Authentication of GNSS OS Signals through the Location Assurance Service Provider

13/03/2012

Miguel Martins
itrust consulting
martins@itrust.lu

Agenda

Agenda

- Motivation
- Background
- Overview of the project
- Current status
- Conclusion

Objectives

- Present an overview and current status of the LASP project.

Motivation

➡ Avoid the GNSS threats

Threats:

- Jamming: intentional interference to prevent receivers from tracking GNSS signals;
- Spoofing: broadcast of fake GNSS-like signals;
- Meaconing: reception, delay and re-broadcast of GNSS signals.

Motivation

➡ Business opportunity for innovative services

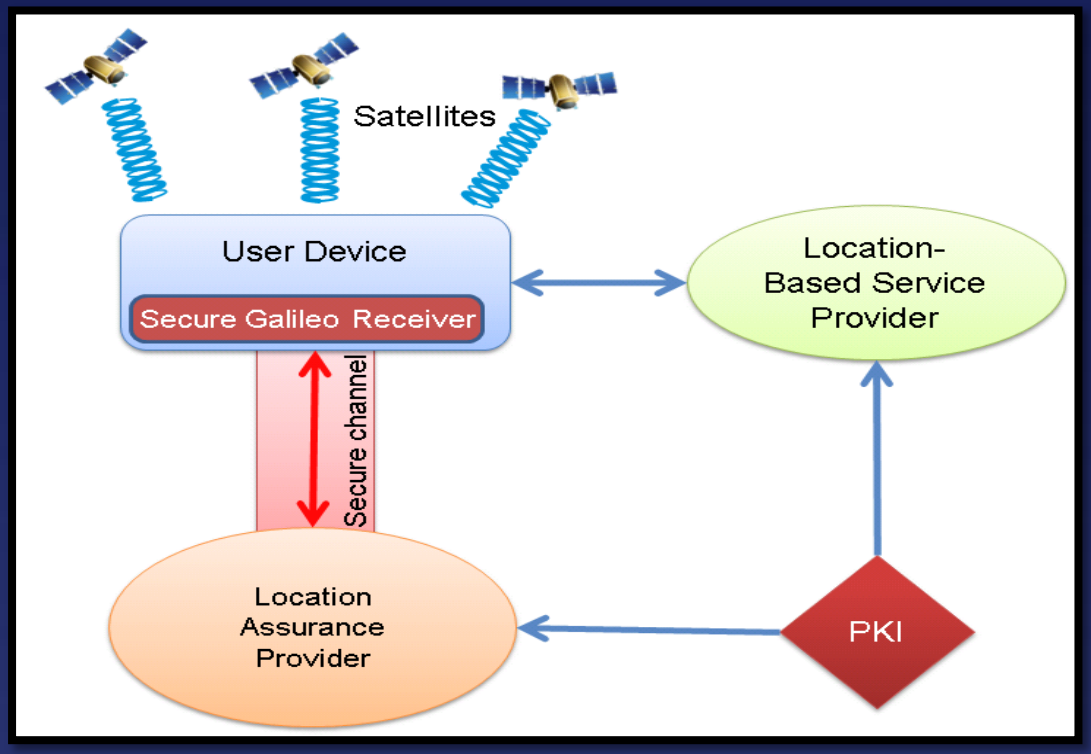
Examples of services relying on GNSS:

- Tracking of dangerous or high value goods
- Journalists in war scenarios
- Location based billing
- PAYD services:
  - Tolls – LKW-Maut (truck-toll in Germany)
  - Insurance schemes
- LBS smartphone applications

Background

➡ Past Studies

- LocProof: ESA study to define the concept
  - ➡ Functionality and security design



- LocAuth: LuxLAUNCH study of business opportunity
  - ➡ LASP service can be a real business opportunity for Luxembourg

Overview

➡ Location Assurance Service Provider

Administrative Details

- ESA funded project
- Duration: 2 years, 2011-2012
- Sub-Contractor: University of Luxembourg/SnT

Project Objectives

- Specify and implement a prototype of a localisation authority
  - Perform security checks before certifying a localisation
  - Establish secure communication protocol between LAP and user device
- Consider privacy issues (like anonymity) for privacy-enhanced services
- Demonstrate and disseminate the service

Overview

➡ Technical issues

itrust consulting s.à r.l.

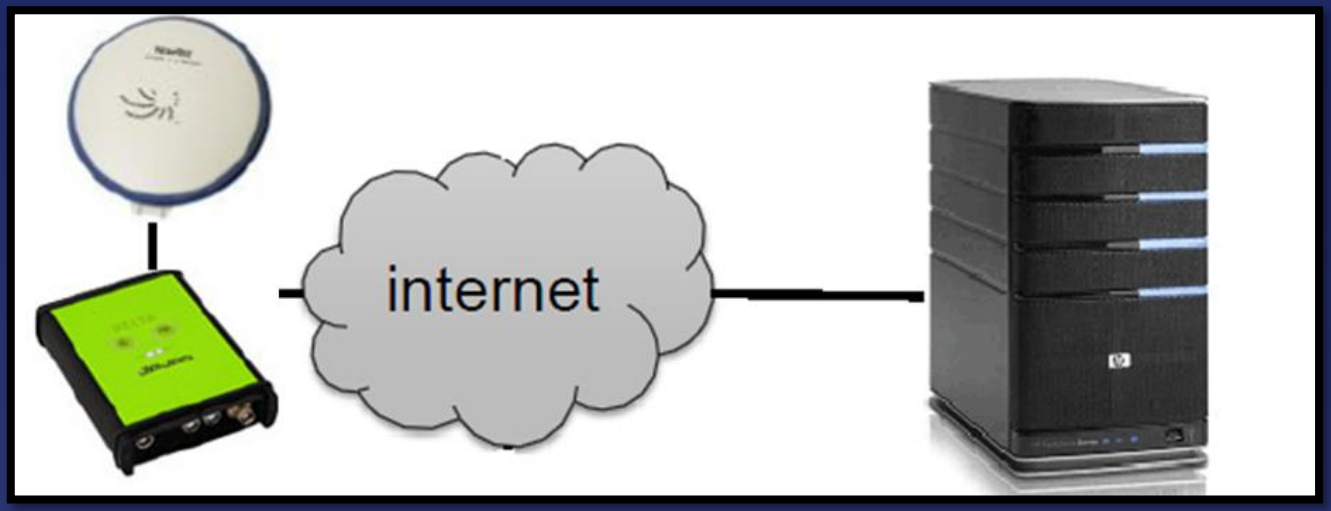
Security checks:

- UD sends time-stamped positions as well as navigation and intermediate data
- Security checks are algorithms that verify if signals are integral (not intentionally modified):
  - Local: single observation
  - Central: continuous observation or observation of multiple receivers
- Result is an assurance level. It depends on the data available

Current status

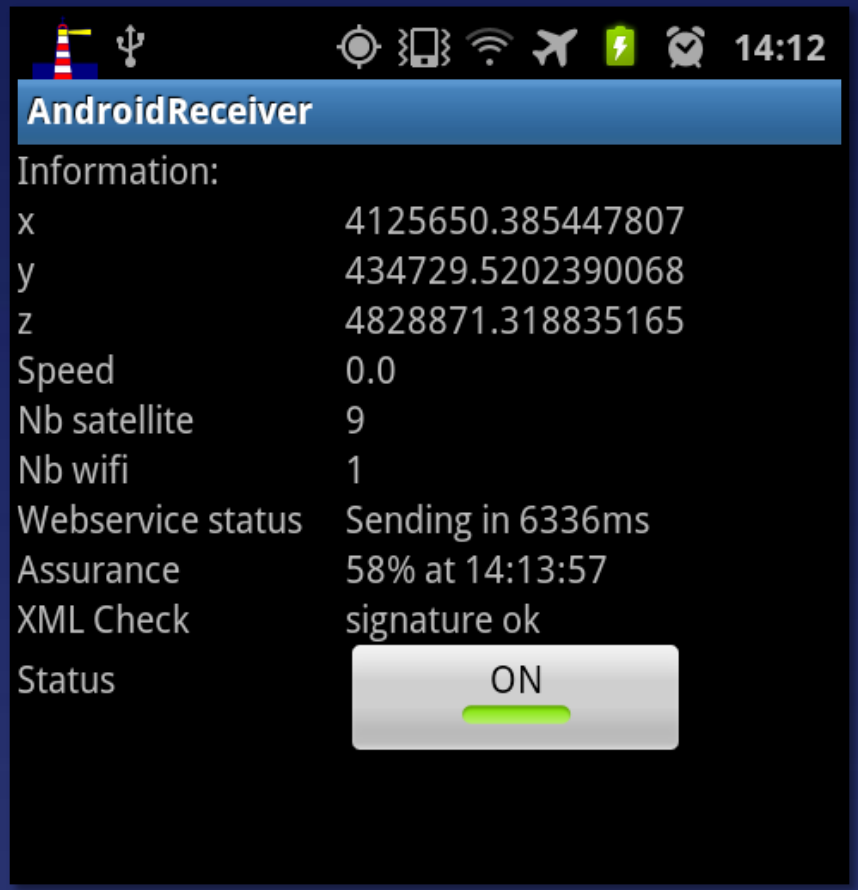
➡ Demonstrator

- Several security checks are implemented (Doppler, power, clock, navigation data,…);
- Communication client/server is working;
- A light version is available for Android.



Current status

➡ Android application



- Can be installed on any GNSS-enabled Android
- Only a subset of security checks can be performed

Current status

➡ Results

itrust consulting s.à r.l.

Achievements:

- Preliminary results are encouraging;
- Selective manipulations are reflected in the final assurance level;
- Successful detection of meaconing attacks simulated with a signal repeater (delay ≈ 80ns)

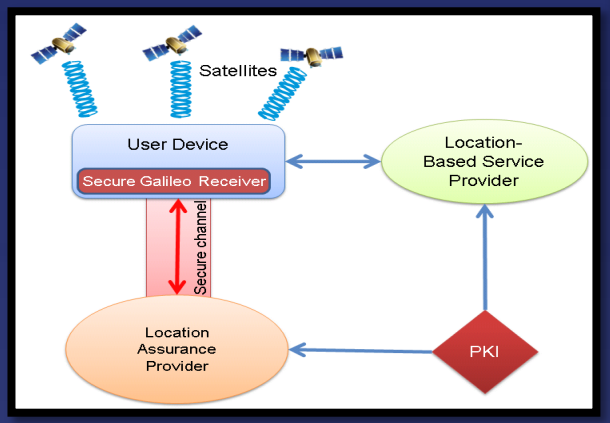
Next Steps:

- Finalise overall integration;
- Do tests at ESA with signal simulators;
- Parameter tuning.

Current status

➡ Privacy

- User's position is private information
- Leak towards the LAP is not problematic because it intends to be a TTP.
- Leak of a certified position towards the LBSP needs to be addressed.
- A proposed solution lets the user control the transmitted accuracy.



Conclusion

Conclusion:

- Localisation assurance is possible
- Preliminary tests are encouraging

Business roll-out:

- Itrust envisages the deployment of the LASP service
- Looking for partners that need some kind of localisation assurance

Technical challenge:

- Show me your spoofers!

Questions & Discussion…

Thank you for your attention!

Miguel Martins
martins@itrust.lu

About itrust consulting

➡ Versatiles services

Consultancy

- Security policies and technical expert reports
- Information risk analysis (Trick-Light)

Audit

- Hacking, intrusion test (TRICK-Tester), Computer forensics
- Process certification and data protection
- ISO 27001, ISO 27799, ISO 15408...

Training

- ISO 270xx, Security testing, Risk management, Security awareness, Security Testing.

R&D – Technical and security design

- ESA: Secure Galileo localisation
- Celtic, ITEA2 ; FP-7: MICIE, LiveLine, CockpitCI, i-GOing
- Information sharing tools for risk prediction, security assurance, management
- LuxLAUNCH innovation studies on LBS, localisation, certification, M2M,…

Multisourcing

- Security officer assistance, Security as a Service