Trusted Location Based Services

Masterprojects @IAIK

Outline

Overview: Location Based Services (LBS)

Security ? - Trusted Location Based Services (T-LBS)

- Prototype 1
- Prototype 2
- Security Analysis

Location Based Services

Numerous applications with users' current location

- Augmented reality
- Navigation
- Context - Awareness

Simple goal: improve user experience

no applications that require trustworthy location

- how to acquire trustworthy information?

Trusted - Location Based Services

Location-Time-Ticket (LTT)

- position
- time

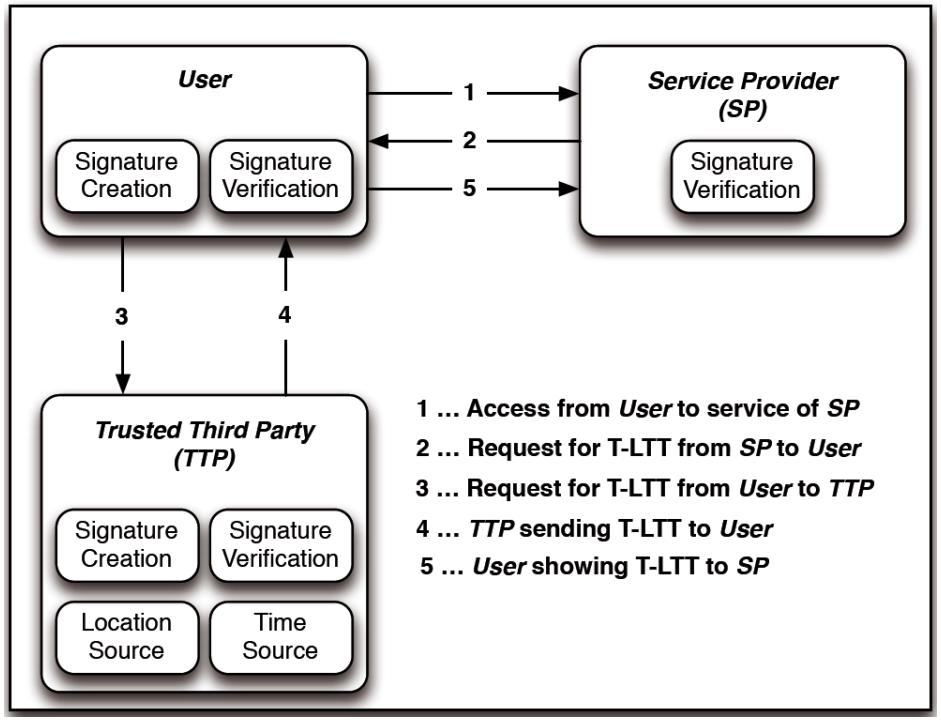
Attested by TTP

- trustworthy location
- for services

→ T-LTT

Mobile Phone Signature

- users' identity, integrity
- non repudiation



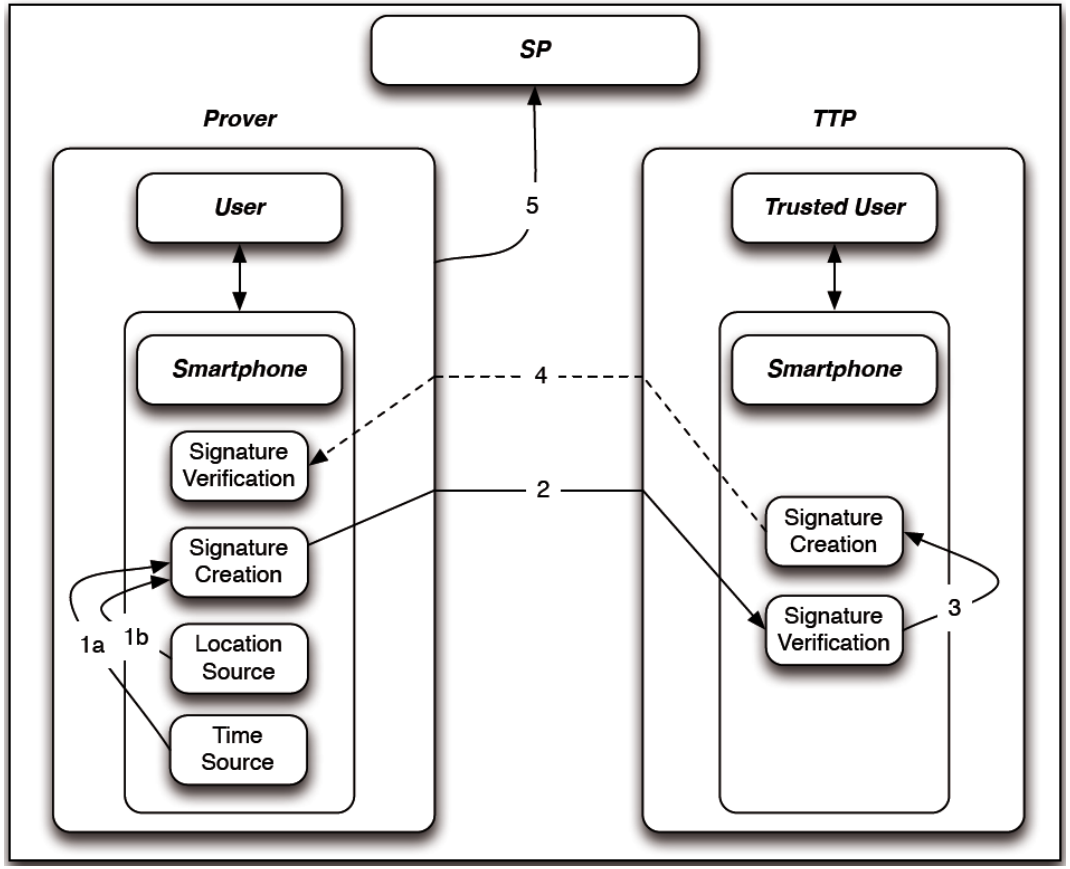
T-LTT Format

```
<dsig:Signature Id="signature-2-1" ...
  <dsig:Object Id="etsi-signed-2-1" ...
    <dsig:Signature Id="signature-1-1" ...
      <dsig:Object Id="etsi-signed-1-1">
        <tltt:ticket xmlns:tltt="http://www.egiz.gv.at/namespaces/tltt/1.0#">
          <tltt:location>
            <tltt:longitude>15.4545233</tltt:longitude>
            <tltt:latitude>47.0605959</tltt:latitude>
            <tltt:accuracy>30.0</tltt:accuracy>
          </tltt:location>
          <tltt:time>2013-01-06T20:46:31+0000</tltt:time>
          <tltt:attachment>
            <tltt:data>ivWXQ.....AOc<tltt:data>
            <tltt:fileEnding>png</tltt:fileEnding>
          </tltt:attachment>
        </tltt:ticket>
      </dsig:Object>
    </dsig:Signature>
  </dsig:Object>
</dsig:Signature>
```

Prototype 1: Peer-to-Peer

Two Smartphones

- one user acts as TTP



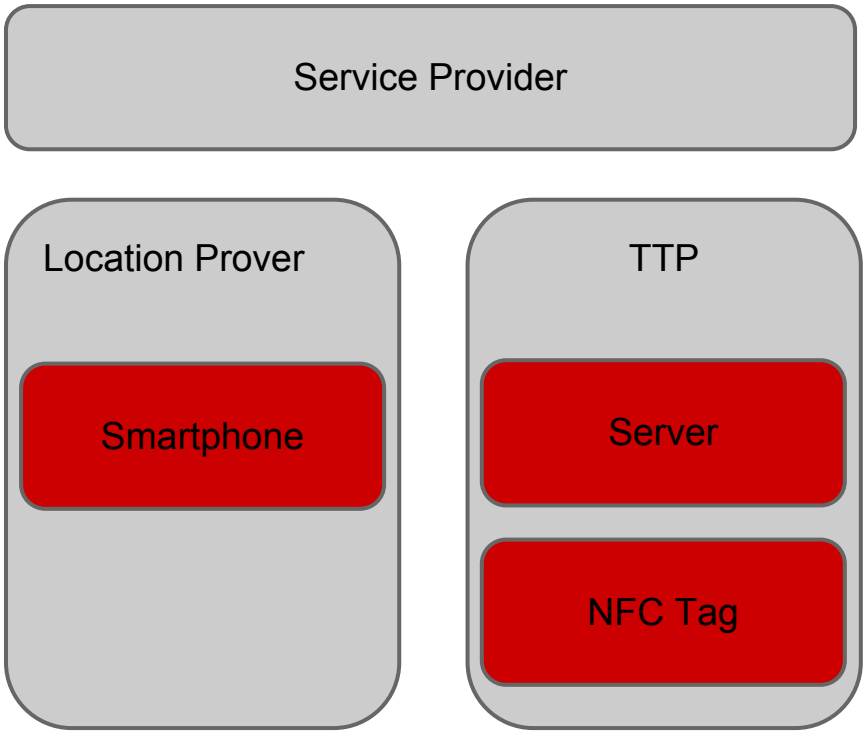
Prototype 2: NFC tag + server as TTP

NFC Crypto tag

- unique id
- electronic signature

Server

- knows location of tag
- timestamp



Use Cases

Prototype 1

- Accident report
- Commissioning (add photo, confirmation)
- ...

suitable if at least one person has strong interest in correctness

Prototype 2

- Maintenance, night watchmen
- Check-in (Foursquare, Facebook)
- Geocaching

no limitations in trustworthiness

Prototype 1: Project goals

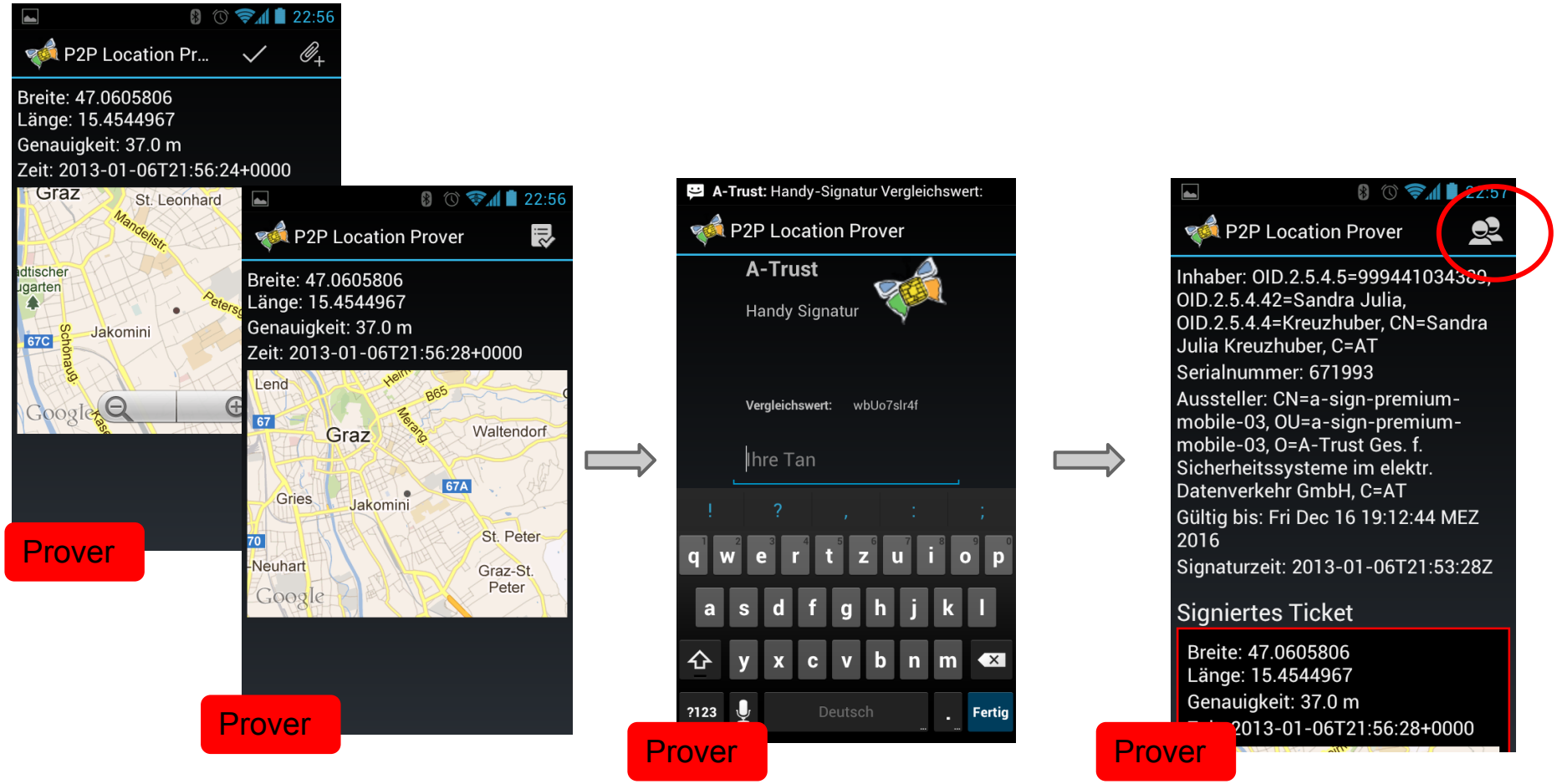
Extend existing prototype

Refine used protocol

Provide reusable code components

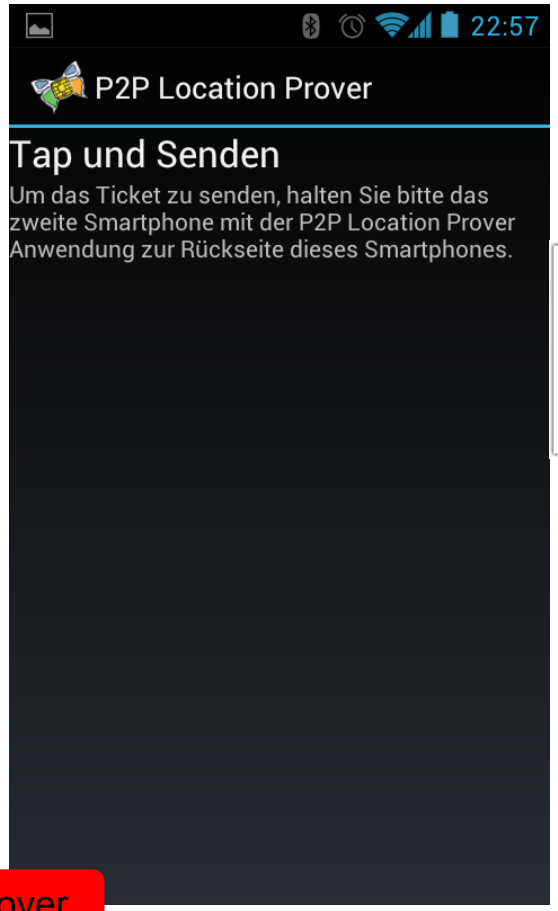
→ Android library + simple demonstrator application

Prototype 1:



Prover creates ticket, checks it, signs it, checks signature

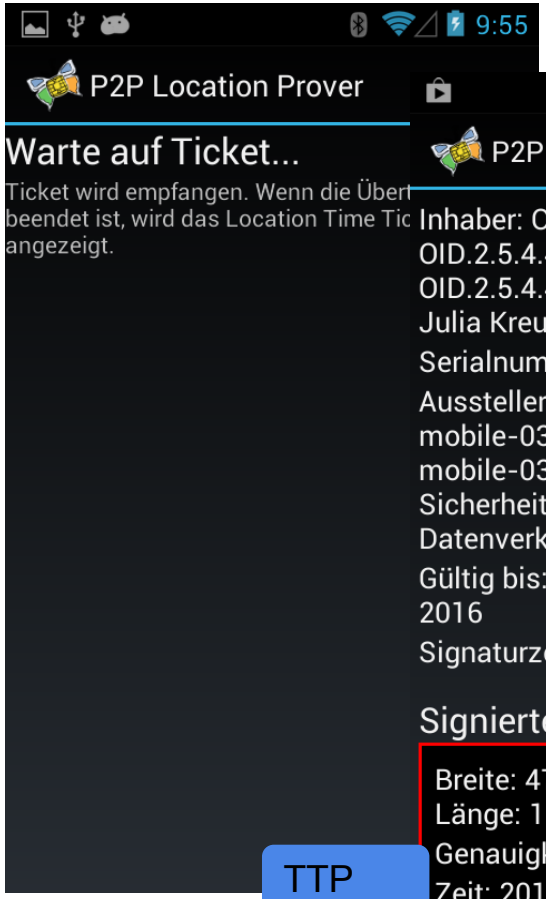
Prototype 1:

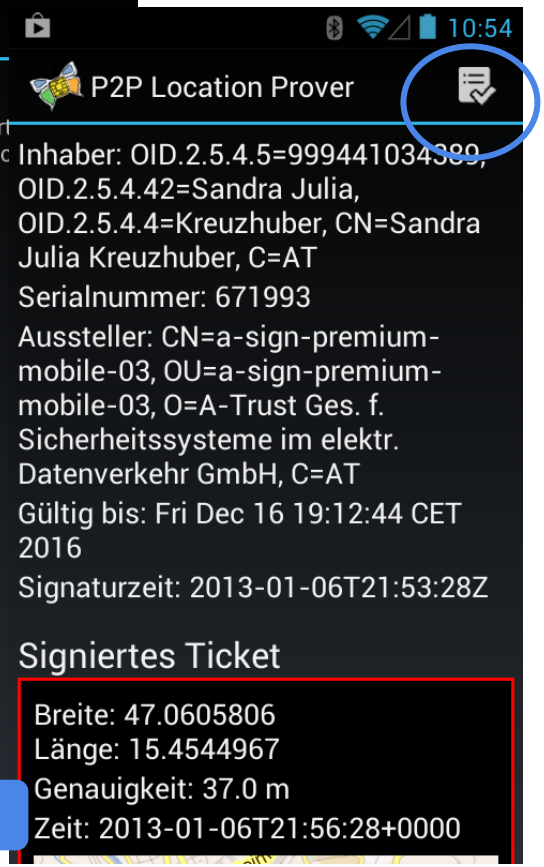


Prover

NFC

MAC

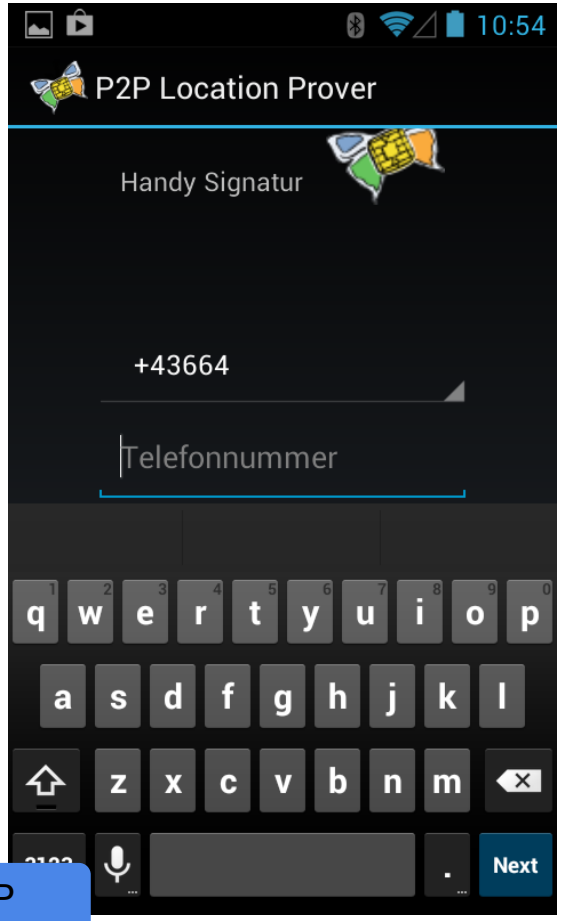




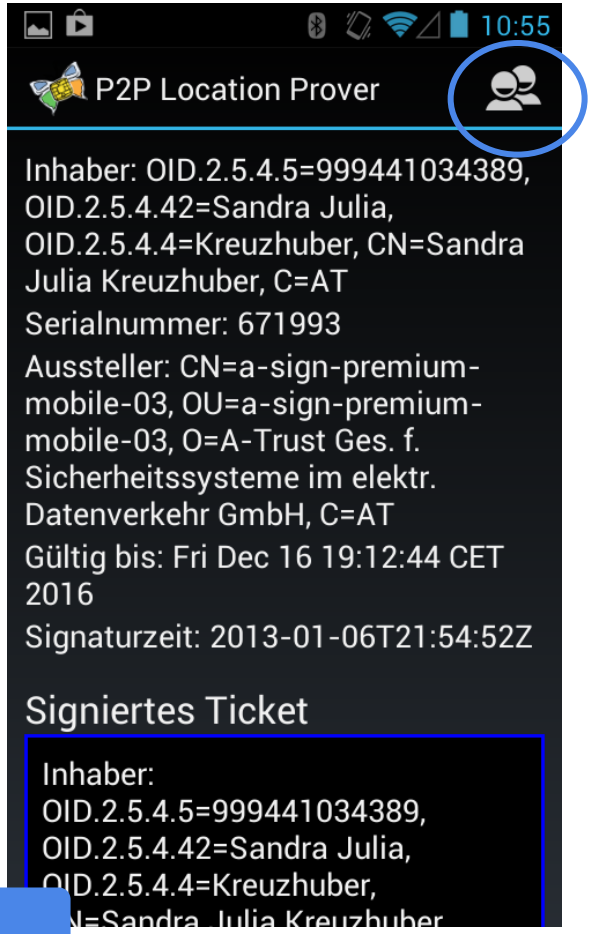
TTP

Share ticket, TTP receives ticket, checks ticket

Prototype 1:



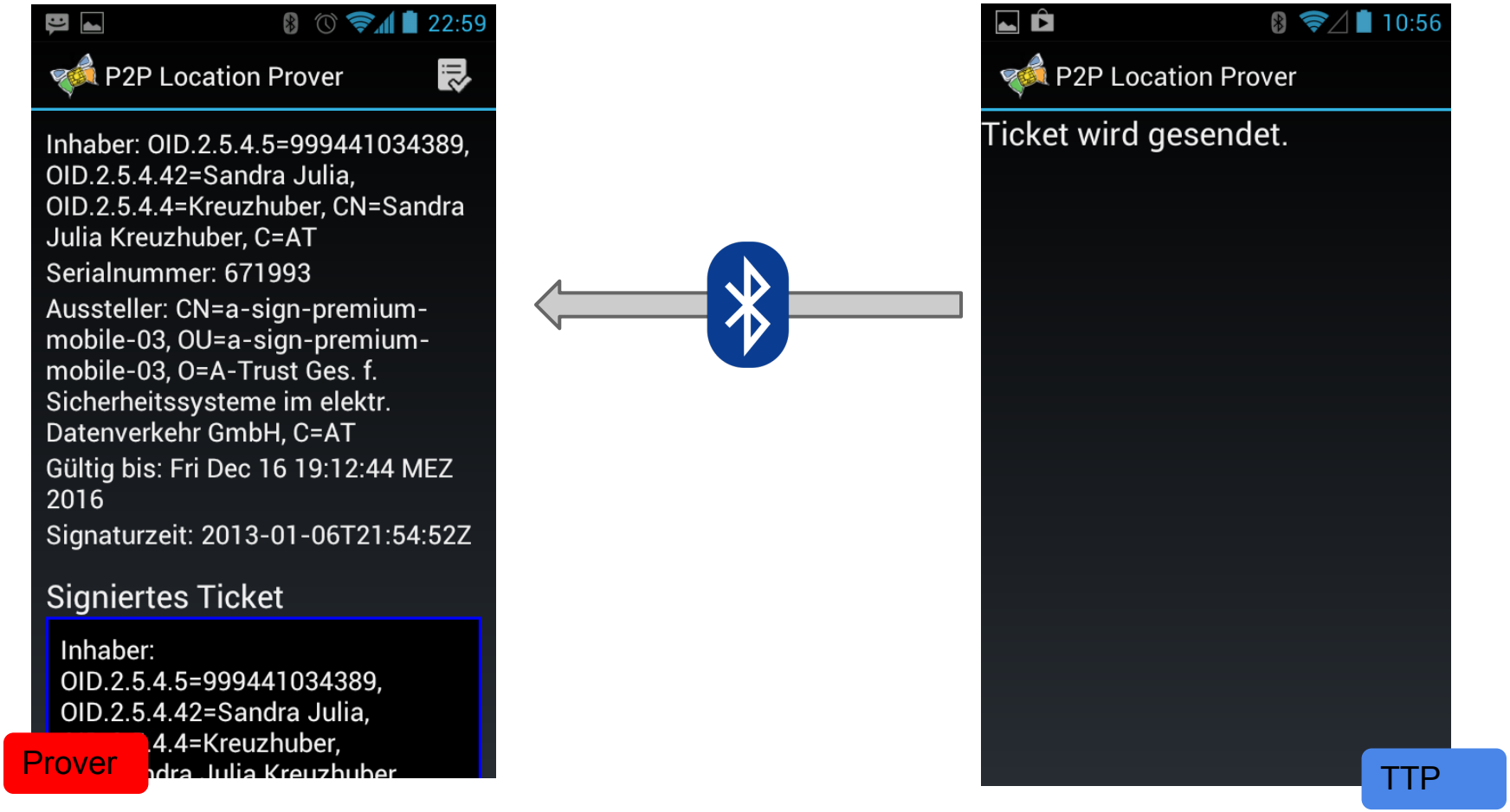
TTP



TTP

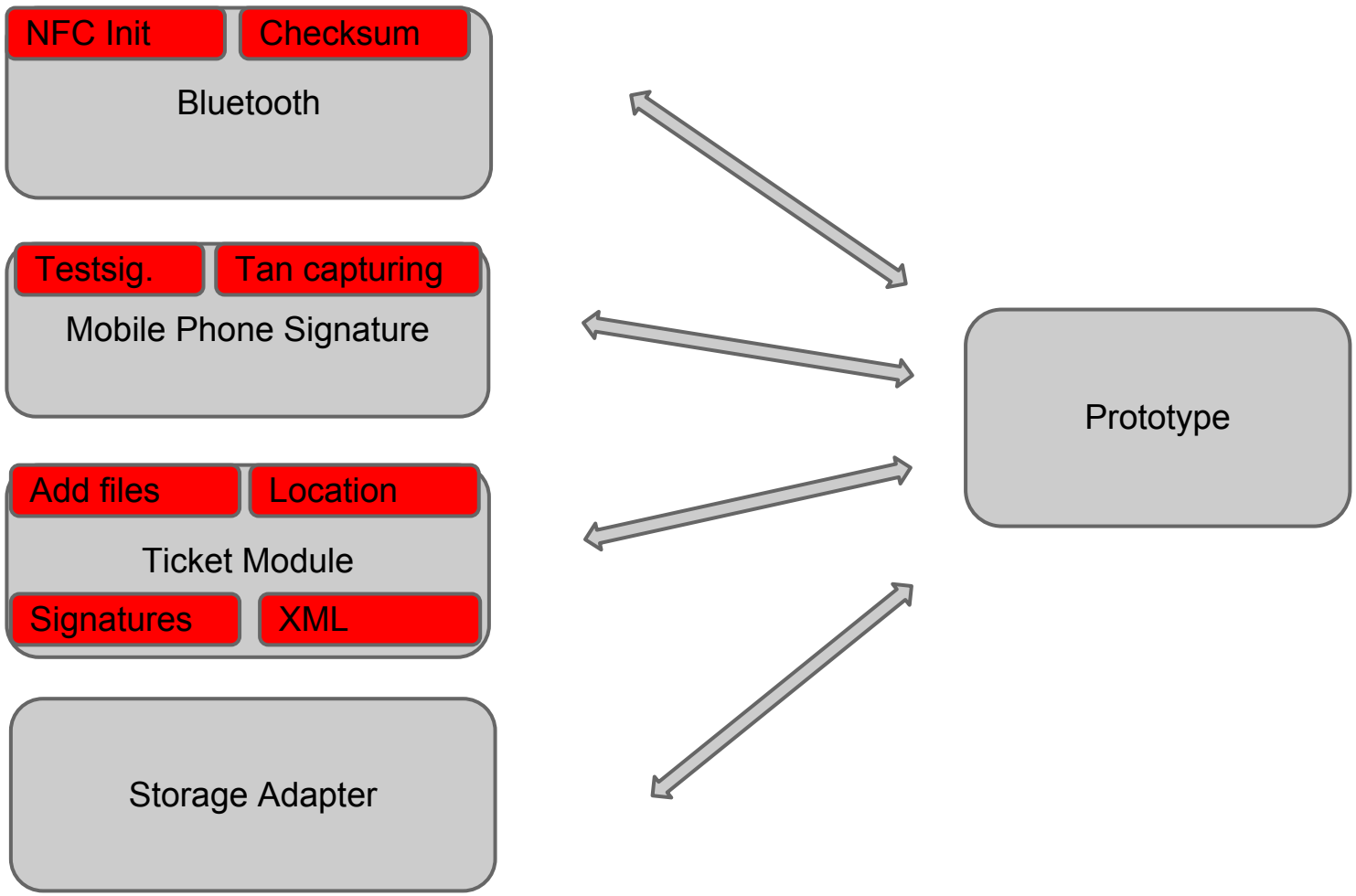
Sign ticket, check signature, share ticket again

Prototype 1:



Ticket is sent back again

Prototype 1: Library components



Prototype 1: Lessons learned

A-Trust Handy Signature:

- Bug: sign ticket twice, same id in signature tag, signatures not verifiable, now fixed

Bluetooth:

- random bytes lost, large files, implemented SHA256 checksum

Prototype 1: Possible extensions

Improvements in User Experience

- Storage dialogs (now "hardcoded" in special dir on SD)
- more defined error messages

Signature Verification on the phone (other bachelor project...)

- display verification result to user

Several "CommunicationDevices" - now Bluetooth, Wifi Direct?

- Android Bluetooth quite a mess...

Prototype 2: Overview

SP

Prover = Android App (on phone) + User

TTP = Server (on Internet) + Crypto Tag (fixed location)

Specific P2 Goals

- Extend ACN project rapid prototype (without server...)
- Feasibility (performance and usability: tag, internet)
- Design protocol
- GAE/GWT Know-how build-up

Prototype 2: Crypta

CRYptographic Protected TAg by IAIK, ams & RF-iT solutions

NFC-enabled (passive, ISO14443A)

ISO7816 APDU commands

NFC Forum Type 4 Tag compliant

read URL for application or Certificate (proof of originality)

7 byte **UID**

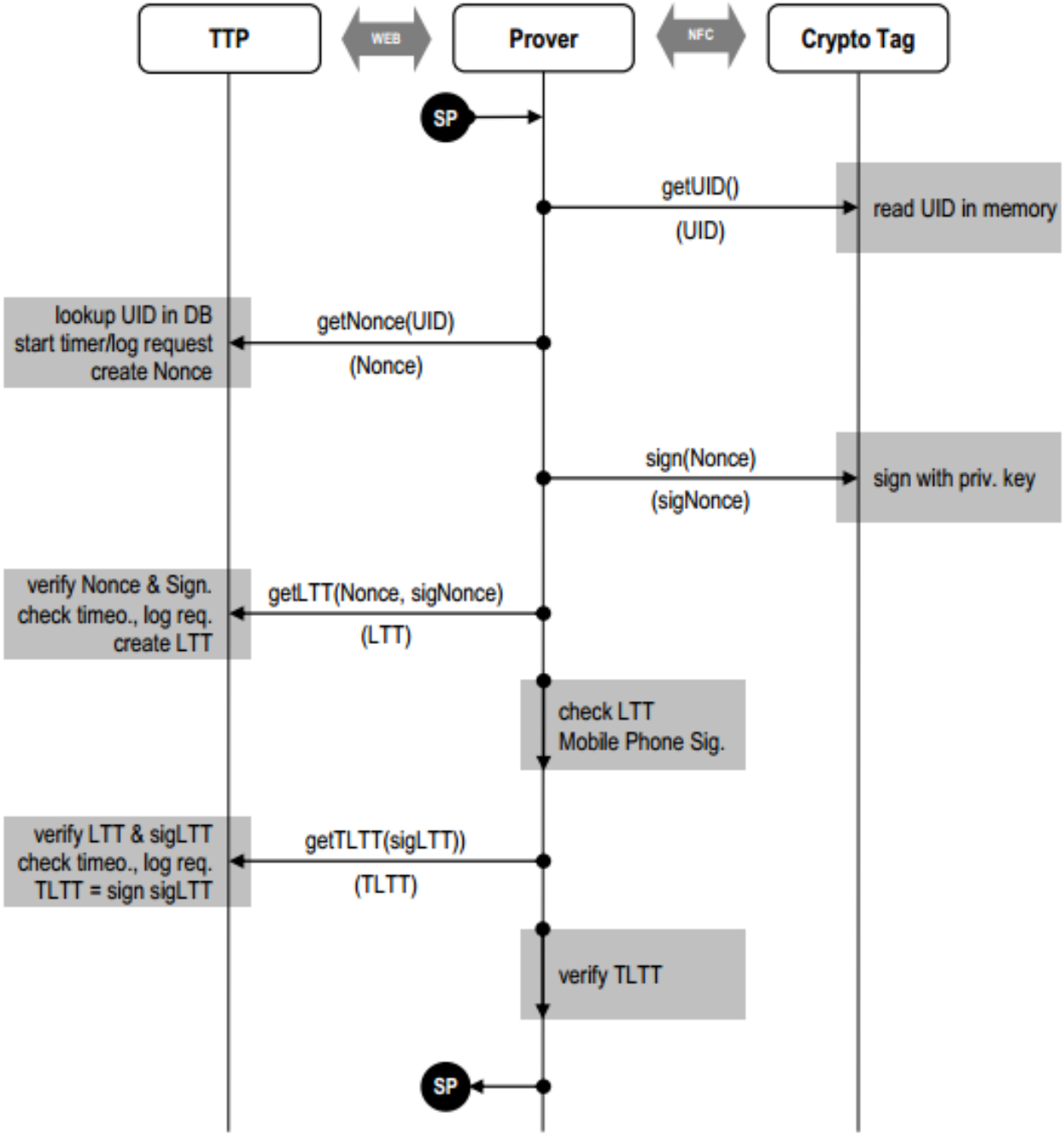
Crypto: ECDSA, AES

ECDSA: sign 16 bit value (192 bit key size)

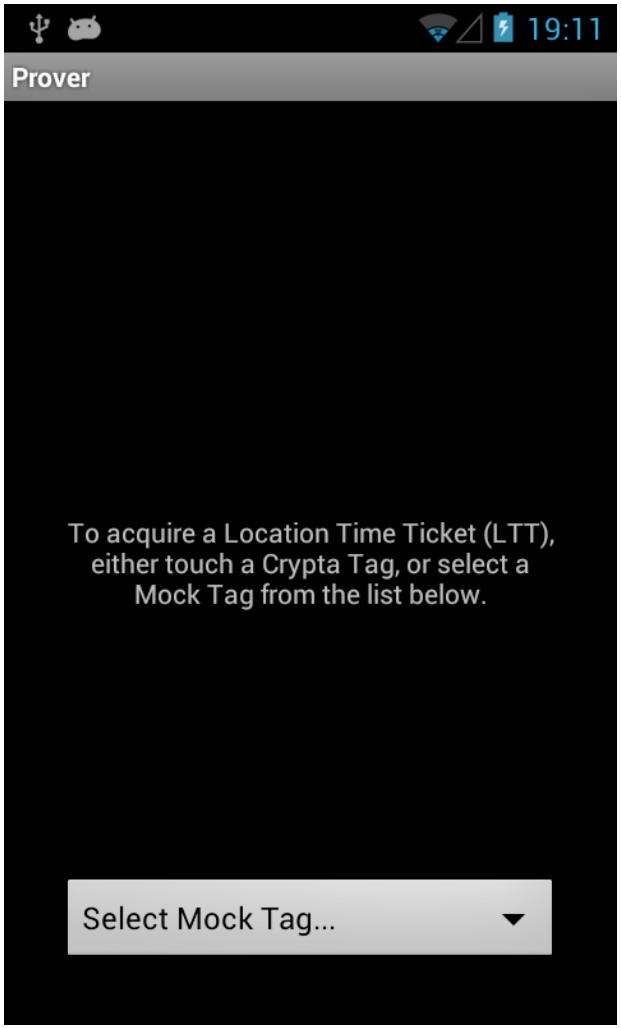
=> Mounted at fixed location; registered with TTP server

Prototype 2

Protocol



Prototype 2: Live Demo /1



Prototype 2: Live Demo /2

Location Aware Signatur...

las-ttp.appspot.com

Location Aware Signature Prototype Variant 2 (Cryptotag/NFC)

Login

Sign in for viewing LTTs and managing tags.

User Name admin

Password ••••

Login

Location Aware Signatur...

las-ttp.appspot.com

Location Aware Signature Prototype Variant 2 (Cryptotag

Start History Management Log Out

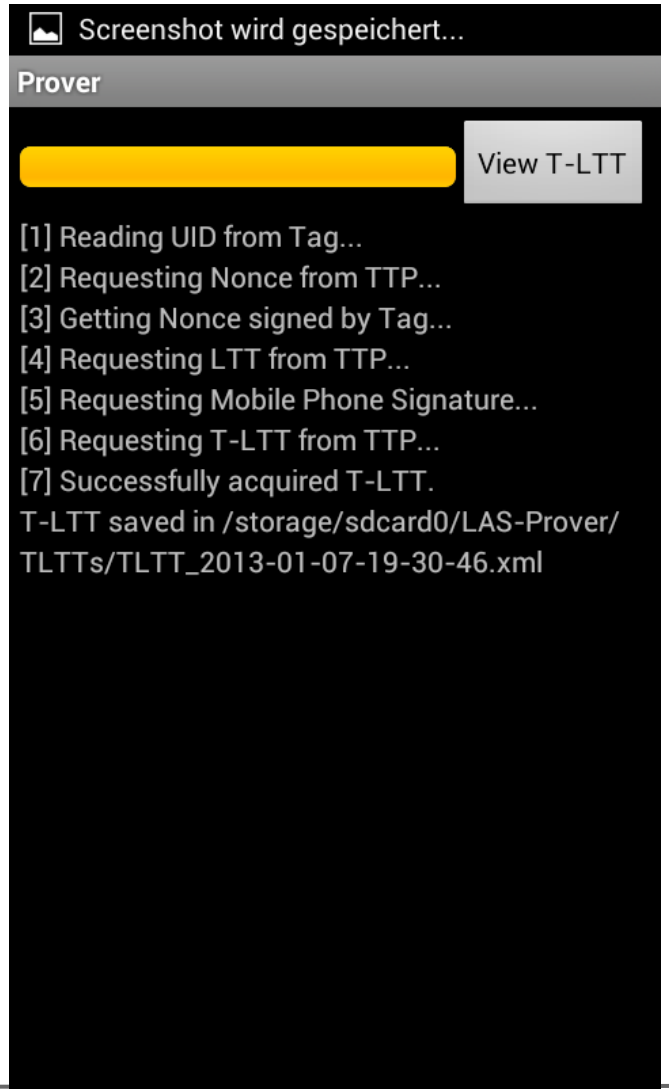
Add a new Tag

Specify the properties of the new Tag.

Name	IAIK CRYPTA Tag	An abritrary name with three or more characters.
Description	the physical one	An abritrary description.
Latitude	47.058421	Any double value between -90 and +90.
Longitude	15.457815	Any double value between -180 and +180.
UID	3F0800A0A1A2A3	A hex string in the form of XXXXXXXXXXXXXX, w
Public Key Certificate File	Choose File Tag_certificate.cer	Choose a valid X.509 Certificate stored on you PC.

Add

Prototype 2: Live Demo /3



Prototype 2: Live Demo /4

Location Aware Signatur...

las-ttp.appspot.com

Location Aware Signature Prototype Variant 2 (Cryptotag/NFC)

Start History Management Log Out

Full Log

Lists any requests to the server.

Clear Log

Time	Tag UID	Nonce	Protocol Step	Status Message
Mon Jan 07 19:30:46 GMT+100 2013	3F0800A0A1A2A3	82DE57589656489DE25D0F2E8FA9FA93	GET_TLTT	Successfully created T-LTT.
Mon Jan 07 19:30:29 GMT+100 2013	3F0800A0A1A2A3	82DE57589656489DE25D0F2E8FA9FA93	GET_LTT	Tag authenticated. Created LTT: <locationTimeTicket xmlns="http://p2.las.iaik.tugraz.at/LocationTimeTicket"> <LocationLatitude>47.058421</LocationLatitude> <LocationLongitude>15.457815</LocationLongitude> <Time>2013-01-07 18:30:29.544 GMT</Time> </locationTimeTicket>
Mon Jan 07 19:30:28 GMT+100 2013	3F0800A0A1A2A3	82DE57589656489DE25D0F2E8FA9FA93	GET_NONCE	Prover (UID=3F0800A0A1A2A3) requested a Nonce (82DE57589656489DE25D0F2E8FA9FA93).
Mon Jan 07 19:22:50 GMT+100 2013	3F0800A0A1A2A3		GET_NONCE	Tag (UID=3F0800A0A1A2A3) is not known to server.

Prototype 2: Live Demo /5

Location Aware Signatur...

las-ttp.appspot.com

Location Aware Signature Prototype Variant 2 (Crypto

Start History Management Log Out

Issued T-LTTs

Lists all Trusted Location Time Tickets (T-LTTs) issued by the server.

Time	Tag UID	Nonce	LTT	
Mon Jan 07 19:56:20 GMT+100 2013	3F0800A0A1A2A3	C2A10B56BBC68256C76E60	<locationTi xmlns="http <LocationLa <LocationLo <Time>201 18:56:13.04 GMT</Time> </locationTimeTicket>	
Mon Jan 07 19:47:58 GMT+100 2013	3F0800A0A1A2A3	DD3490AF57AD8492B6DF27	<locationTimeTicket xmlns="http://p2.las.iaik.tugra <LocationLatitude>47.058421 <LocationLongitude>15.4578 <Time>2013-01-07 18:47:50.887 GMT</Time> </locationTimeTicket>	5395 Bytes
			<locationTimeTicket	

19:53

Bearbe...

etsi:Cert></etsi:SigningCertificate><etsi:
SignaturePolicyIdentifier><etsi:
SignaturePolicyImplied/></etsi:
SignaturePolicyIdentifier></etsi:
SignedSignatureProperties><etsi:
SignedDataObjectProperties><etsi:
DataObjectFormat
ObjectReference="#reference-1-1"><etsi:
MimeType>text/plain</etsi:MimeType></
etsi:DataObjectFormat></etsi:
SignedDataObjectProperties></etsi:
SignedProperties></etsi:
QualifyingProperties></dsig:Object><dsig:
Object Id="signed-
data-1-1"><locationTimeTicket
xmlns="http://p2.las.iaik.tugraz.at/
LocationTimeTicket">
<LocationLatitude>47.058421</
LocationLatitude>
<LocationLongitude>15.457815</
LocationLongitude>
<Time>2013-01-07 18:47:50.887 GMT</
Time>
</locationTimeTicket></dsig:Object></
dsig:Signature></si:
CreateXMLSignatureResponse>

Prototype 2: Implementation

TTP - Server

- hosted on GAE/J & datastore (DB of tags in the wild)
- UI for Administration and History (GWT)
- API implementation for protocol (Hessian)

TTP - Crypto Tag (black box - public & private key provided)

- Mock Tags (for unit testing or testing without physical crypto tag)

Prover (Android App)

- RPC to API (Hessian)
- NFC communication with Crypto Tag
- Mobile Phone Signature (using Library from P1)

Prototype 2: Lessons Learned/Future

Troublesome Mobile Phone Signature on GAE

GAE SDK >= 1.7 (mid 2012): register **own** JCE provider

RPC: Android/GAE => Hessian (after setup troubles)

Fix issue in protocol by either:

- SSL encryption for communication Prover<->API
- simplify protocol by combining getNonce & getLTT

Store application download URL on Crypto Tag (Personaliz.)

Public Key Infrastructure for Crypto Tags (+ Cert. onto Tag)

MOA on Google App Engine (GAE)

TTP (Server): needs to sign & verify Mobile Phone Signature

1. URL Fetch API

   no sockets can be opened on GAE (P1 code)

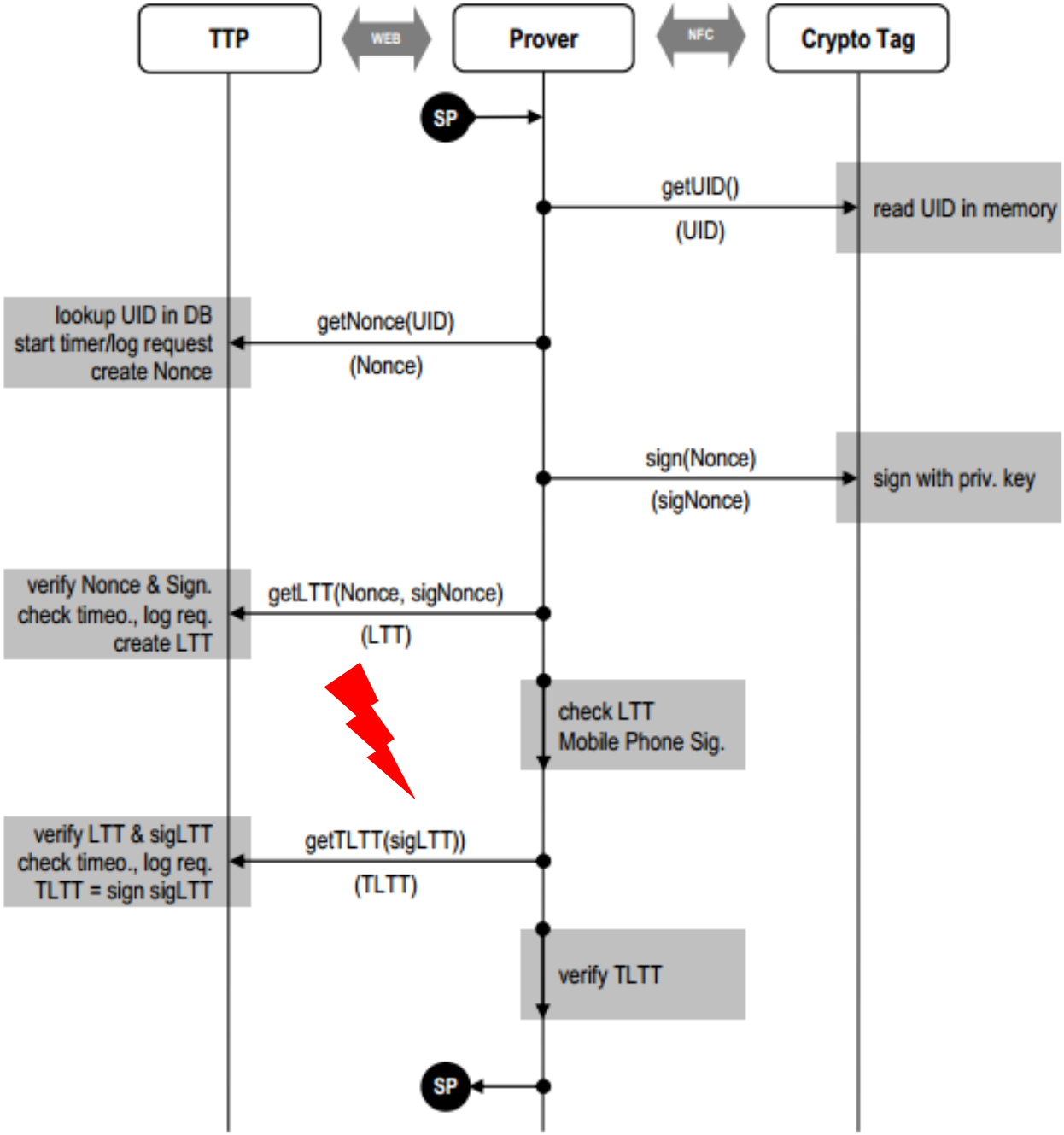
2. MOA SS/SP Java API on GAE

   GAE: limited, sandboxed JRE (JRE Class White List)
   read-only access to the filesystem (gae-filestore)
   ~~IAIK security provider~~ (resolved since GAE 1.7)
   No sockets can be opened

[MOAs in der Cloud, Bernd Zwattendorfer]

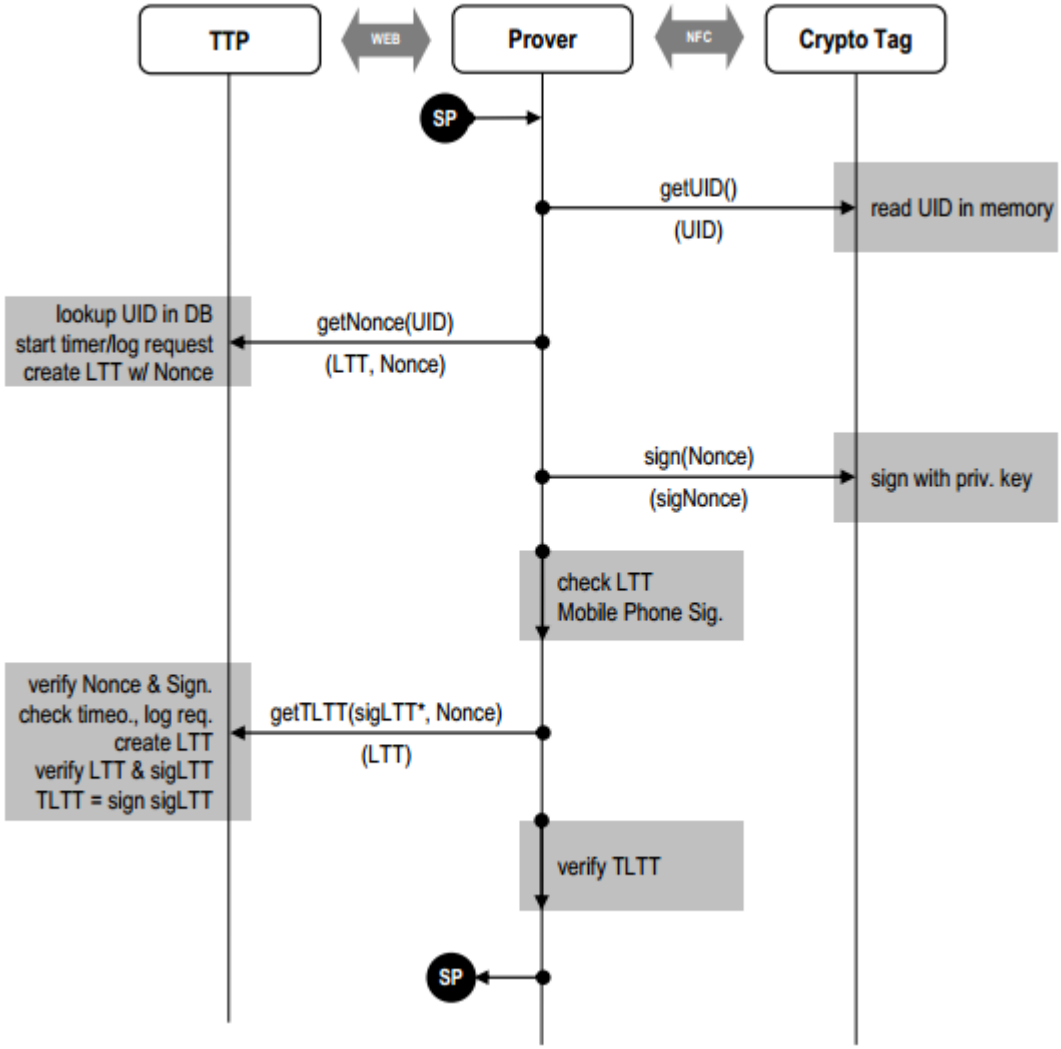
Prototype 2

Protocol



Prototype 2: Protocol Extension

Before Prover requests T-LTT by sending **getTLtt(signedLTT)** to the TTP Server, an attacker might send an unmodified LTT, but signed by himself to the TTP.



Security Analysis: Common Aspects

Protocol design & implementation

Protection of cryptographic material

Possible malicious entities

- LP ... Location Prover
- EXT ... Some 3rd party
- TTP ... Trusted Third Party

Security Analysis: Prototype 1

TTP = 2nd Smartphone and its User

- User = real person: pros and cons
- TTP has to have strong interest in use case

LP+TTP: Cooperation

LP: Malware onto TTP; Credentials; Distraction of TTP

TTP: Malware onto LP; Credentials; access to T-LTT

EXT: Malware onto LP, TTP, or TTP and LP

Security Analysis: Prototype 2

TTP = Tag (fixed location) + Server

- trusted as long as not compromised by external attack
- LTT generation on server
- thoroughly evaluated before deployment (in theory)
- TTP is not a real person

LP: proxy to malicious person (tag is not human)
LP: key extraction of tag, side-channel attacks
EXT: malware on LP smartphone

=> more possible scenarios, but also more complex

Security Analysis: Risks/Conclusion

1. Cooperation of LP and TTP in P1
   => applications where TTP has strong interest

2. Cooperation of LP and EXT in P2
   => TTP-Server cannot verify identity of LP

3. Stealing of credentials for Mobile Phone Signature (both)
   => quite difficult (two factor authentication), but possible

4. Malware injection on any involved smartphone

Conclusion

Both prototypes demonstrate technical possibility
(but Limitations with P2/GAE)

P1 serves components for P2 (Mobile Phone Signature)

Security:
Aspect 1: Protocol & Implementation
Aspect 2: General Principle of our TLBS
=> use case limitations

Trusted Location Based Services

Thank you for your Attention!

Q&A