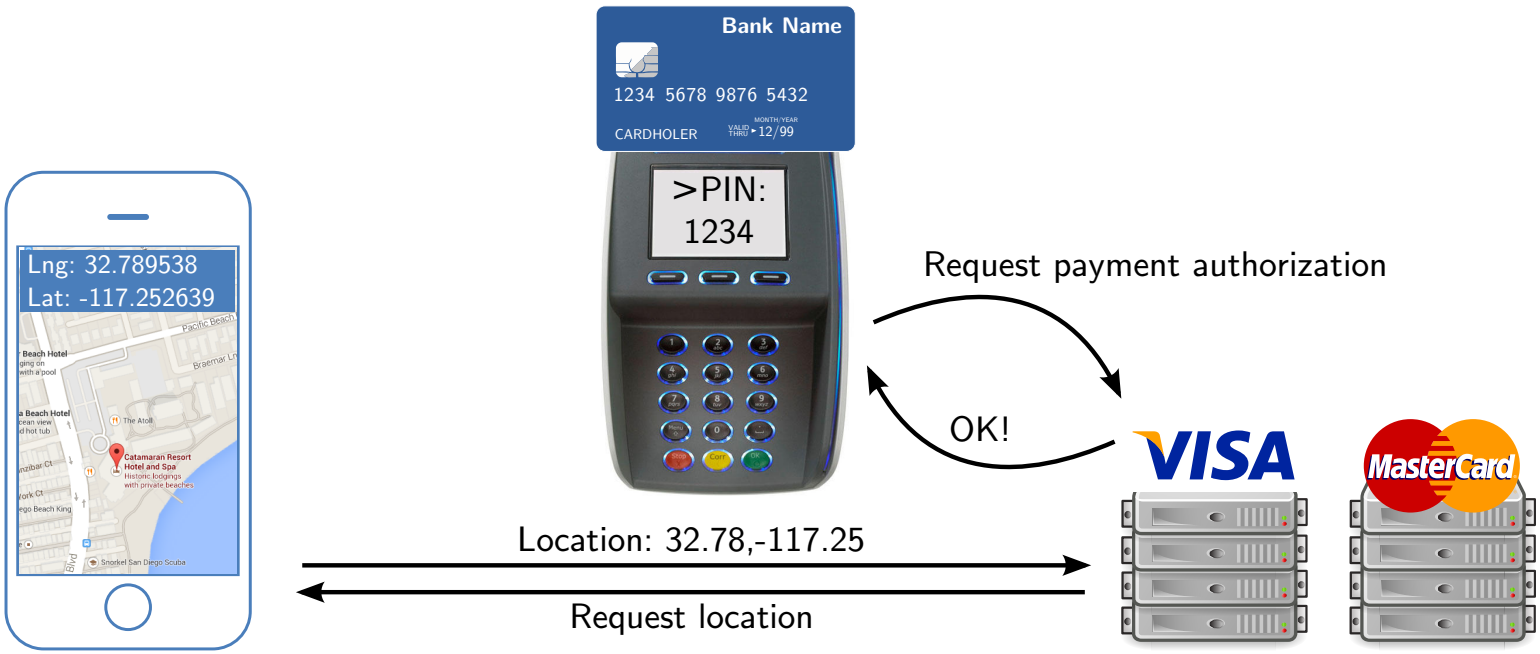
Location-based Second Factor Authentication



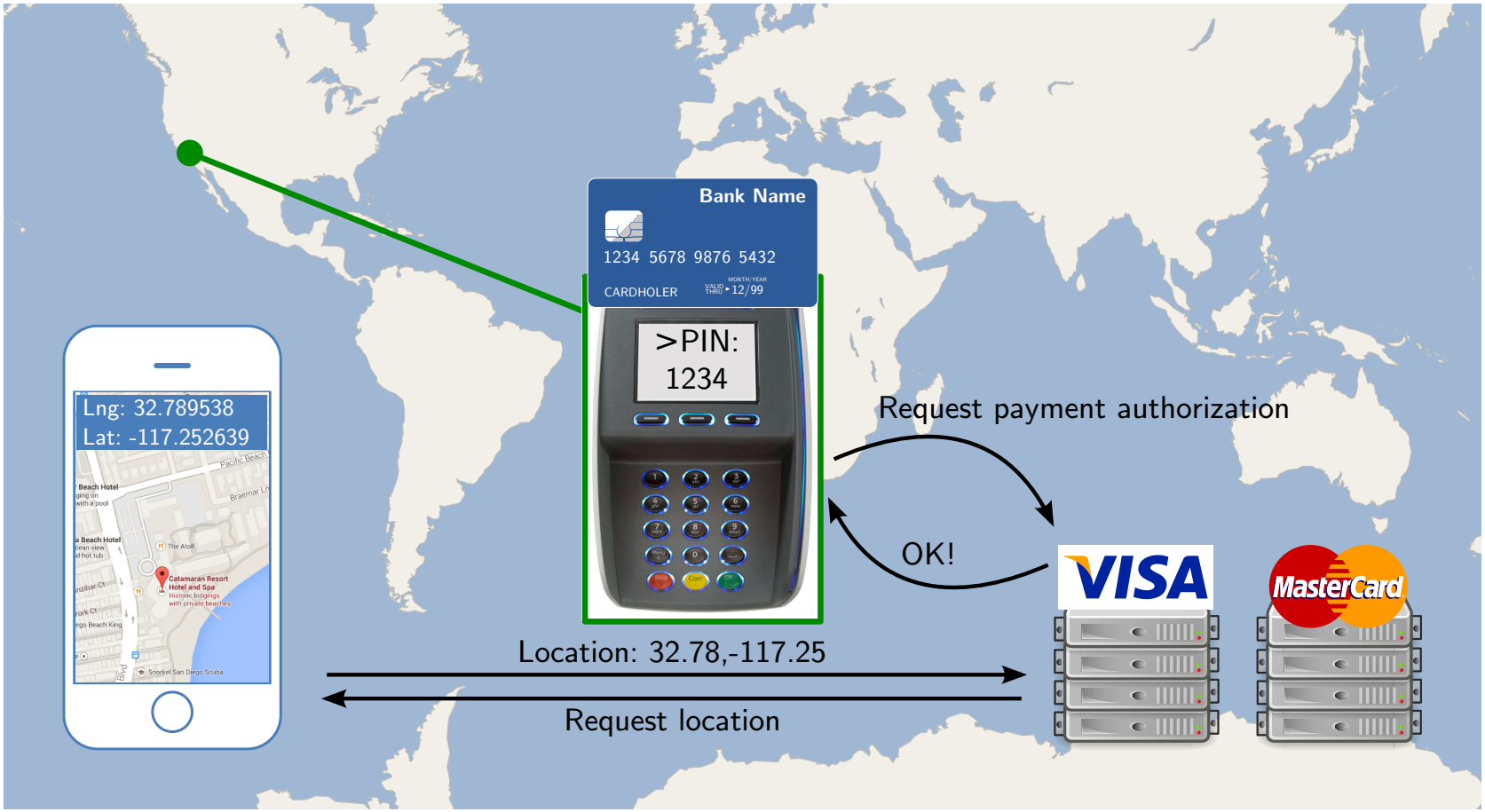
[1] F. S. Park, C. Gangakhedkar, and P. Traynor, "Leveraging cellular infrastructure to improve fraud prevention", ACSAC'09

[2] P. Fourez and Mastercard International Inc., "Location controls on payment card transactions", Patent No. WO/2011/022062, 2011.

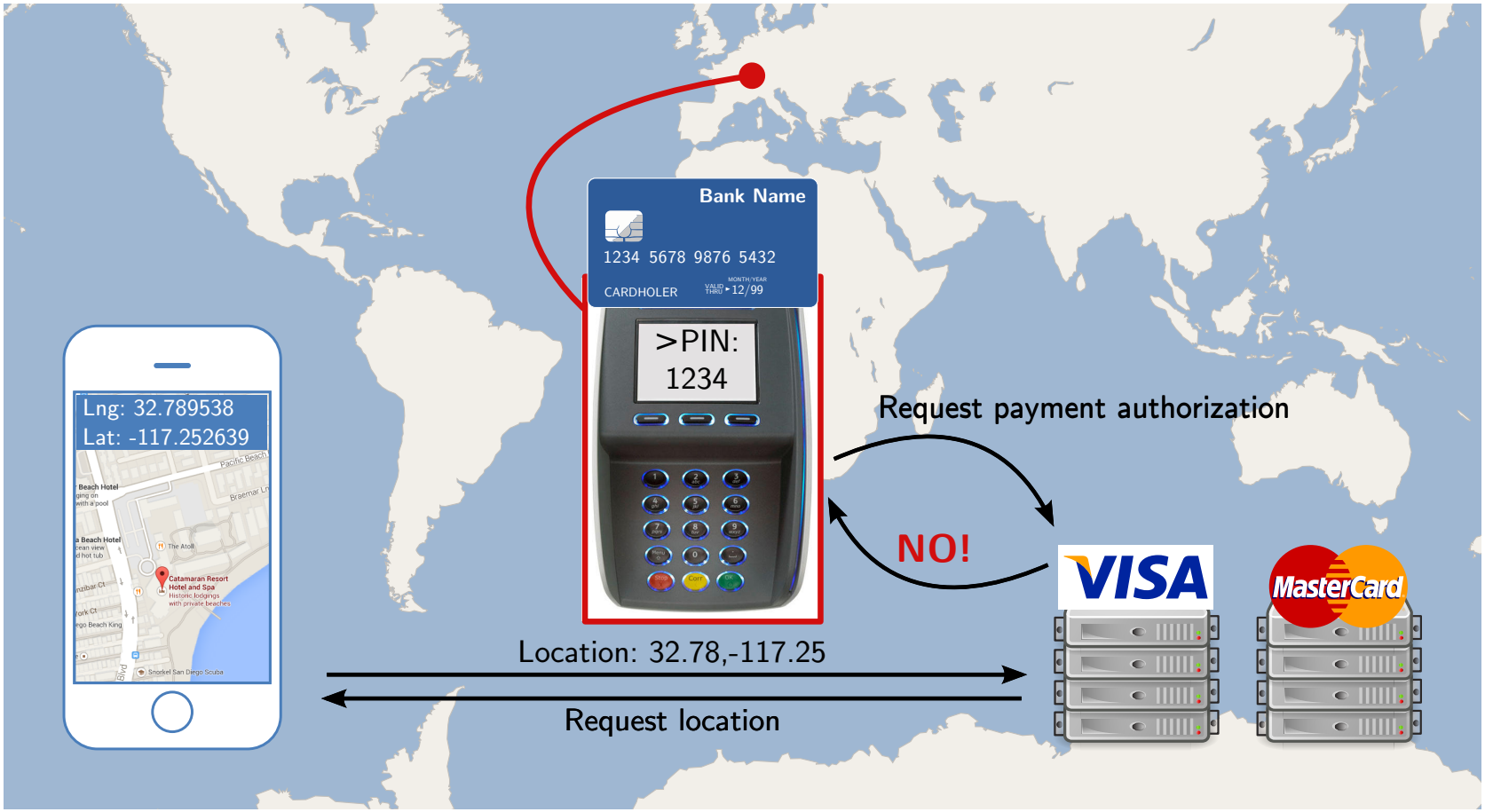
Secure?


Bank Name
1234 5678 9876 5432
CARDHOLER
VALID THRU 12/99
>PIN:
1234
Lng: 32.789538
Lat: -117.252639
Request payment authorization
OK!
VISA
MasterCard
Location: 32.78,-117.25
Request location

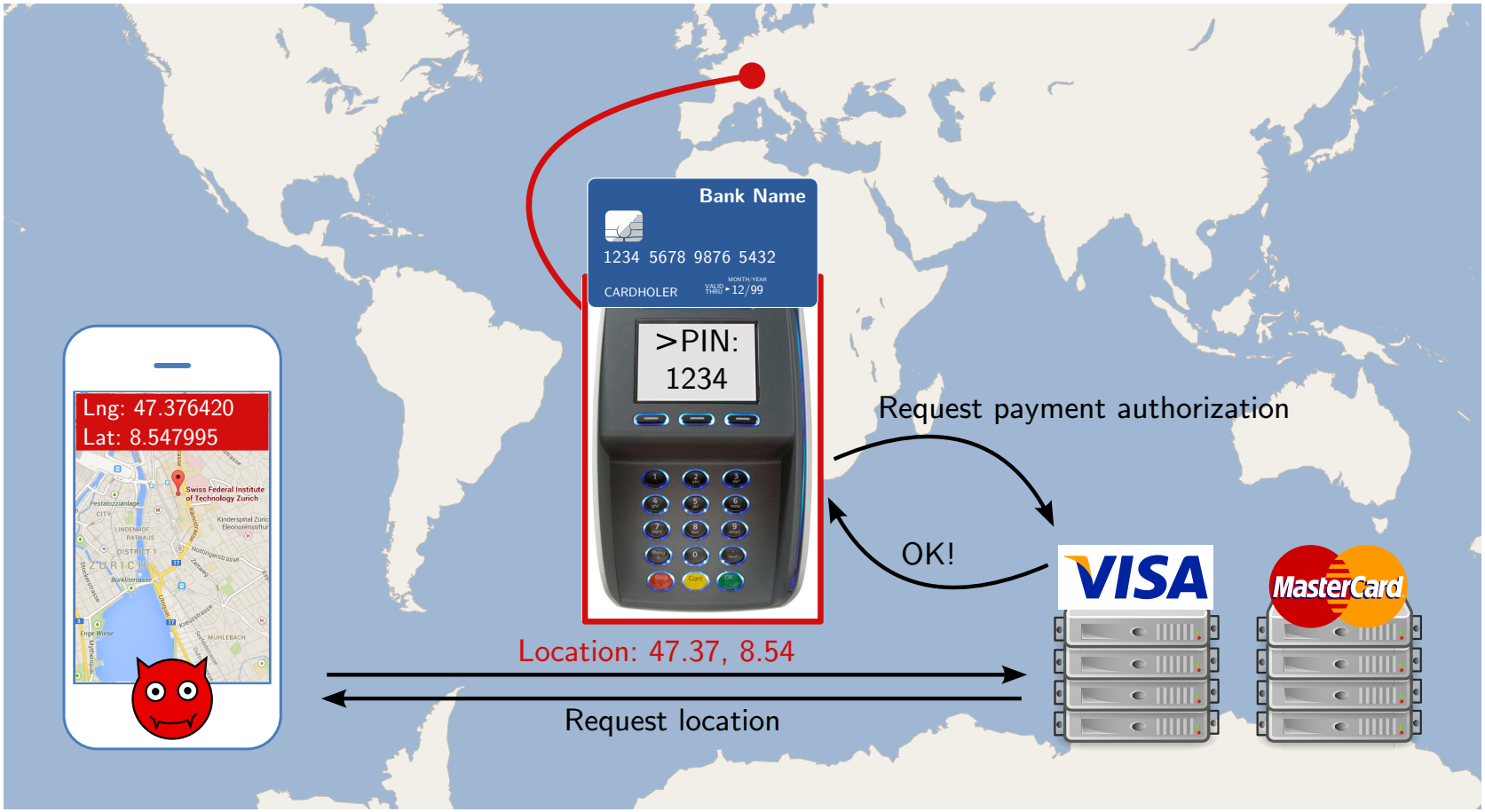
Secure?


Bank Name
1234 5678 9876 5432
CARDHOLER
VALID THRU 12/99
>PIN:
1234
Lng: 32.789538
Lat: -117.252639
Request payment authorization
OK!
VISA
MasterCard
Location: 32.78,-117.25
Request location

Secure?

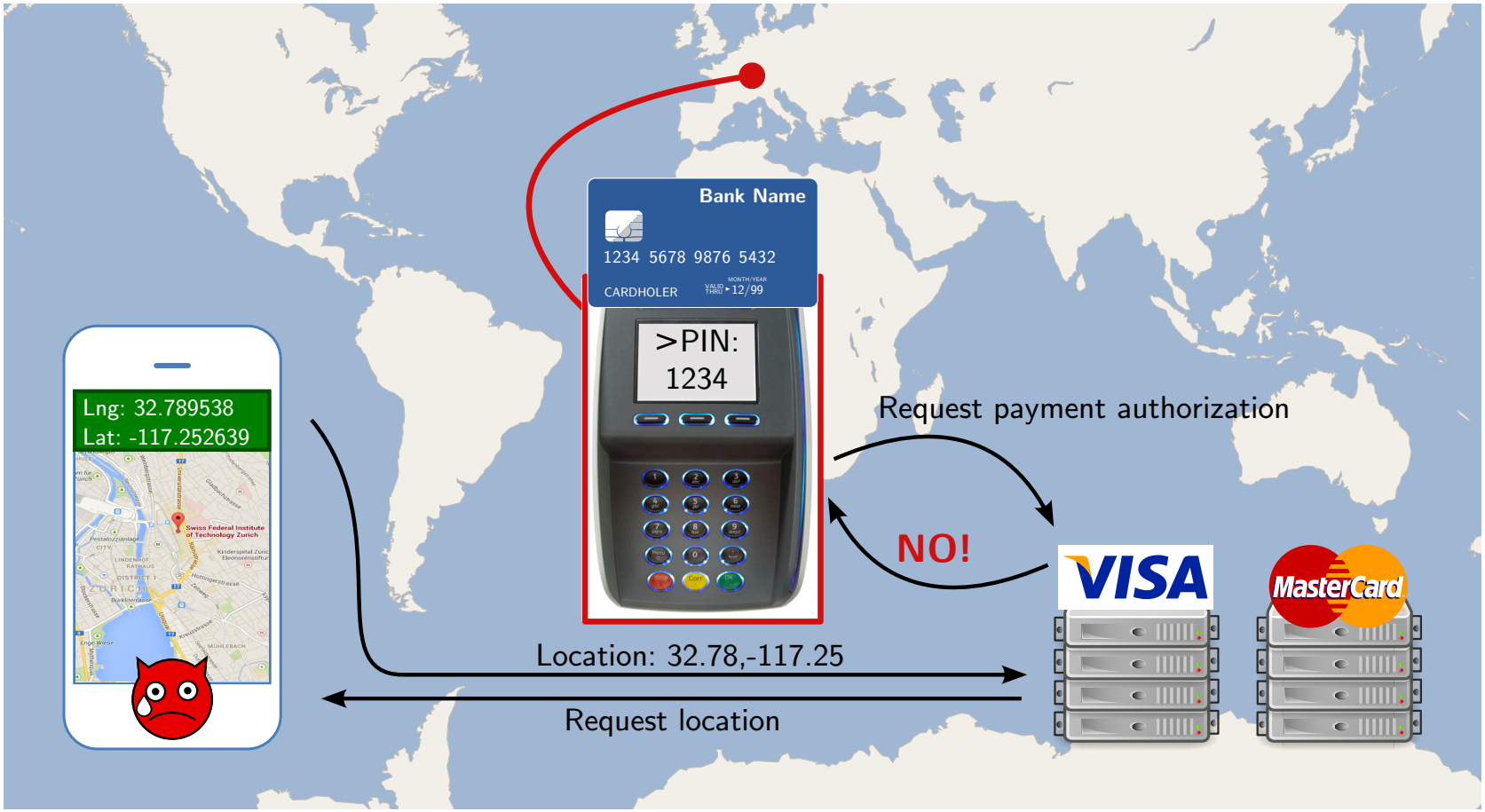

Bank Name
1234 5678 9876 5432
CARDHOLER
VALID THRU 12/99
>PIN:
1234
Lng: 32.789538
Lat: -117.252639
Request payment authorization
NO!
VISA
MasterCard
Location: 32.78,-117.25
Request location

Secure?



→ An attacker that controls the victim's mobile OS can forge the GPS coordinates

Secure?

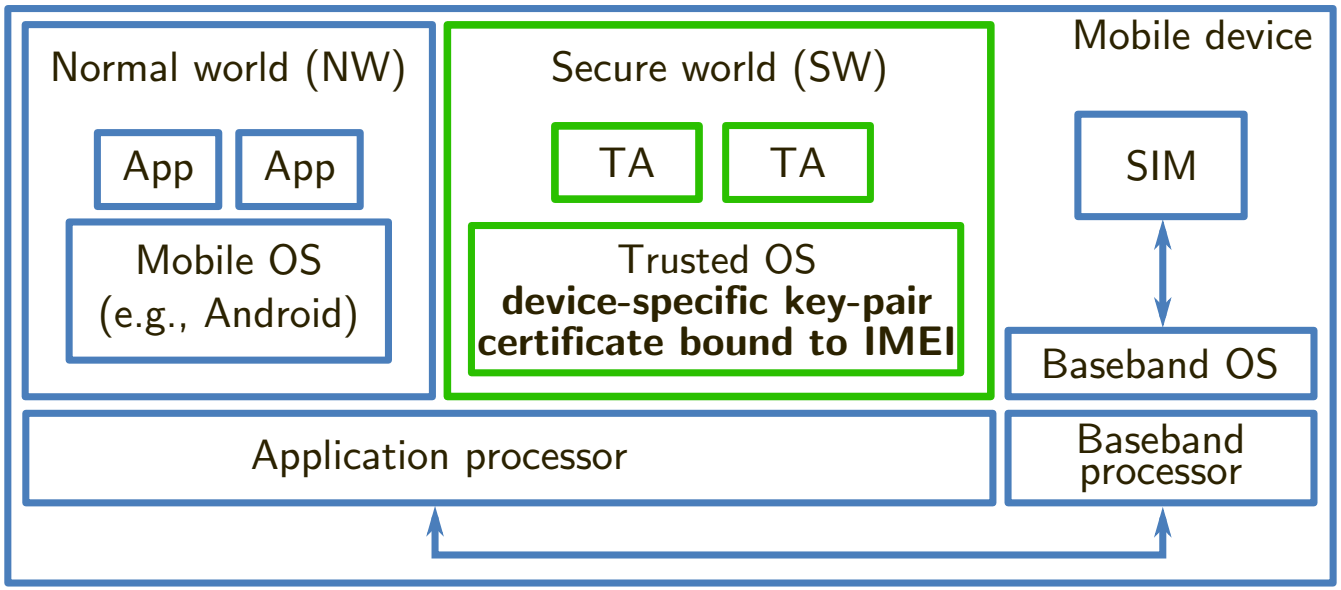


→ Trusted Execution Environments (TEEs) can generate GPS location statements that the attacker cannot change!

Contributions

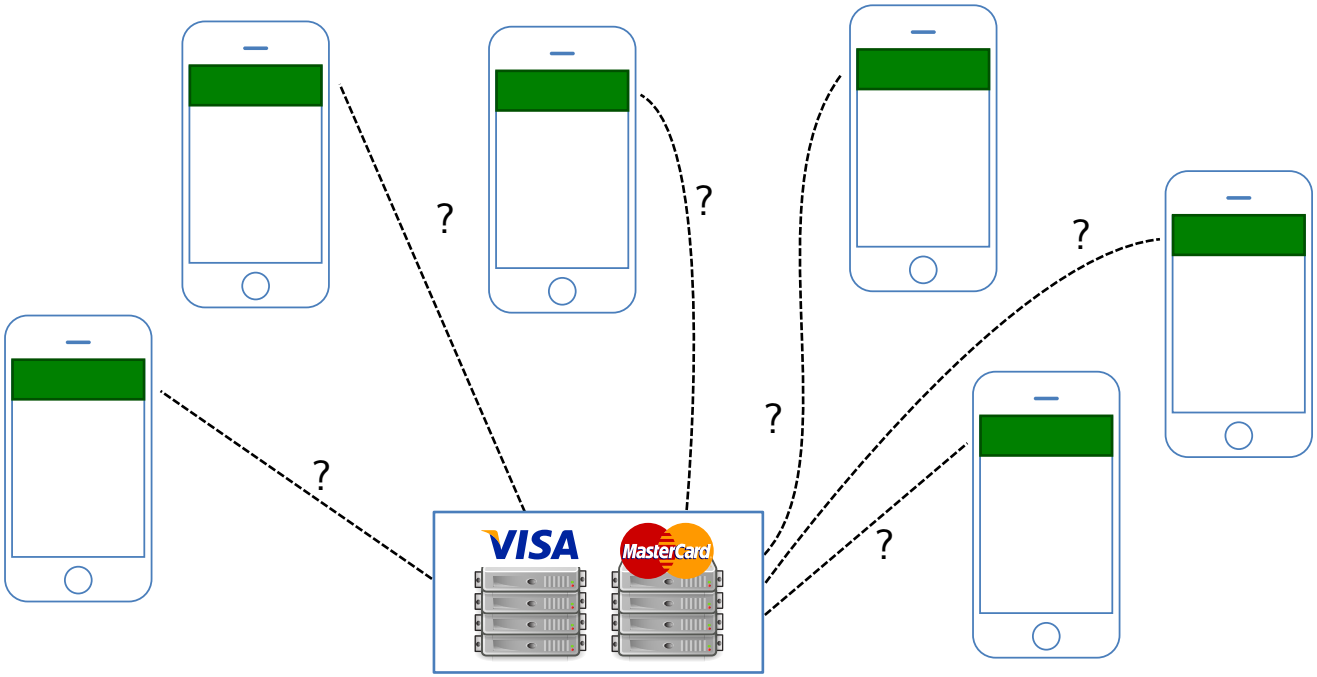
1. **secure** smartphone-based second-factor authentication solution for payments at PoS leveraging a TrustZone-aware phone's reported **location**
2. two novel secure (against different attacker models) **enrollment schemes** supporting easy migration
3. prototype and evaluate the **ease of deployment** and **effectiveness** of our solution
4. show applicability to different application scenarios (buildings access, transportation, . . .)
5. integration of our solution into the EMV standard

ARM TrustZone



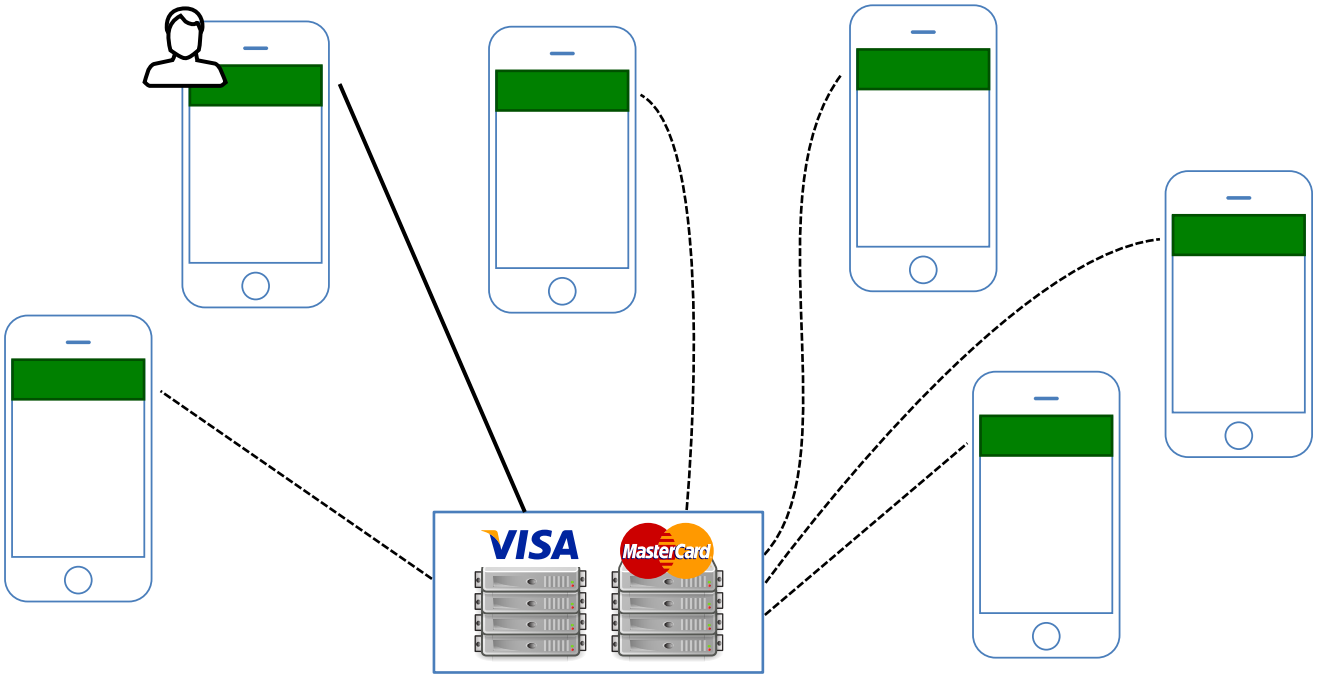
- Hardware **supported** and **enforced** security
- Resources partitioned across the entire system in two states or worlds **Secure** and **Normal** World
- Run (part of) an application in isolation from the rest of the system
- Design principle: keep the **Secure World** as **small** as possible

The Problem of Secure Enrollment



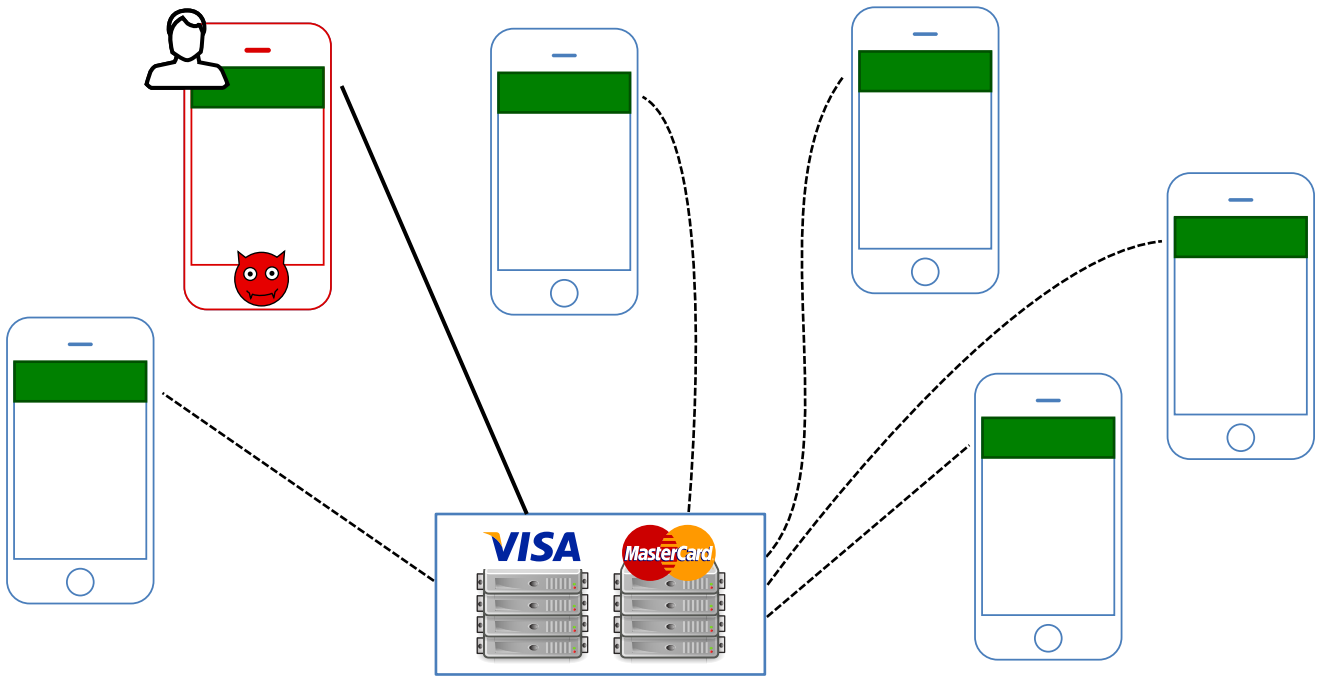
- Establish an authentic channel

The Problem of Secure Enrollment



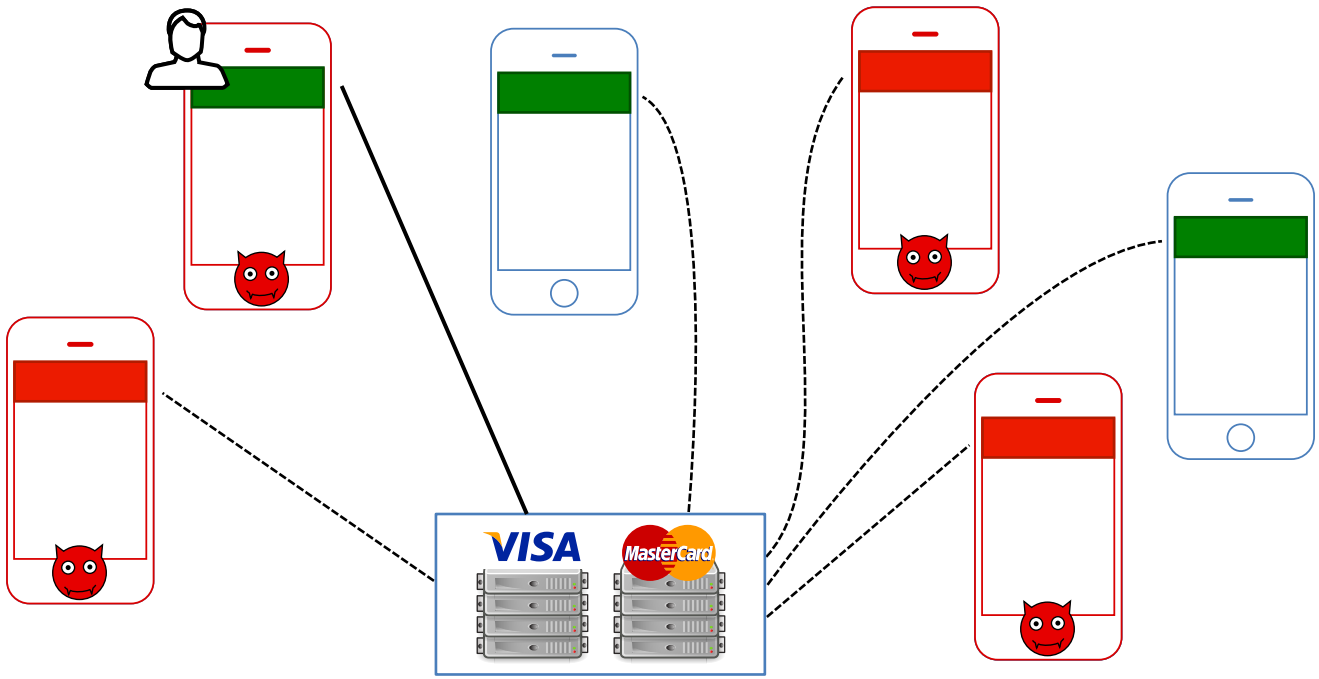
- Establish an authentic channel
- With the correct user's device TEE

The Problem of Secure Enrollment



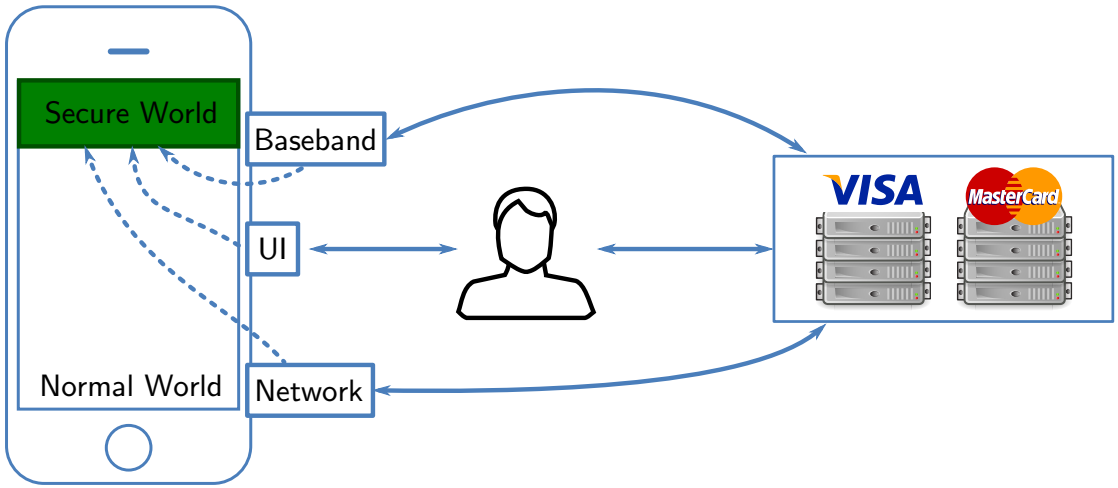
- Establish an authentic channel
- With the correct user's device TEE
- In the presence of an adversary that controls the victim's device

The Problem of Secure Enrollment



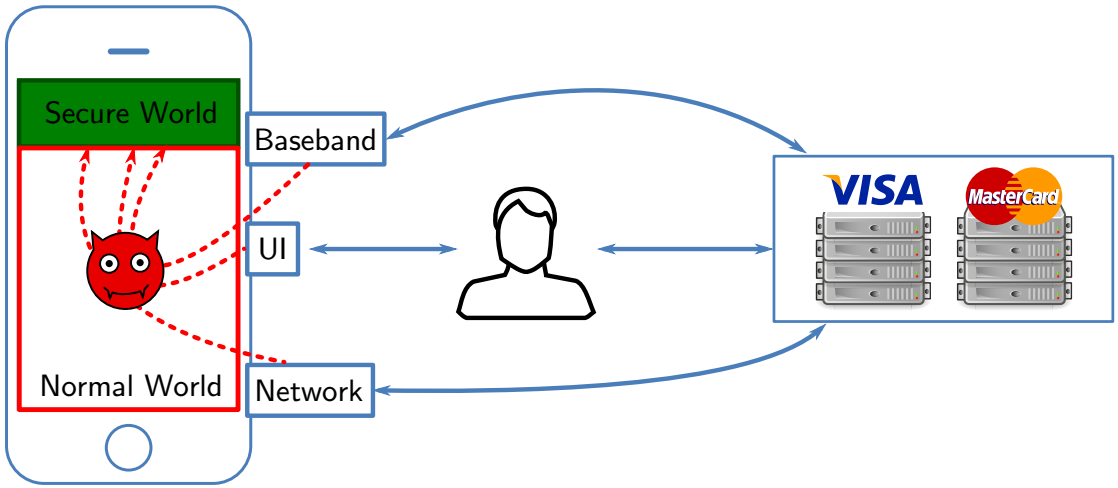
- Establish an authentic channel
- With the correct user's device TEE
- In the presence of an adversary that controls the victim's device
- And potentially other devices

The Problem of Secure Enrollment (II)



- All the communication to the Secure World is **mediated** by the Normal World

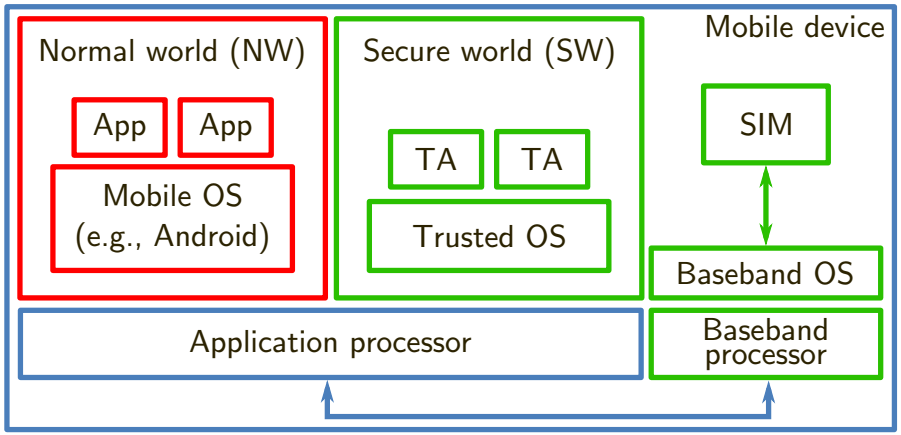
The Problem of Secure Enrollment (II)



- All the communication to the Secure World is **mediated** by the Normal World
- Potentially controlled by an attacker

Attacker Model

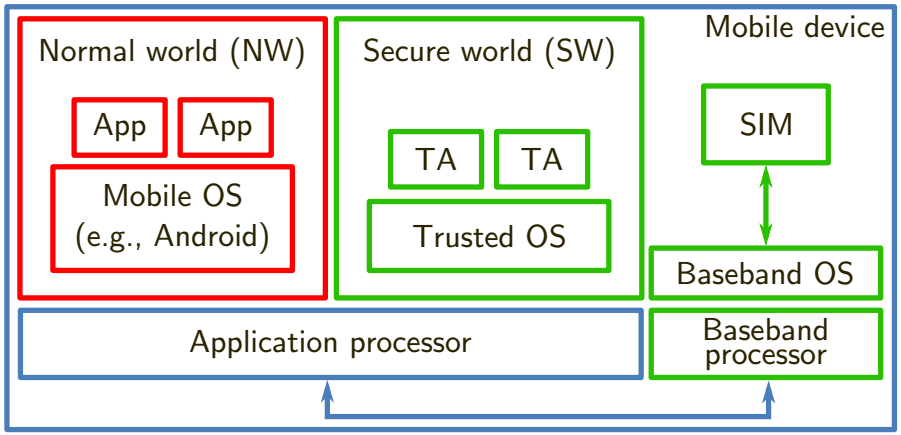
Victim's Device



- Remote compromise
- Normal World is completely controlled by the attacker

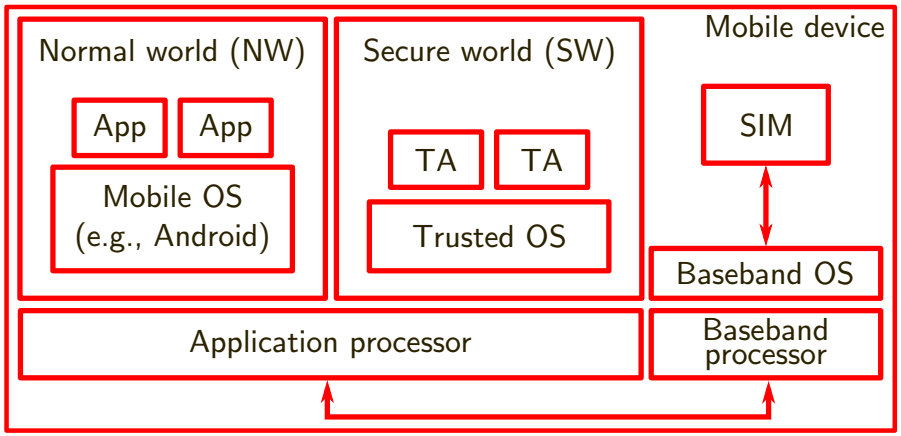
Attacker Model

Victim's Device



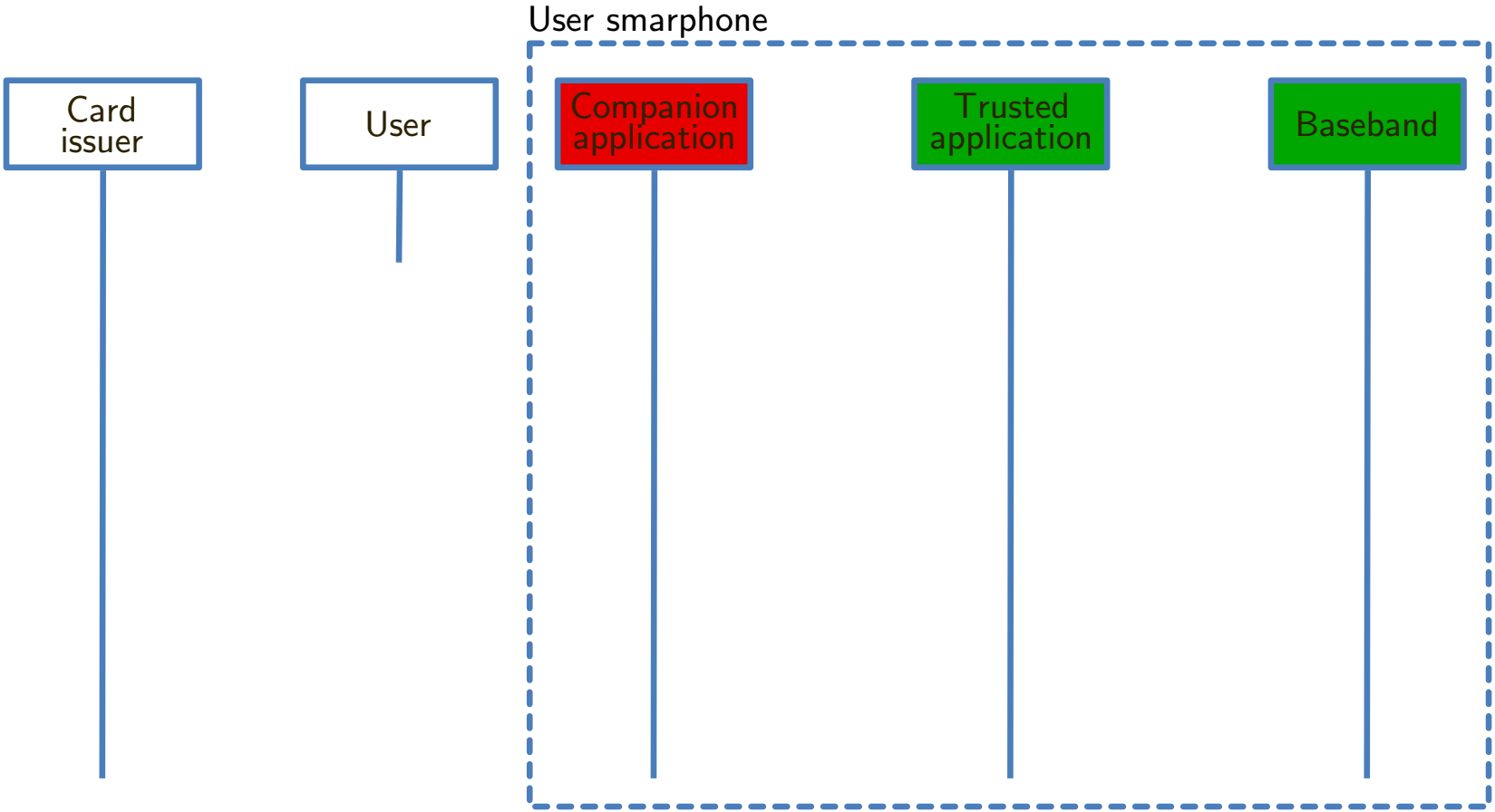
- Remote compromise
- Normal World is completely controlled by the attacker

Attacker's Device(s)

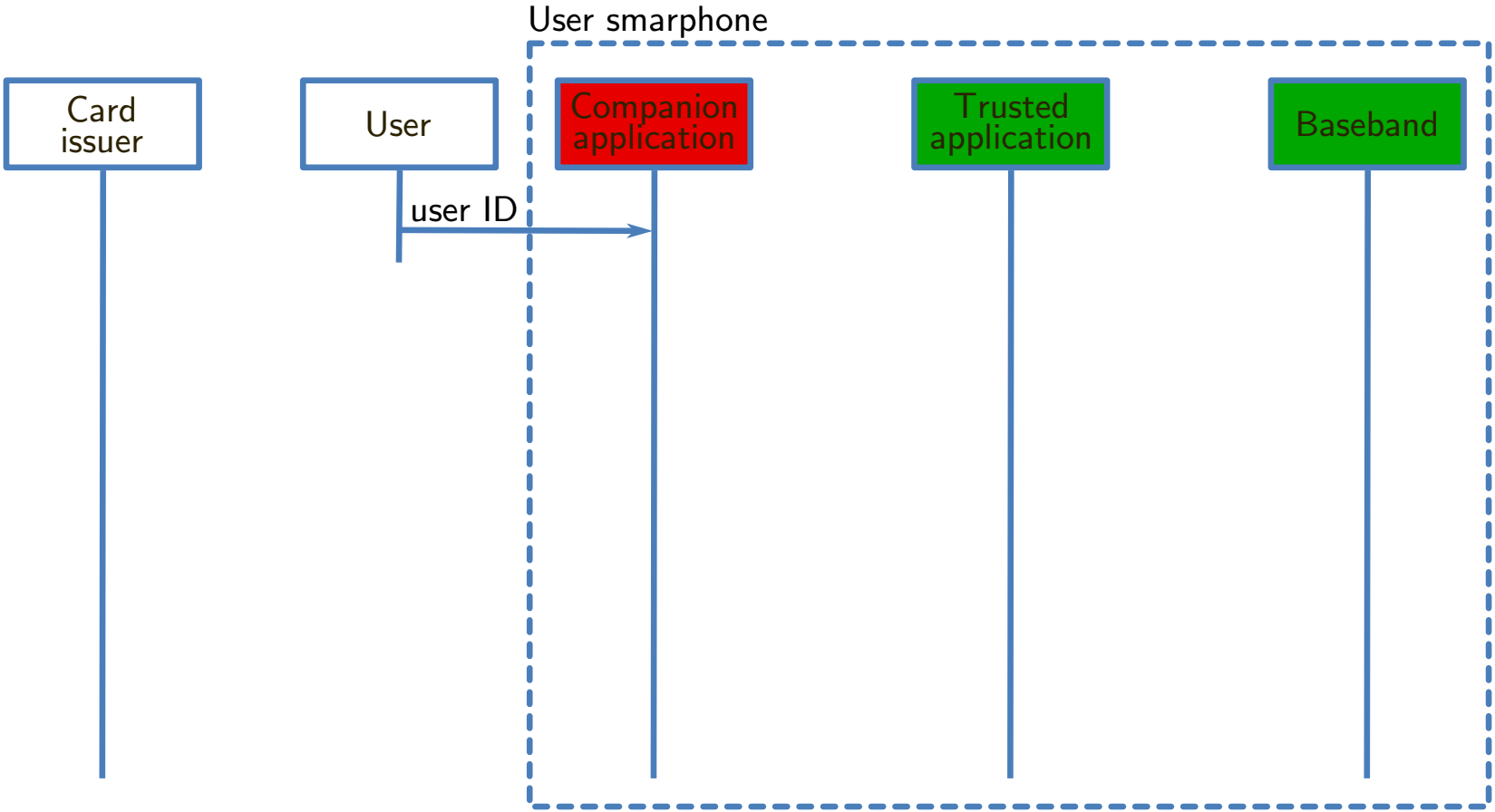


- Hardware attacker
- Compromised execution of Normal and Secure World
- Access to all TZ-sealed keys

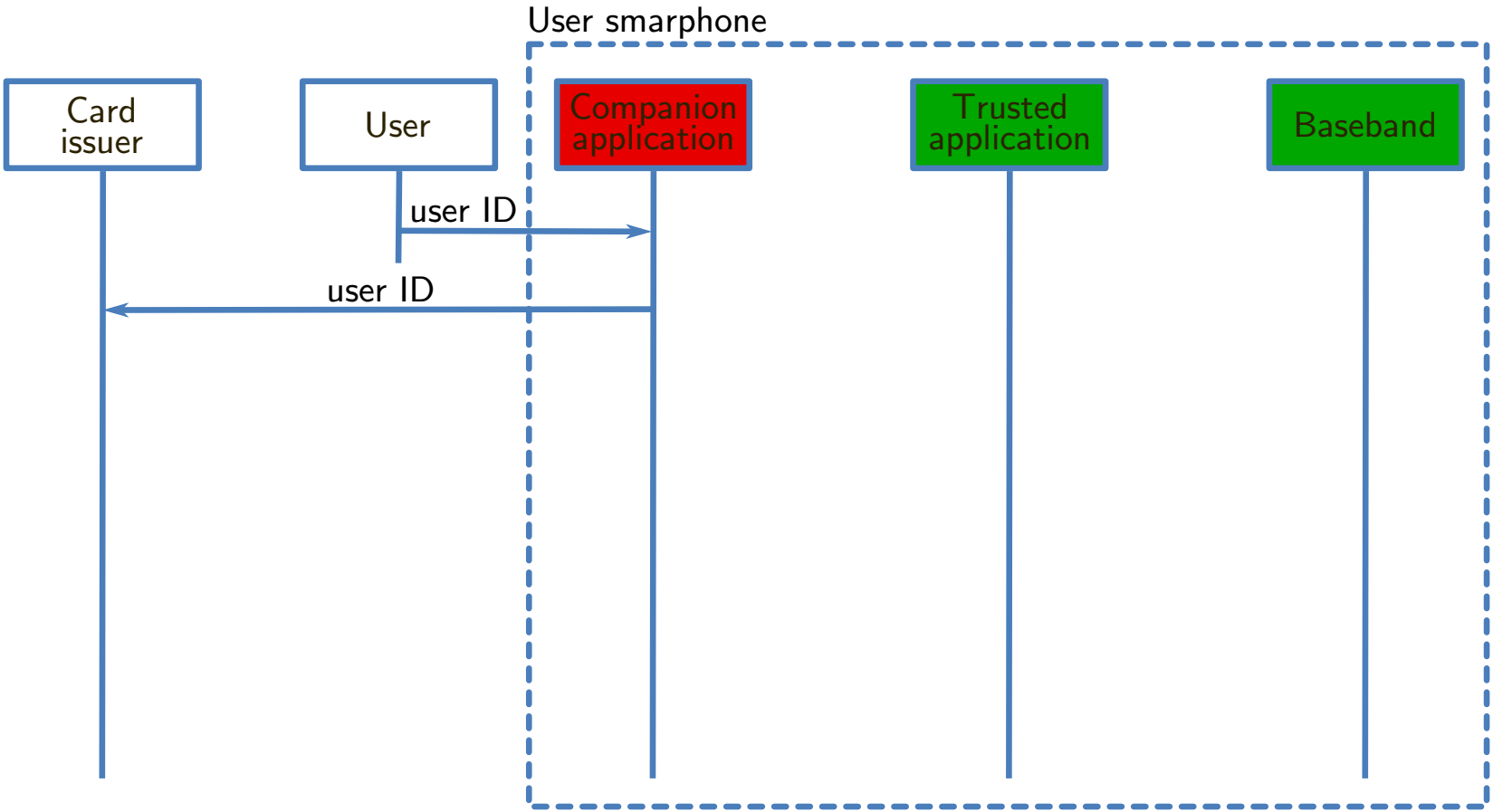
Baseband-assisted Secure Enrollment



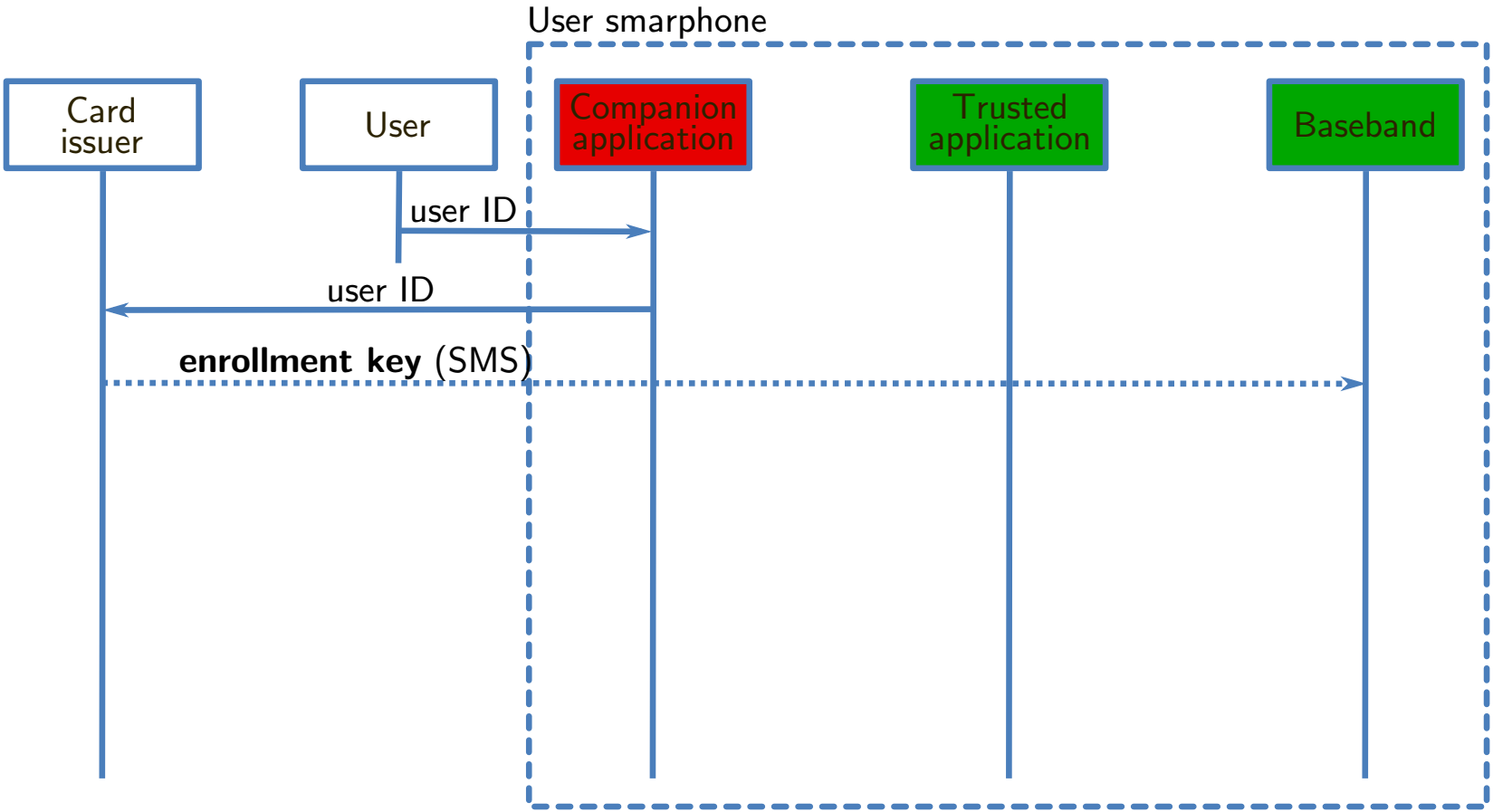
Baseband-assisted Secure Enrollment



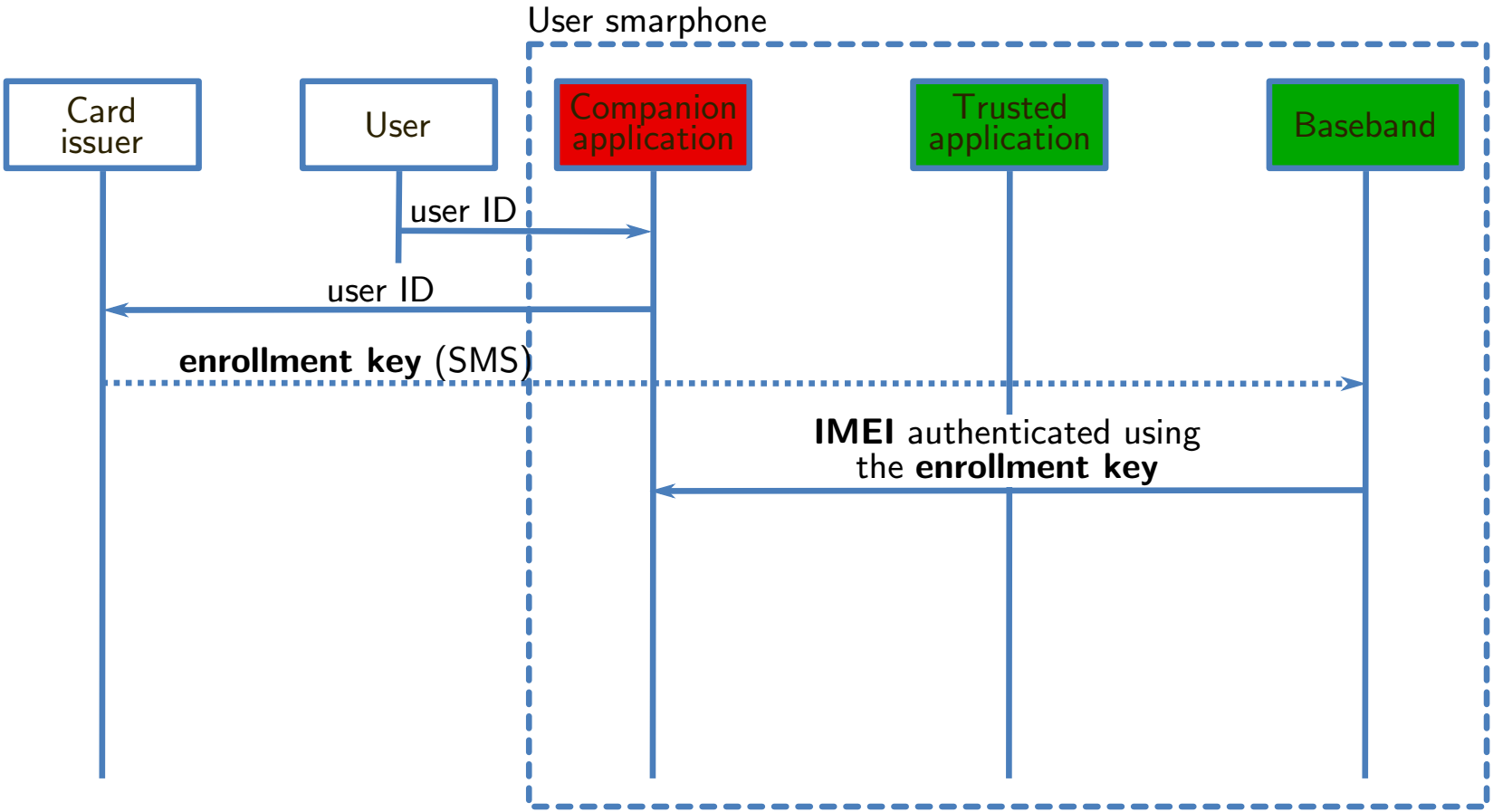
Baseband-assisted Secure Enrollment



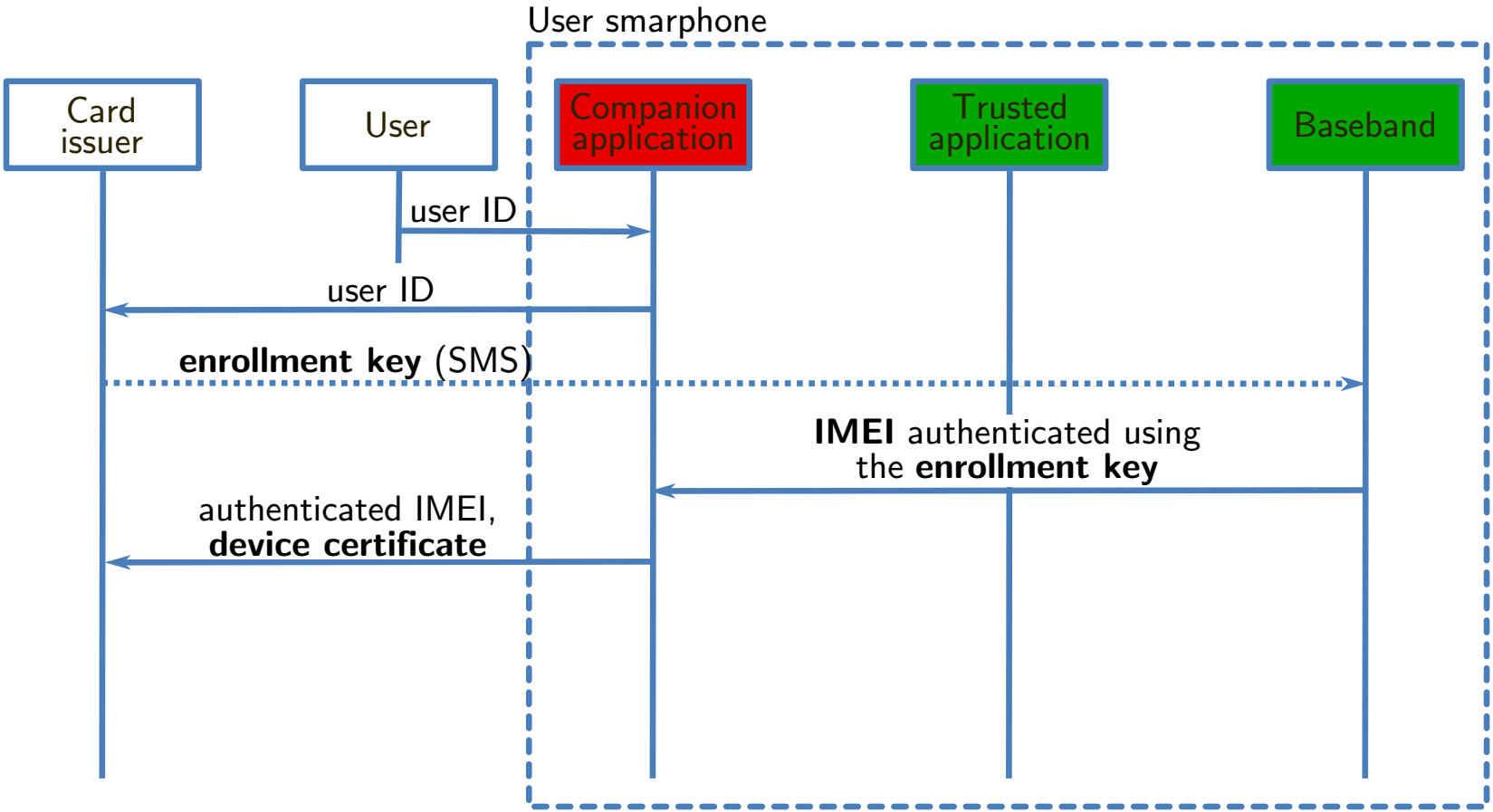
Baseband-assisted Secure Enrollment



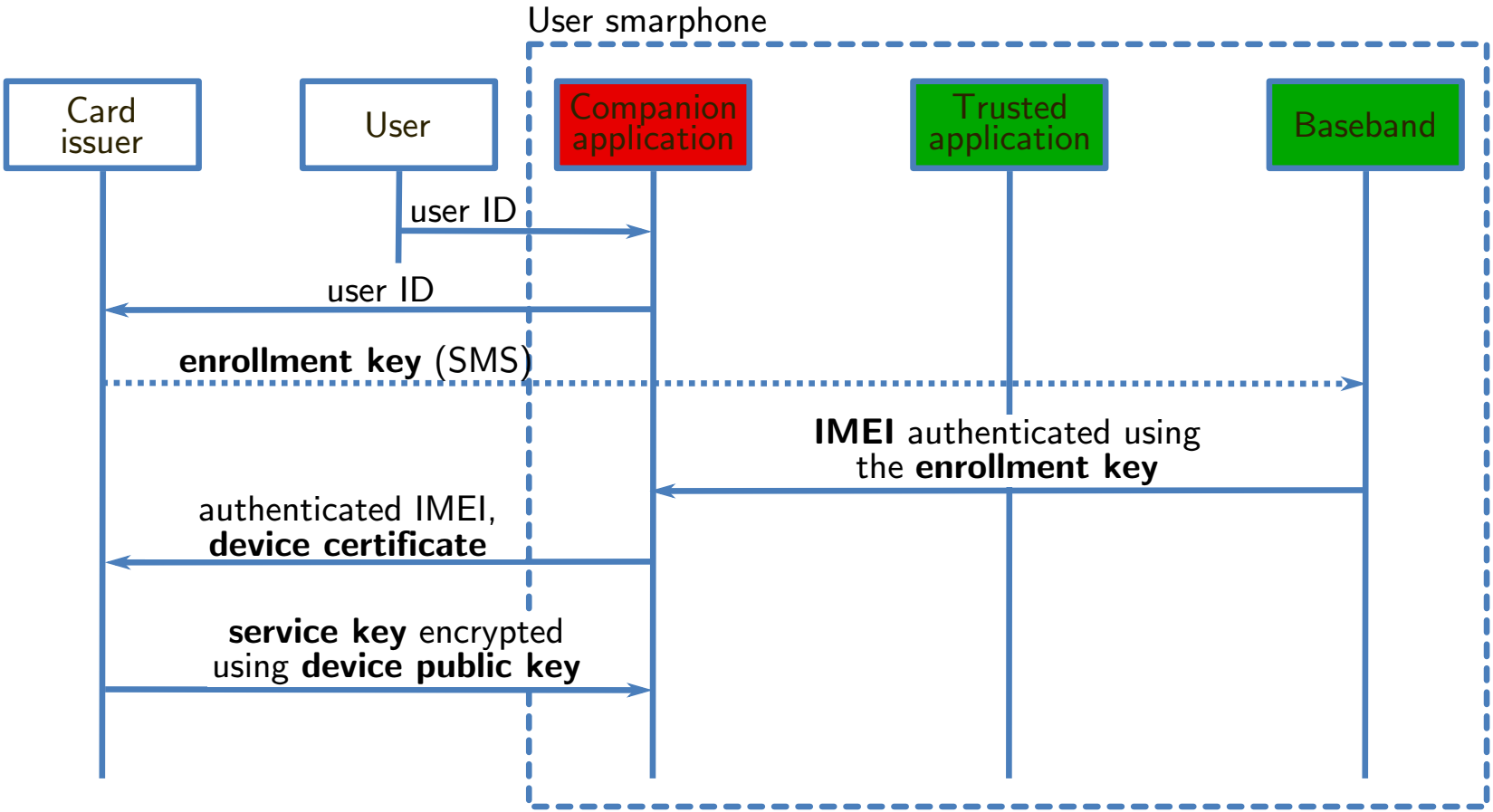
Baseband-assisted Secure Enrollment



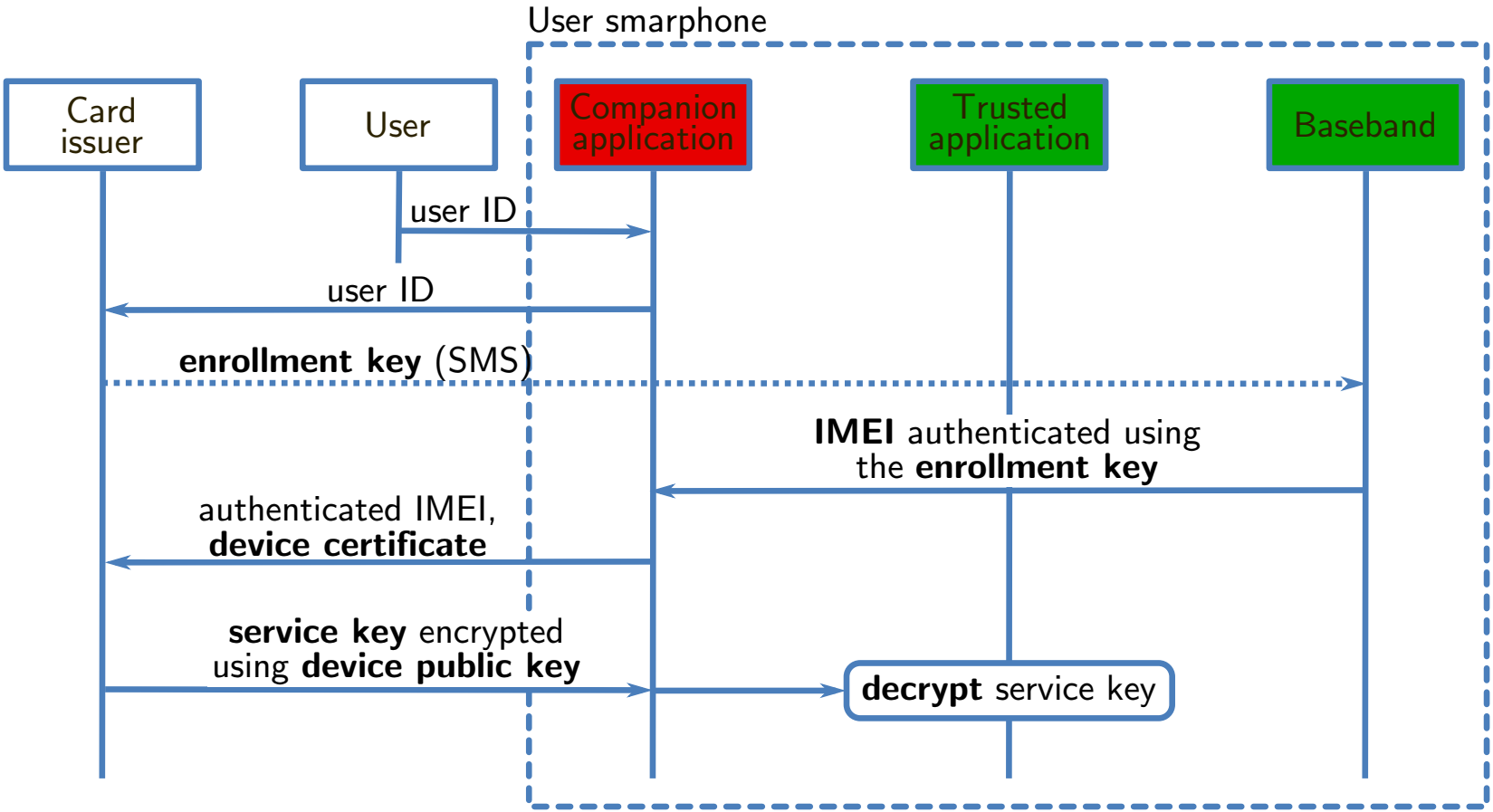
Baseband-assisted Secure Enrollment



Baseband-assisted Secure Enrollment



Baseband-assisted Secure Enrollment



Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

Secure Enrollment Outcome

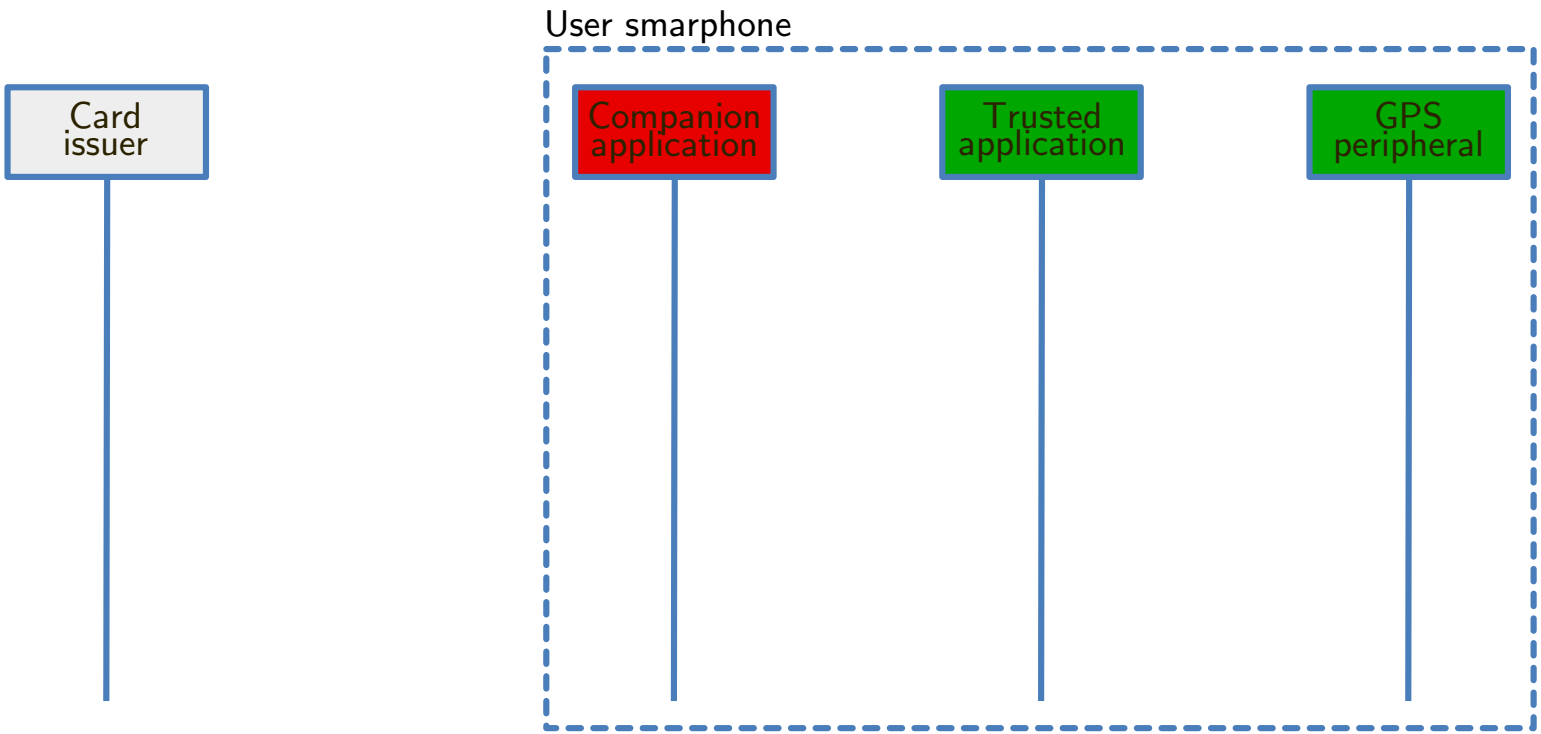
- → The card issuer and the TEE of the user's phone share a **service key**.
- → Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification

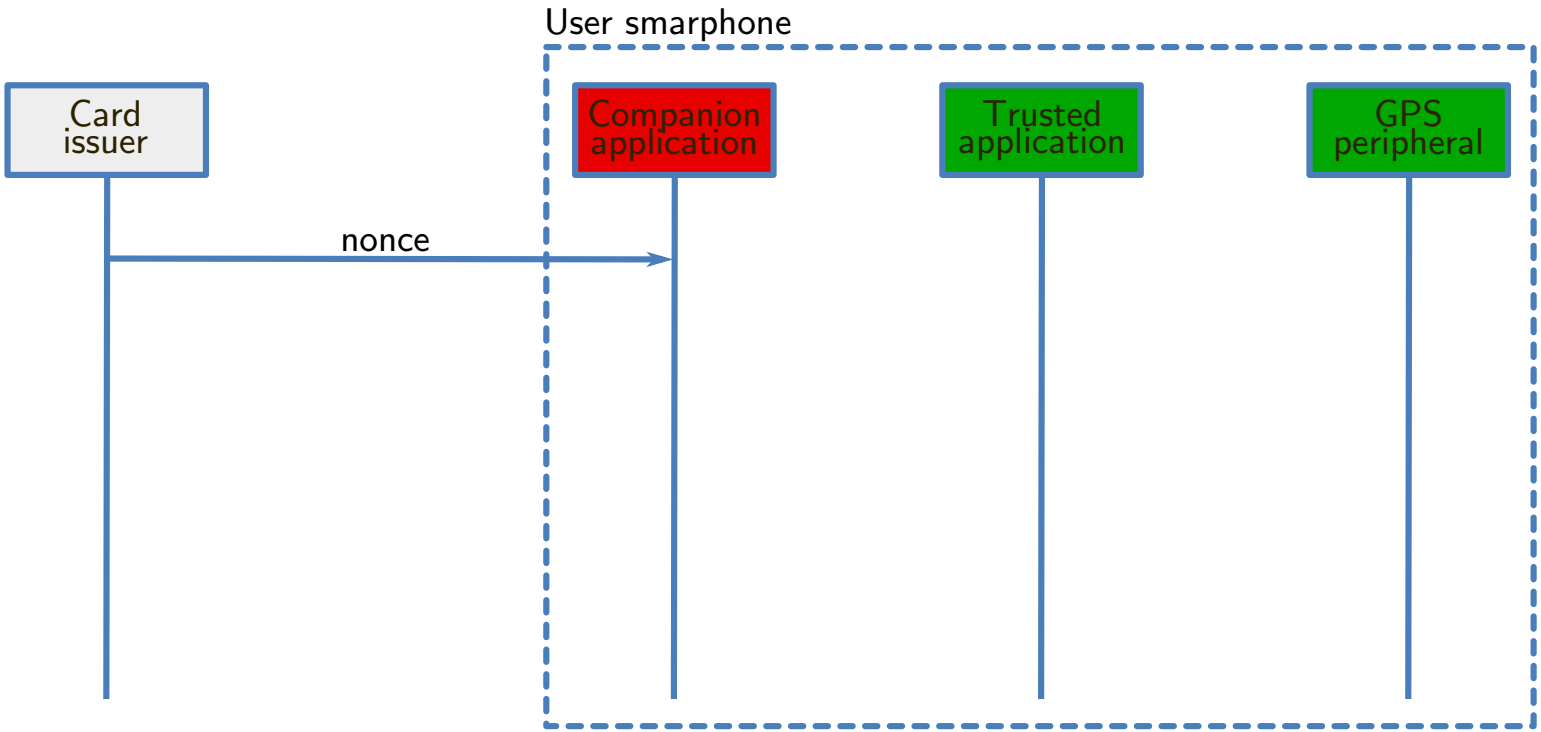


Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification

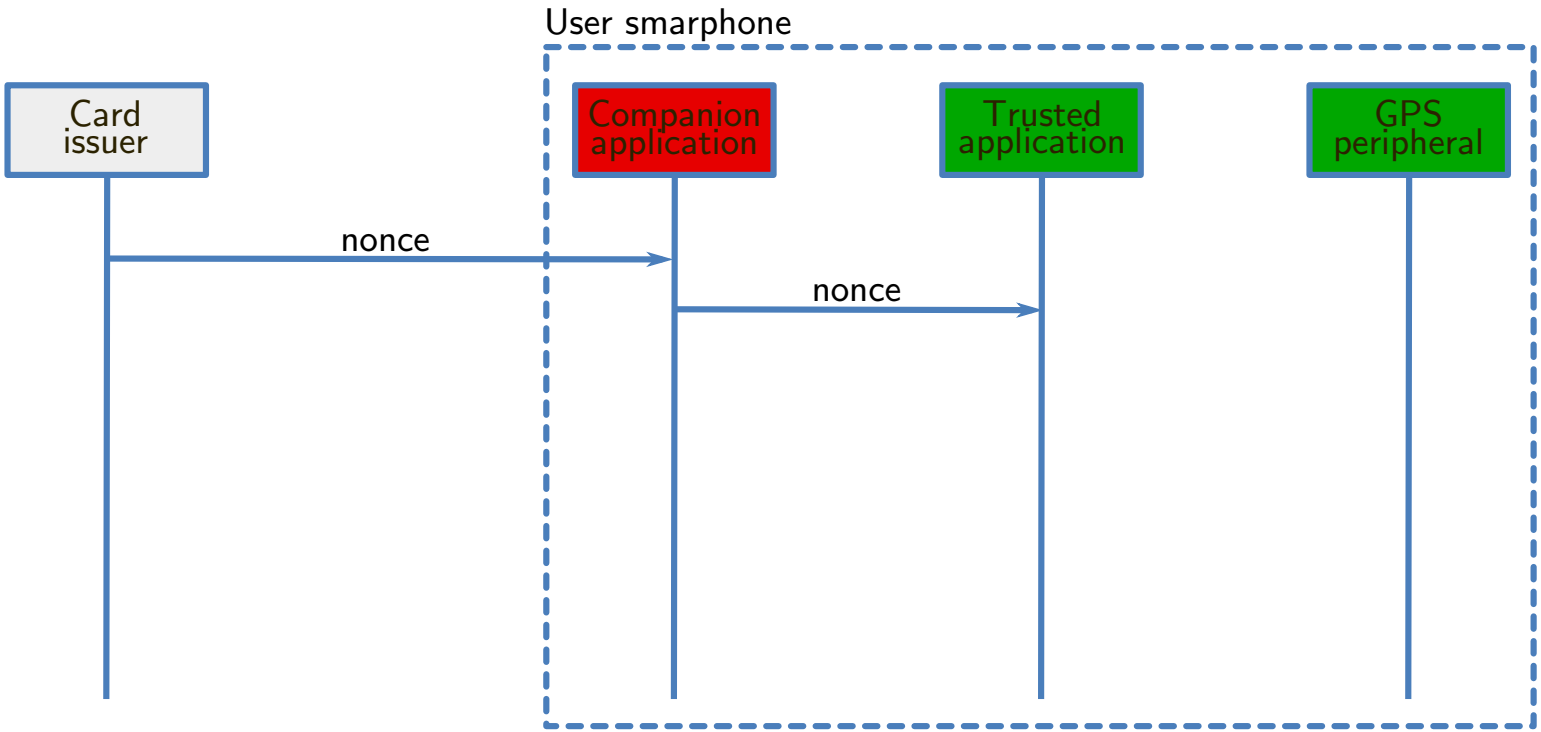


Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification

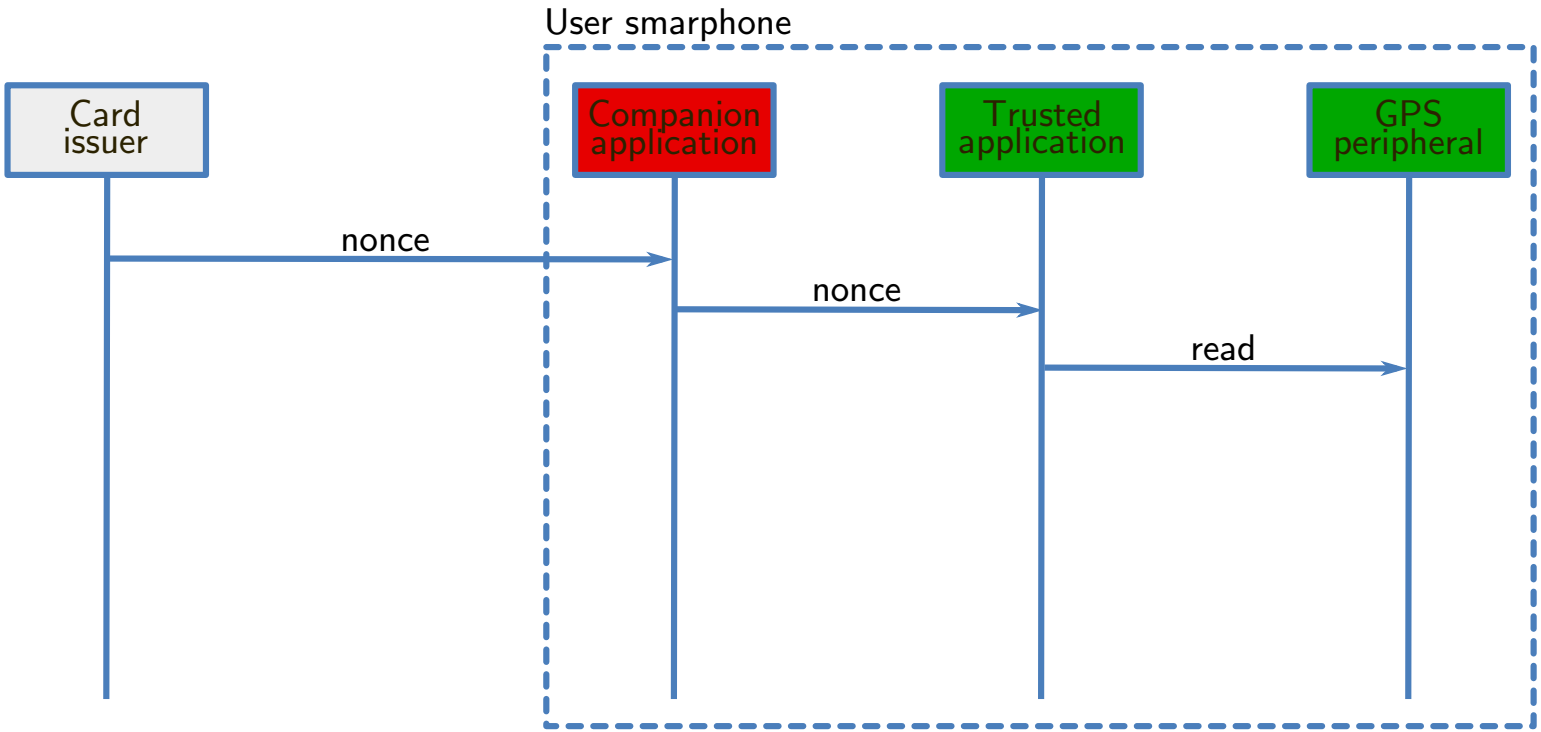


Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification

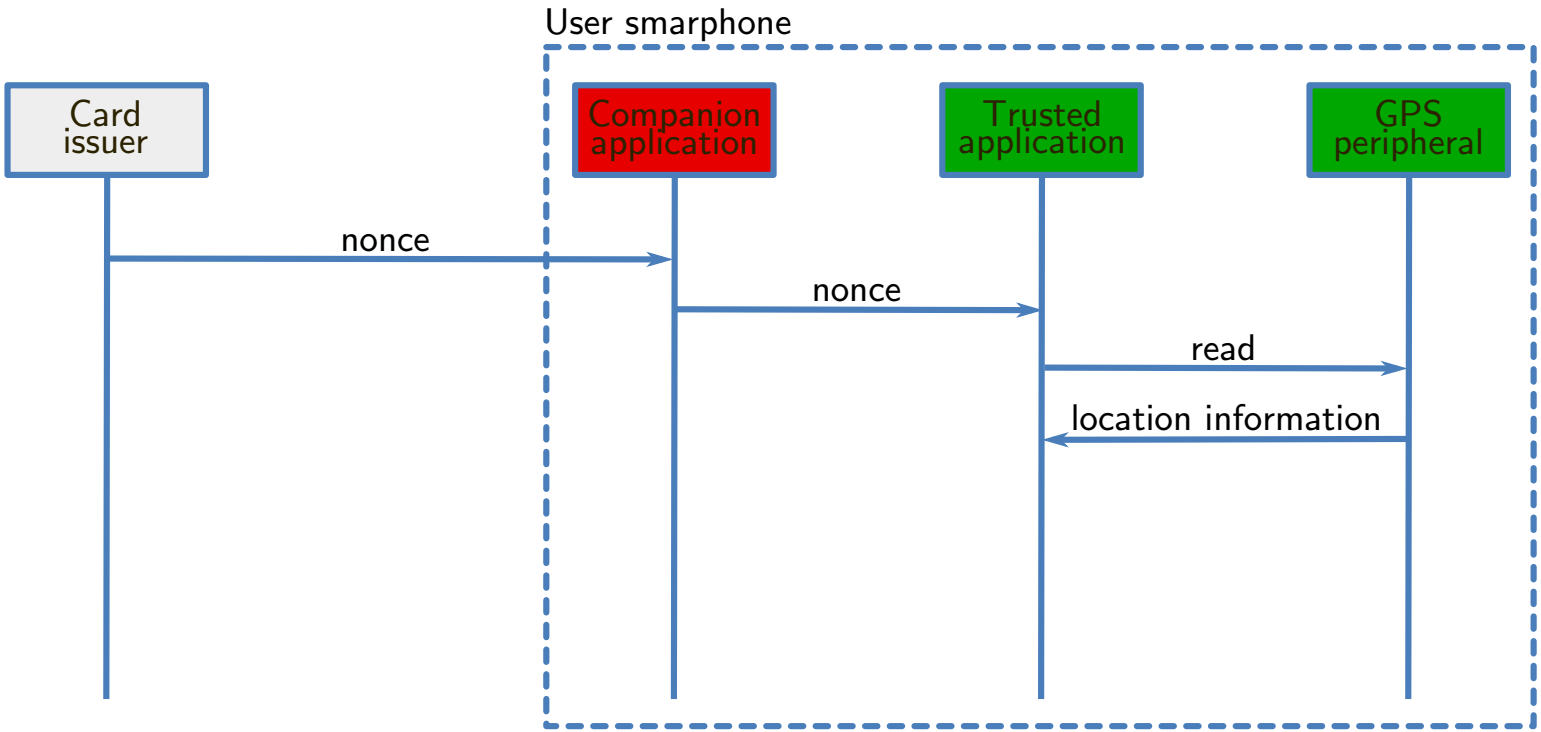


Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification

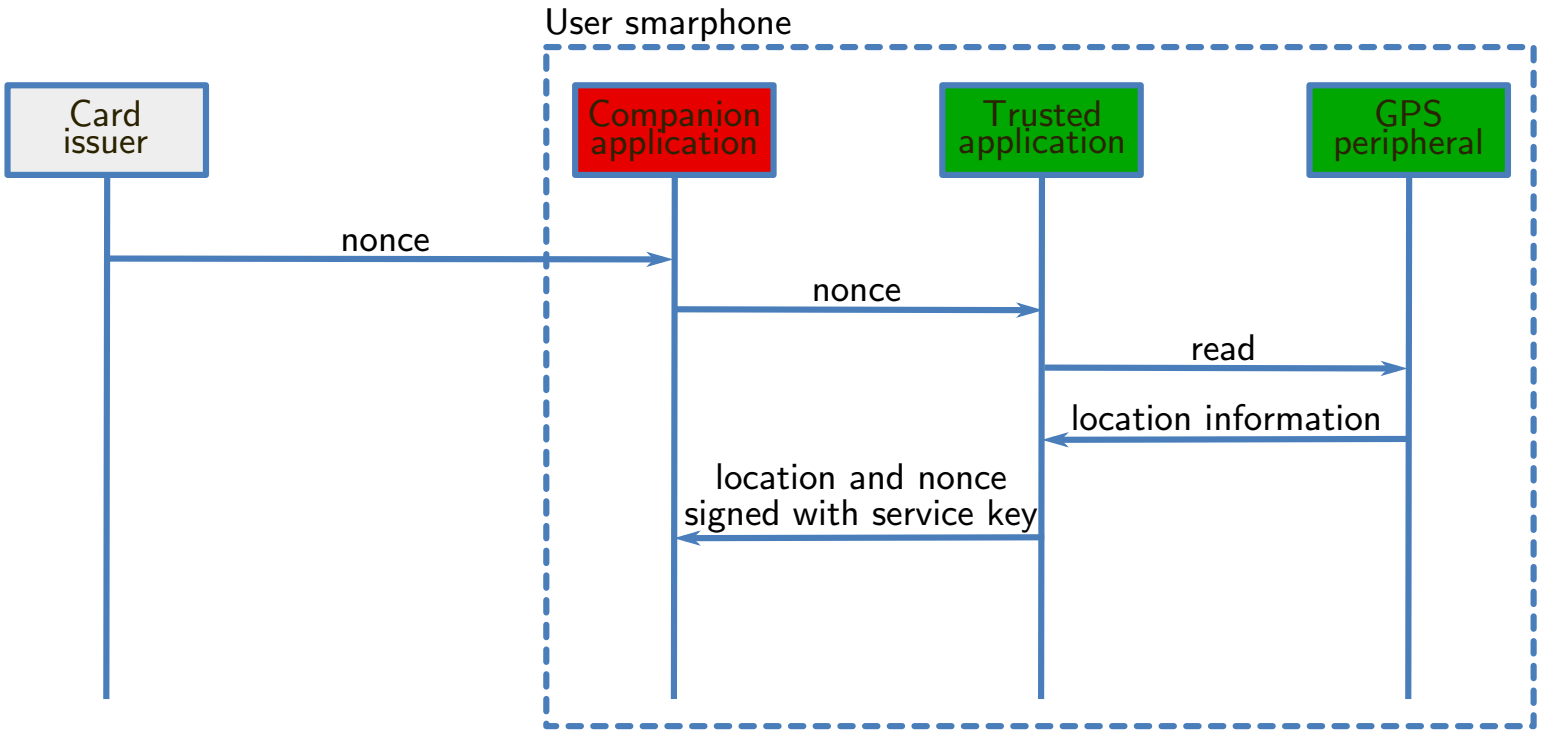


Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification

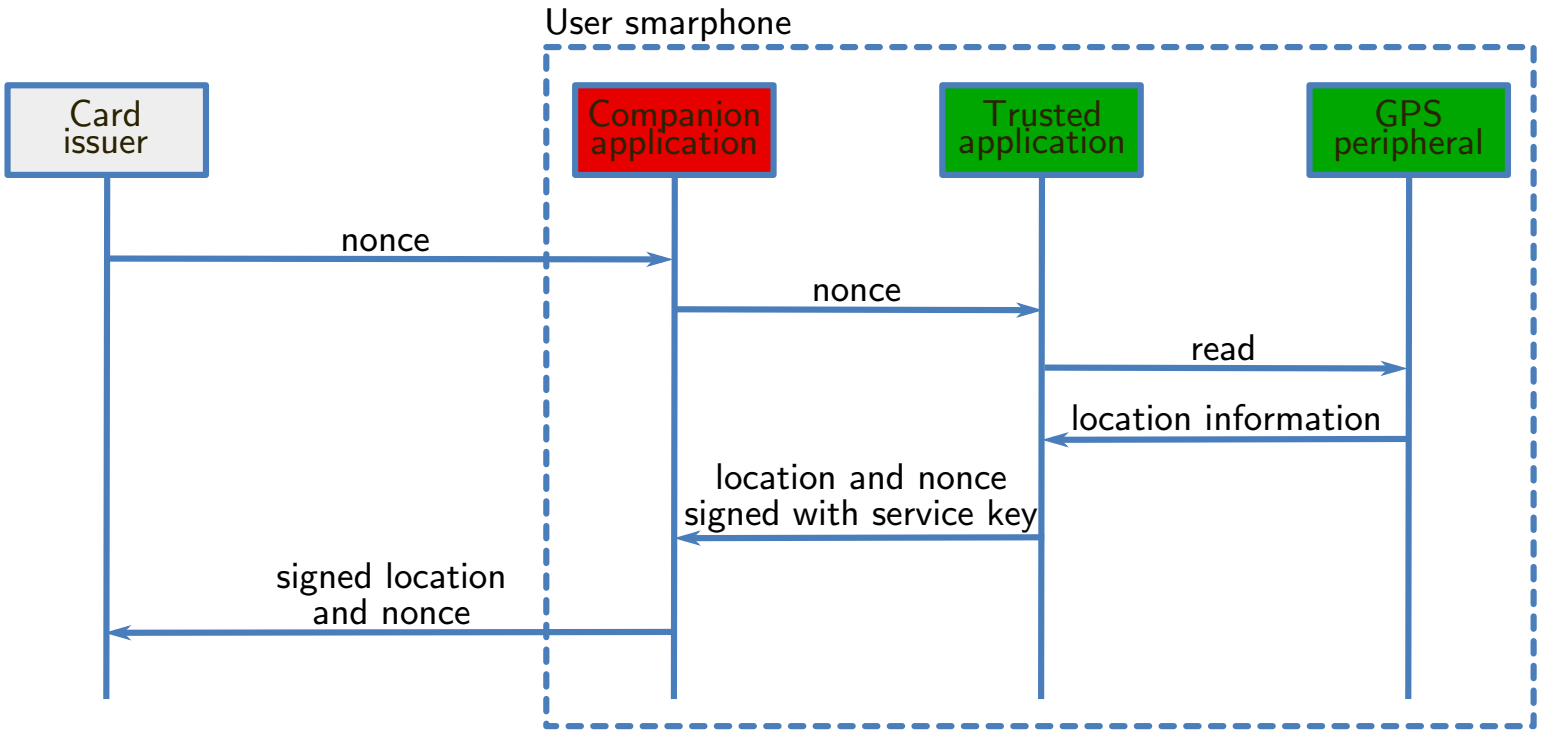


Secure Enrollment Outcome

→ The card issuer and the TEE of the user's phone share a **service key**.

→ Moving the SIM card to a new phone and re-running the protocol enables **easy migration** to new devices.

Location Verification



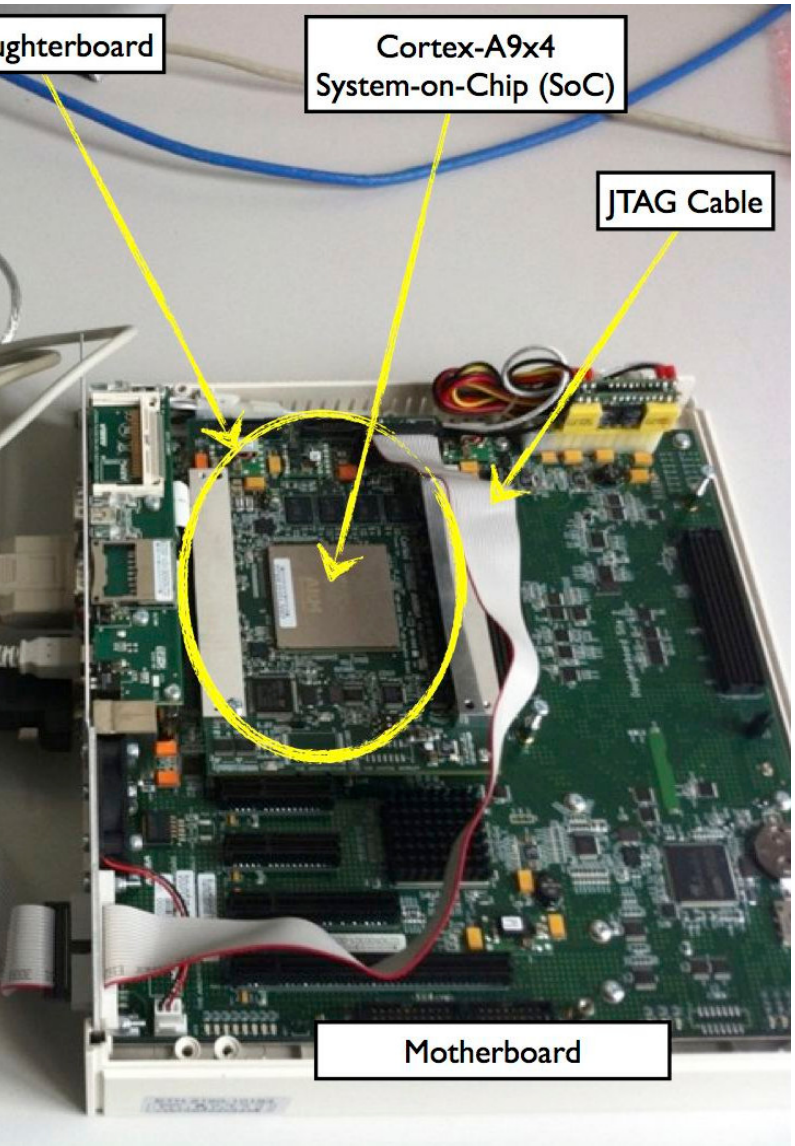
Baseband Prototype Implementation

www.reviewhandphone.com/

- OsmocomBB[1] open-source baseband
- Embed the key in the User Data Header of an SMS
- Changes amount to ∼**523 LoC** or +2.7% (451 for PolarSSL[2] code)

[1] http://bb.osmocom.org/
[2] https://polarssl.org/

TrustZone Prototype Implementation



- 400MHz TrustZone-enabled Cortex-A9 processor
- SW: Sierraware Open Virtualization[1]
- NW: Android 4.1.1
- Trusted Application ∼**150 LoC**
- **Only** ∼**3 ms** to generate an authentication tag (HMAC-256) over the GPS coordinates

[1] `http://www.openvirtualization.org/`

Android Prototype Implementation

www.cnet.co.uk/

Server:

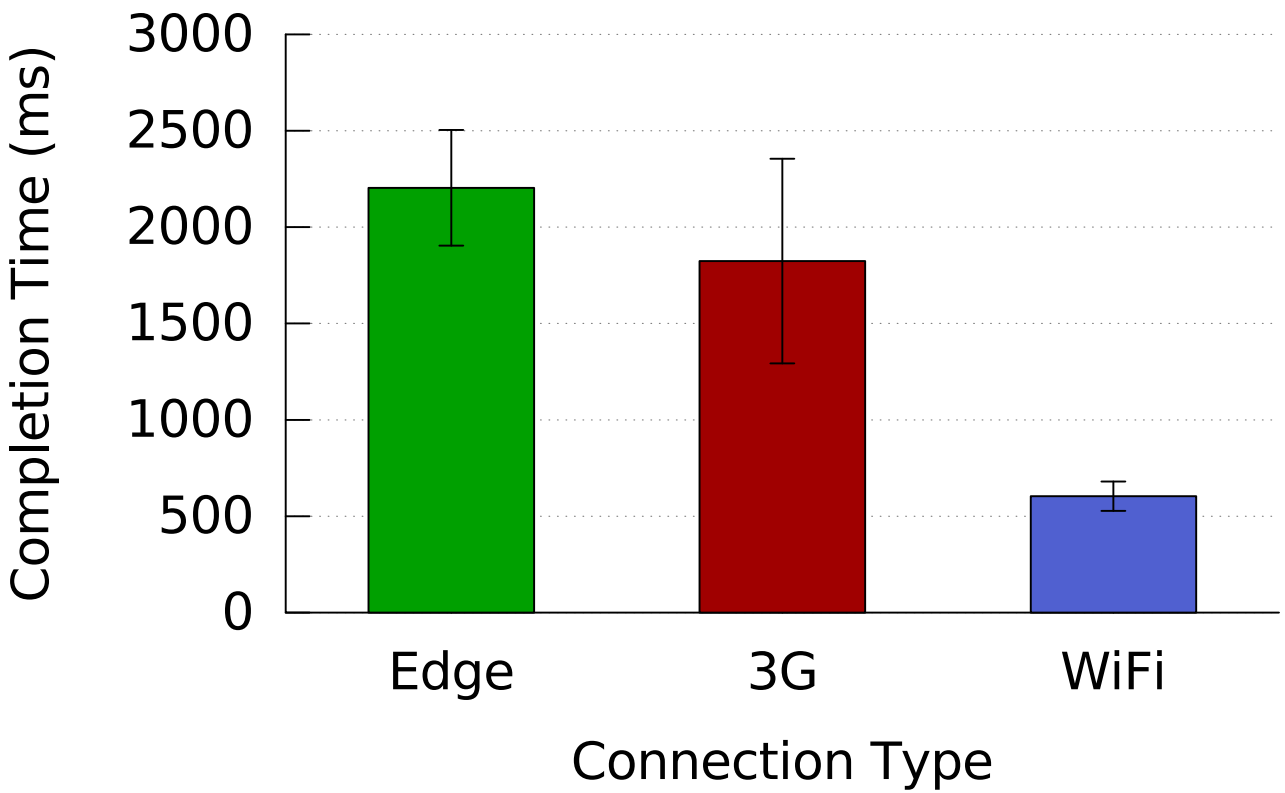
- Python (CherryPy) and SQLite database, running on a laptop
- API for IMSI-based enrollment and to start a location verification request
- Server-Client communication using Google Cloud Messaging (push notifications)

Client:

- Samsung Galaxy SIII, Android 4.1

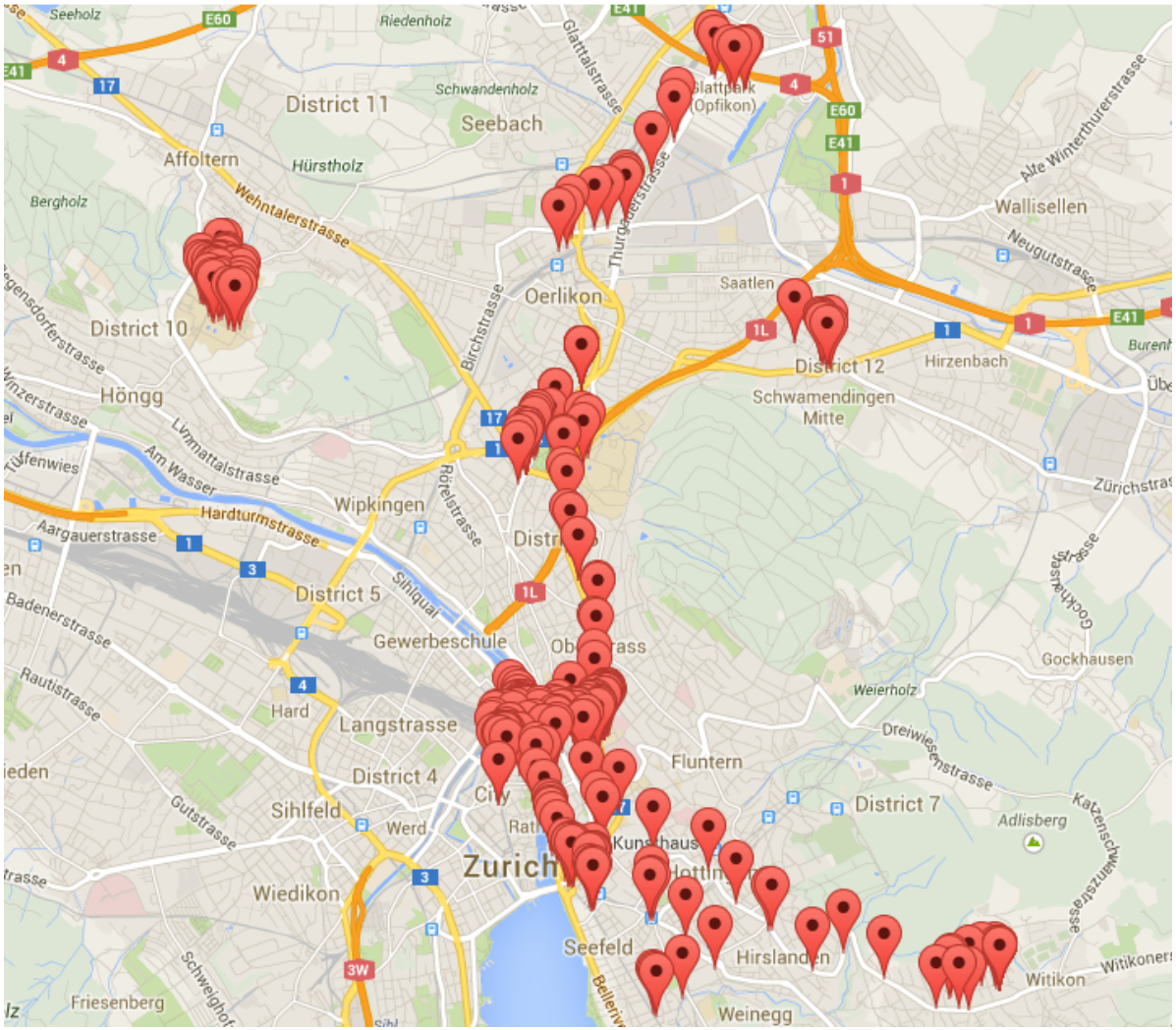
Office Test

Office environment, 100 location verification requests
(1 every 30 seconds)



Field Study

Walking around Zürich, triggering a location verification request close to PoS (museums, shops, ticket machines, . . .).



Field Study

	Field study (3G)	
	Orange (n=46)	Sunrise (n=34)
average (sec)	2.54	3.68
std dev (sec)	0.78	1.45

GPS accuracy (mt)		
average	max	min
17.40	48.0	4.0

- Tolerable delay (**max ∼4 seconds**)
- GPS accuracy good to **distinguish nearby shops**
- Minimal/No reception problems underground (train stations) or inside shops
- **No** user interaction required
- **No** privacy concerns, the card issuer already knows where the transaction takes place

Conclusion

1. **secure** smartphone-based second-factor authentication solution for payments at PoS leveraging a TrustZone-aware phone's reported **location**
2. two novel secure (against different attacker models) **enrollment schemes** supporting easy migration
3. prototype and evaluate the **ease of deployment** and **effectiveness** of our solution
4. show applicability to different application scenarios (buildings access, transportation, . . .)
5. integration of our solution into the EMV standard

Conclusion

1. **secure** smartphone-based second-factor authentication solution for payments at PoS leveraging a TrustZone-aware phone's reported **location**
2. two novel secure (against different attacker models) **enrollment schemes** supporting easy migration
3. prototype and evaluate the **ease of deployment** and **effectiveness** of our solution
4. show applicability to different application scenarios (buildings access, transportation, . . .)
5. integration of our solution into the EMV standard

Questions?

claudio.marforio@inf.ethz.ch