Location Assurance Service Provider

06/11/2012

itrust consulting s.à r.l.
6 Z.I. Bombicht
L-6947 Niederanven

Tel: +352 26 176 212
Fax: +352 26 710 978
Web: www.itrust.lu

7th ICG Meeting, Beijing

Agenda

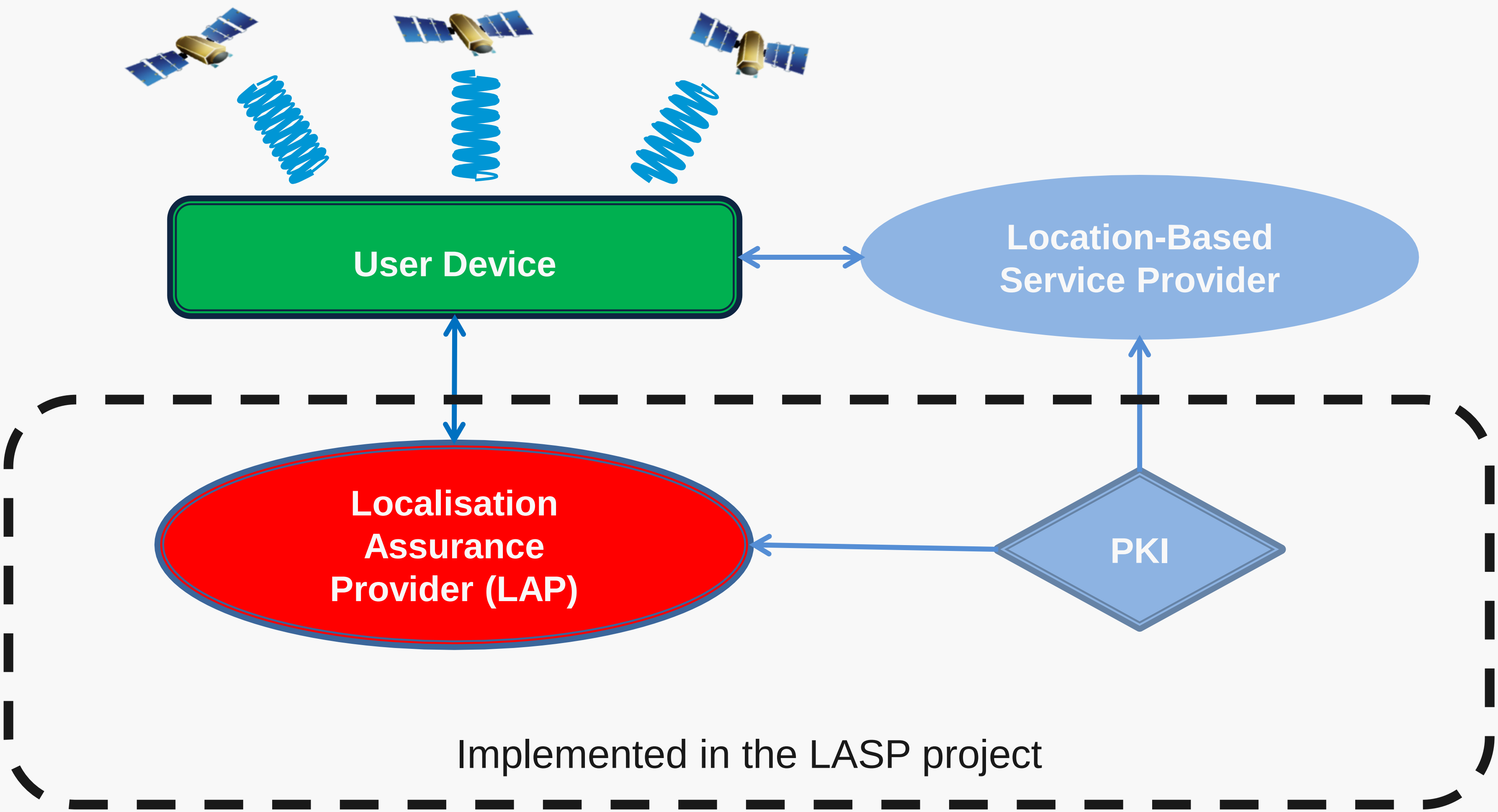
- Motivation
- Proposed solution
- Architecture of the LAP
  - Input/output
  - Confidence Checks
- Validation tests
- Confidence and privacy
- Conclusion and next steps

Motivation
Services relying on correct GNSS localisation

- Tracking of dangerous or high value goods
- Location based billing
- Pay As You Drive (PAYD) services:
  - Road tolls (e.g. trucks in Germany)
  - Car insurance (e.g. insurance schemes in the UK)
- LBS smartphone applications

Proposed solution

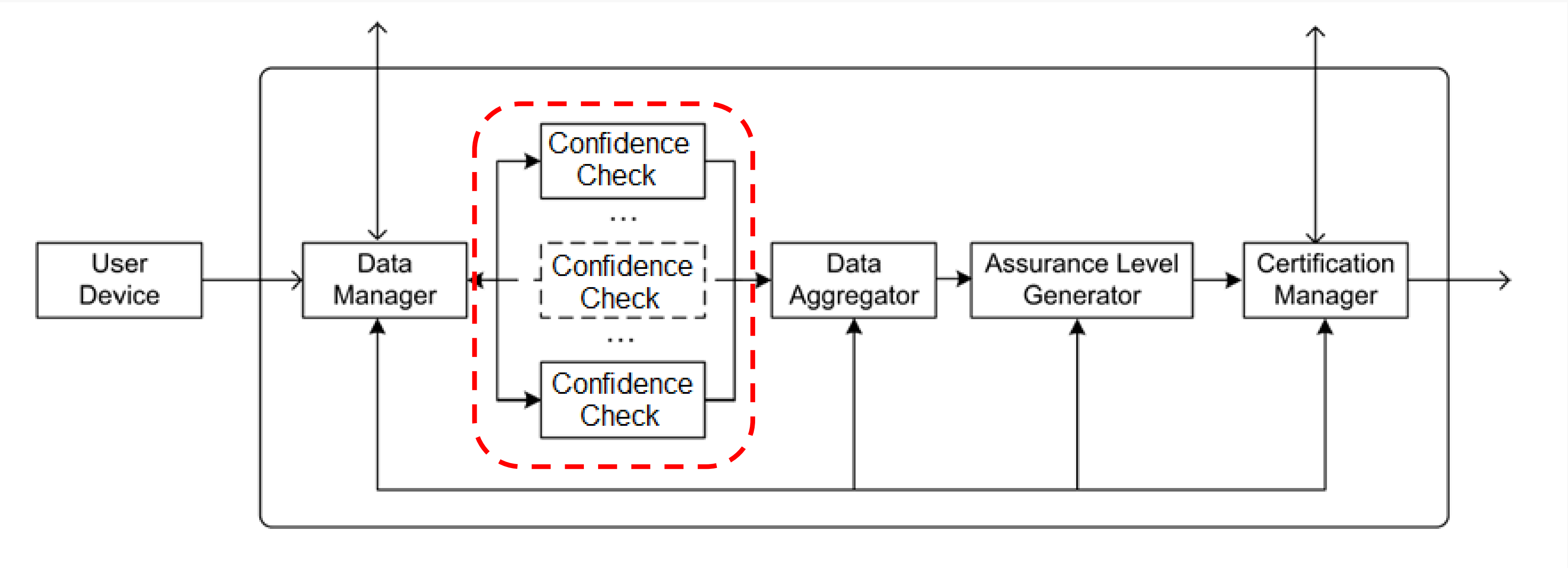
Inclusion of a Localisation Assurance Provider



LASP project
Localisation Assurance Service Provider

- Project objectives
  - Specify and implement a prototype of a localisation authority
  - Perform Confidence 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

Architecture of the LAP



- Confidence checks are algorithms that verify if signals are intact (not intentionally modified).

Input/output

- UD sends time-stamped positions as well as navigation and intermediate data;
- It receives a digital certificate.

Client Request


```
+ <position>
+ <accuracy class="data.AccuracyReceiver">
+ <velocity class="data.VelocityReceiver">
- <utc__time>
    <year>2012</year>
    <month>9</month>
    <day>4</day>
    <tod>52327</tod>
    <clock__bias>-3.8452939500586476E-4</clock__bias>
  </utc__time>
- <satellites>
  - <data.SatelliteReceiver>
      <id>3</id>
    - <signal__strength class="data.SignalStrengthGPS">
        <CA__L1>52.0</CA__L1>
        <P__L1>38.25</P__L1>
        <P__L2>38.25</P__L2>
        <CA__L2>NaN</CA__L2>
        <L5>NaN</L5>
      </signal__strength>
    - <doppler class="data.DopplerGPS">
        <CA__L1>-2784.191162109375</CA__L1>
        <P__L1>-2784.191162109375</P__L1>
        <P__L2>-2169.53369140625</P__L2>
        <CA__L2>NaN</CA__L2>
        <L5>NaN</L5>
      </doppler>
      <navigation__data>0FA8C222502952D21C00842A3F
      <azimuth>286</azimuth>
      <elevation>39</elevation>
```


Server reply

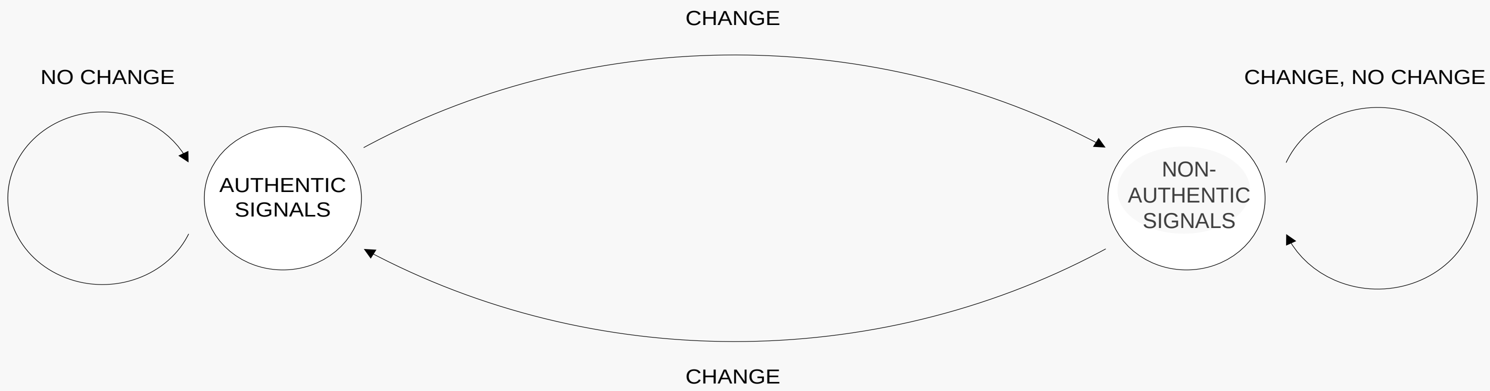

```
="1.0" encoding="UTF-8"?>

2</version>
umber>ID-LAP-ID-LAC</serial_number>
ID>3031044834779901</request_ID>
>test</issuer_ID>
ame>fff</issuer_name>
vice_ID>device_1</user_device_ID>
certificate_information>
ion>
>49.64426191596962</x>
>6.2660184518943325</y>
tion>
racy>8.836222138378647</Accuracy>
>20121019-105215</time>
rance_level>0.9210149788649977</assurance_level>
_certificate_information>
e xmlns="http://www.w3.org/2000/09/xmldsig#">
edInfo>
CanonicalizationMethod Algorithm="http://www.w3.org/T
SignatureMethod Algorithm="http://www.w3.org/2000/0
Reference URI="">
nedInfo>
atureValue>RxWEgx3xecbcgbBggMhexx3WUWySRuTK6
nfo>
re>
```

Confidence checks

- Examples of Confidence checks:
  - SNR per satellite and elevation angle;
  - Considering user and satellite dynamics, Doppler can be estimated;
  - Doppler ratio when different signals from one satellite are available;
  - Verification of navigation data with an Internet-based trusted source;
  - Calculated elevation;
  - User altitude;
  - Clock jumps;
  - Receiver Autonomous Integrity Monitoring (RAIM);
  - Consistency with Wi-Fi positioning;
  - Reachability between consecutive positions;
  - Computed time should be aligned with current time.

Confidence checks

- **State-based** can be evaluated at a single observation, e.g. SNR level or ground height;
- **Transition-based** require at least two observations and explore abrupt changes, e.g. reachability or jumps in the clock.



Confidence checks

- Each Confidence check outputs a Subjective Logic opinion composed of belief, disbelief and uncertainty;

- Results are merged using Subjective Logic operators;

- Final opinion is mapped into an assurance level between
1 and 5

Validation tests

- Tests with GNSS signal generator:
  - Implementation works correctly;
  - By properly controlling the transmitted power, the non-authentic signals can remain unperceivable;
  - LAP is not fool-proof...
  - Literature suggests more than what can be achived in practice:
    - The Doppler values estimated based on user dynamics are corrupted because user dynamics is estimated based on Doppler measurements;
    - Power correlation among different satellites exhibits multiple false alarms – signals’ SNR are naturaly correlated.

Confidence and privacy

- Communication between user device and LAP are secured;
- LBSP can check if the localisation assurance certificate was issued by the LAP through a PKI;

- Users can control up to which level of granularity service providers will know about their locations;
- In fact, service providers receive certified but encrypted locations, and their ability in decrypting is given to them by users.

  E.g. 40.7XXXXX° instead of 40.713361°

Conclusion and next steps

- Conclusion:
  - LAP provides end-users with an assurance level reflecting the level of trust of a localisation;
  - Many non-authentic signal scenarios can be detected;
  - LAP considers Confidence and privacy issues in whole service;

- Next steps:
  - Assess the interest of end-users on signal authentication;
  - Design a commercial exploitation service and establish a business plan;
  - Compare LASP solution with services providing built-in Signal-in-Space authentication.

itrust
consulting

Any questions?

Thank you for your attention

Project team: LASP@itrust.lu