Secure Localisation with Location Assurance Provider

ENC-GNSS 2009

Dr Carlo Harpes

Benoît Jager

Brian Gent

Project supported by
ESA contract 21753-08

itrust consulting s.à r.l.
18, Steekaul
L-6831 Berbourg
www.itrust.lu

Nokia Siemens Networks
20, rue des Peupliers
L-2328 Luxembourg-Hamm
www.nokiasiemensnetworks.com/lu/

Agenda

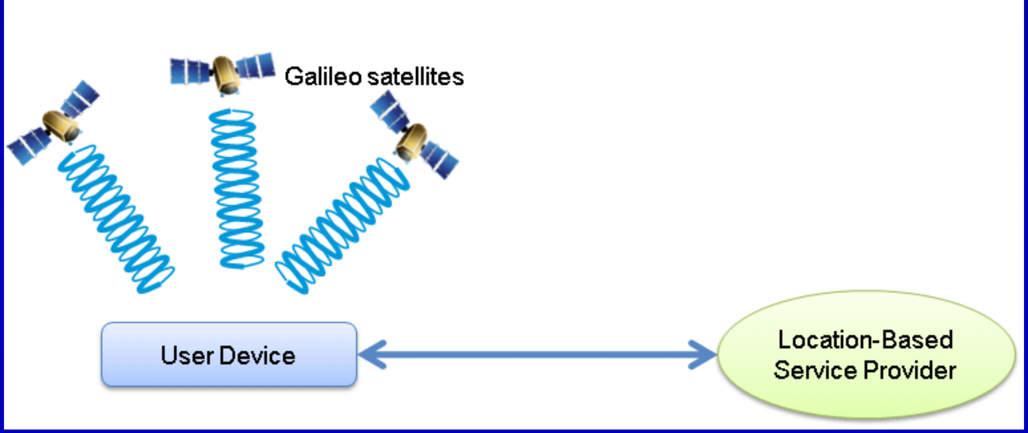
1. Context and objectives
2. Threats on Galileo
3. Security measures
4. Location Assurance Provider architecture
5. Missing Galileo navigation message authentication
6. Security requirements (cf ISO 15408 Common Criteria)
7. Conclusion

1. Context…

Over the last 10 years, GNSS became a widely used technology.

Enabled development of Location-Based Service (LBS)

Permits location-based access control.



Galileo Open Service has multiple weaknesses:

- Signals cannot be authenticated: any adversary could generate a false signal to mislead localisation;
- Any hacker could potentially manipulate the software or firmware executing the localisation algorithms on an ordinary GNSS receiver.

which prevents deployment of LBS requiring high-level of trust: Secure parcel delivery, tracking of journalist, Secure container tracking, goods and hazardous transportation, …

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

1. … and objectives

- Determine which threats could occur with Galileo;
- Make a review of existing projects, papers in relation to location proofs mechanisms;
- Use identified location proofs mechanisms to design an architecture scheme enabling to get location assurance;

Agenda

1. Context and objectives

2. Threats on Galileo

3. Security measures

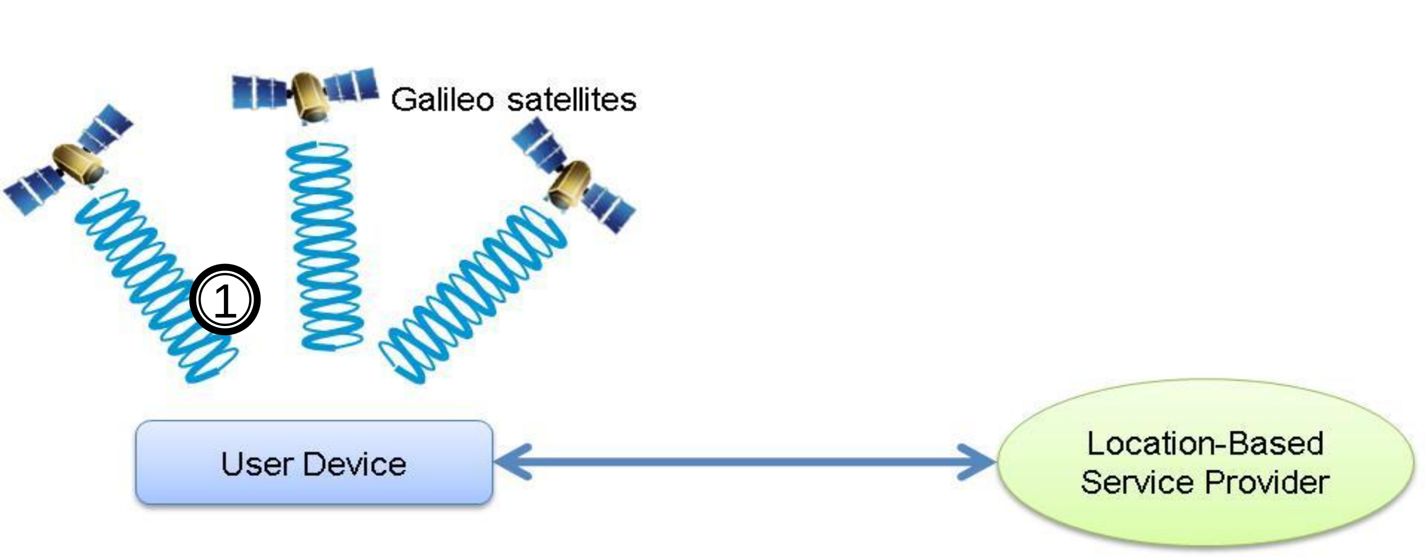
4. LAP architecture

5. Missing authentication

6. Common Criteria

7. Conclusion

2. Threats on Galileo



① Galileo signals

Shielding: insert noise into Galileo signals to prevent right localisation.

Jamming: prevent reception of Galileo signals.

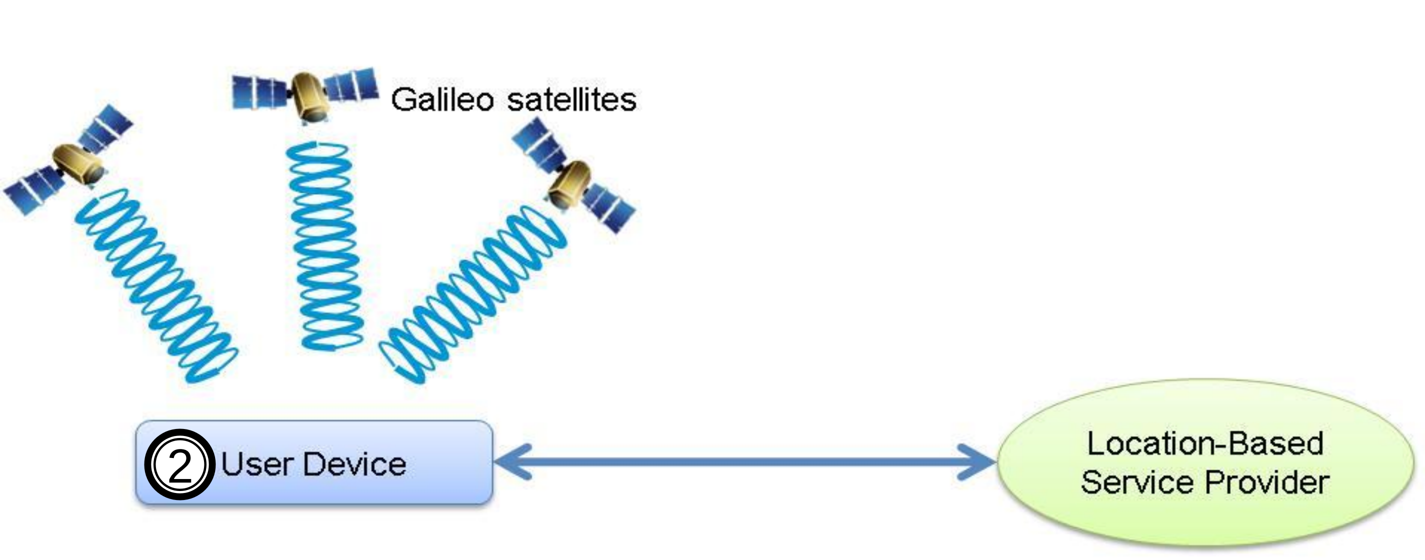
Meaconing: interception and delaying of Galileo signals to confuse receiver during localisation.

Spoofing: coherent modification of Galileo signals in order that receivers compute a defined location.

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

2. Threats on Galileo



2 Galileo receiver

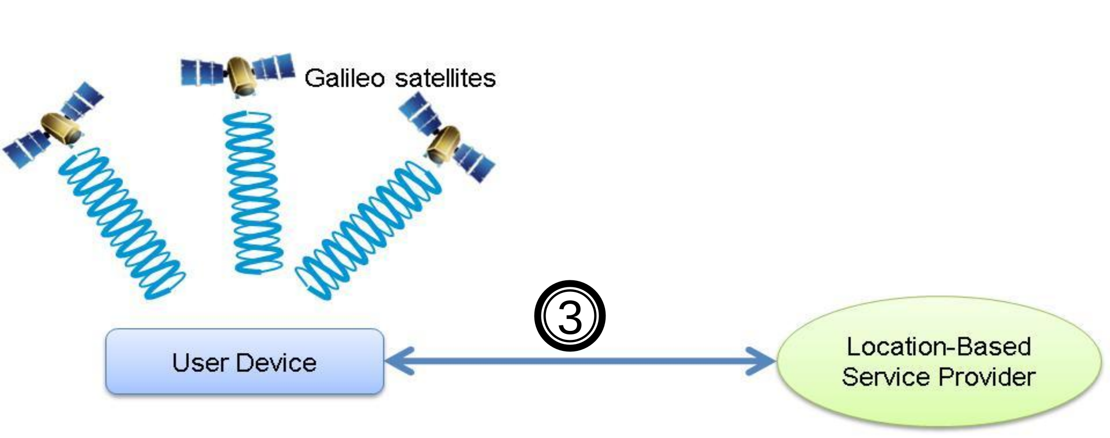
Software code spoofing: an infected software is installed inside Galileo receiver and sends false locations to the LBSP.

User is the attacker: user directly sends false locations to the LBSP.

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

2. Threats on Galileo



③ Channel between UD and LBSP

Message manipulation

Man in the middle: attacker impersonates both UD and LBSP and is then able to send fake location to the LBSP.

We used the threat list of MAGERIT
= risk analysis and management methodology for information systems

Out of scope threat types:

- Natural disasters
- Of industrial origin
- Errors and unintentional failures

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

05/05/2009

3. Security measures

Analysed papers

[1] Guenter W. Hein, Felix Kneissl, Jose-Angel Avila-Rodriguez and Stefan Wallner: Authenticating GNSS Proofs against Spoofs; Inside GNSS; September/October 2007.

[2] Oscar Pozzobon, Chris Wullems and Kurt Kubic: Secure Tracking using Trusted GNSS Receivers and Galileo Authentication Services; In Journal of Global Positioning Systems (2004) Vol. 3, No 1-2.; 2005.

[3] Logan Scott: Location Assurance; GPS World; 1 July 2007.

[4] Dave Singelée and Bart Preneel: Distance Bounding in Noisy Environments; Leuven, Belgium; 2007.

[5] Markus Kuhn: An asymmetric mechanism for navigation signals; Lecture Notes in Computer Science, Volume 3200/2005; Springer Berlin / Heidelberg; 2005.

[6] Edward Felten and Brent Waters: Secure, Private Proofs of Location; Princeton Computer Science TR-667-03; 2003.

[7] Todd E. Humphreys, Mark L. Psiaki, Paul M. Kintner, Jr., Brent Ledvina and Brady O' Hanlon: Assessing the Spoofing Threat; GPS World; January 2009.

Agenda

1. Context and objectives

2. Threats on Galileo

3. Security measures

4. LAP architecture

5. Missing authentication

6. Common Criteria

7. Conclusion

3. Security measures

Relevant security measures:

- **Spread Spectrum Security Codes (SSSC)**: synchronous cipher streams seeded by an unsent digital signature from an Authentication Navigation Message;
- **Received Clock Bias (RCB)**: comparison between computed time (localisation) and internal user device time;
- **Received Signal Strength (RSS)**: monitor the quality of the power of the Galileo signals;
- **Tamper Resistant Device (TRD)**: preventing a user from tampering with the user device.
- **Navigation Message Authentication (NMA)**: digital signature of navigation data for delayed authentication;

Conclusion
• Cryptographic security measures cannot provide complete security against all theoretical attacks.
• Non-cryptographic countermeasures will remain a valuable and necessary complement.

Agenda

1. Context and objectives

2. Threats on Galileo

3. Security measures

4. LAP architecture

5. Missing authentication

6. Common Criteria

7. Conclusion

3. Security measures

Other security measures not found in these papers:

- **Central Assurance Provider:** centralising the entity which will decide if a location is trustworthy based on risk management principles (-> Location Assurance Provider);
- **Tracking and Plausibility Checks:** monitoring of the localisation, derivation of speed and comparing speed and location with parameters applicable for a given device;
- **Public Key Infrastructure:** to digitally sign a user device location together with an attribute indicating the *assurance level*.

-> Location Assurance Certificate (LAC)

Agenda

1. Context and objectives

2. Threats on Galileo

3. Security measures

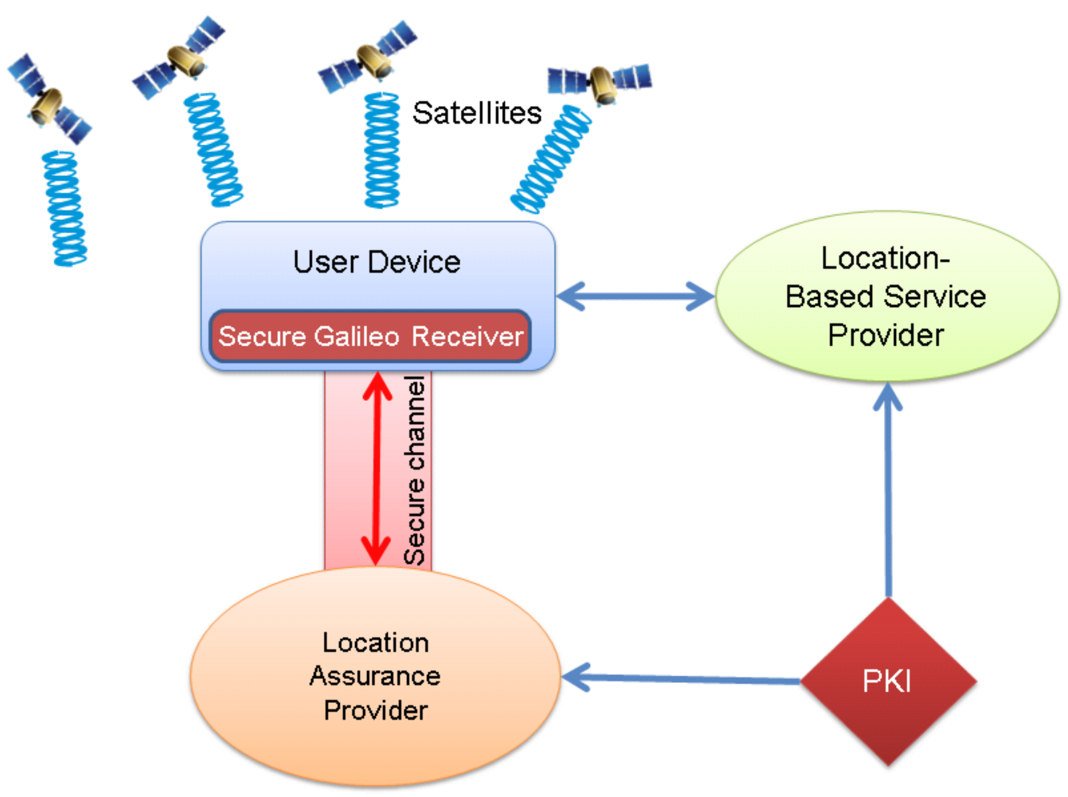
4. LAP architecture

5. Missing authentication

6. Common Criteria

7. Conclusion

4. Location Assurance architecture



Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

4. Location Assurance architecture

1. Send of Galileo signals

The operation of the architecture begins with the sending of Galileo signals. The signal includes Ephemeris information, Almanacs information, Clock correction, ionospheric correction…

2. Location computation

User device computes its location using signals coming from Galileo constellation.

In order to fulfil this function in a trustworthy way, the receiver uses a Secure Galileo Receiver implementing Tamper Resistant Device (TRD), in order to make sure that the localisation based on multilateration is integer.

3. Request of Location Assurance Certificate

User device requests a LAC, sending location, time of location, Clock bias, Satellite signal strength, etc to the LAP.

Channel between the UD and the LAP must be secure i.e. require integrity (prevent data tampering), confidentiality (attacker unable to trace an UD) and availability (guarantee the service) of data.

4. Location Assurance architecture

4. Location assurance level determination

Location Assurance Provider analyses receiver information and determine level of assurance of receiver location, after several *security checks*: RCB, RSS, TPC.

Assurance levels depend on the results of the check executed by the LAP.

5. Location Assurance Certificate returned

LAP generates a LAC and returns it to the receiver.

6. LAC forwarding

The User Device can forward LAC to its LBSP in order to request a service (proof its location.

7. LAC validity checking

LBSP checks LAC validity using PKI before authorising the User Device to access to a service.

Agenda

1. Context and objectives

2. Threats on Galileo

3. Security measures

4. LAP architecture

5. Missing authentication

6. Common Criteria

7. Conclusion

5. Missing Galileo navigation message authentication

Problem

- Galileo Open Service comes with no authentication
- => Attacker can modify content of Galileo messages

Different authentication strategies:

- Cryptographic authentication
- Comparison with Reference UD
- Signal authentication (not really considered here)

Data to protect:

- Ephemeris
- GST Time
- Clock correction
- Ionospheric correction

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

5. Missing Galileo navigation message authentication

Solution 1 Use spare bits of Galileo signal content to add authentication

Firstly, determine number of available spare bits :

	F/NAV		I/NAV			
Time (s)	E5a	Total E5a	E5b	Total E5b	L1b	Total L1b spare bits
10	26	26	144 (31)	144 (31)	37 (14)	37 (14)
20	0	26	447 (7)	591 (38)	336 (7)	373 (20)
30	8	34	303 (183)	894 (221)	234 (200)	607 (221)
40	5	39	144 (31)	1038 (252)	37 (14)	644 (235)
50	0	39	447 (7)	1485 (259)	336 (7)	980 (242)
60	26	65	303 (183)	1788 (442)	234 (200)	1214 (442)
70	0	65	144 (31)	1932 (473)	37 (14)	1251 (456)
80	8	73	447 (7)	2379 (480)	336 (7)	1587 (463)
90	5	78	303 (183)	2682 (663)	234 (200)	1821 (663)

Values in brackets are without SoL authentication fields

Secondly, consider length of cryptographic algorithms:

Scheme	Key size (lifetime of 20 years)	Signature size (bit)
DSA	1024	320
DSA	2048	448
DSA	3072	512
ECDSA	160	320
RSA	1600	1024

Length of digital signature

HMAC	Output size (bit)
HMAC-SHA-0	160
HMAC-SHA-1	160
HMAC-SHA-256	256
HMAC-SHA-384	384
HMAC-SHA-512	512

Length of MACs

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

5. Missing Galileo navigation message authentication

Cryptographic authentication possibilities according to spare bits available and lengths of authentication codes.

	Symmetric	Asymmetric
F/NAV	Verification every 50 seconds Truncated MAC (26 bits)	Not acceptable since 400 observation period before signing is too long (DSA 320 bits).
I/NAV	Verification every 30 seconds MAC with 160 bits	Verification every 60 seconds Digital signature: DSA 320 bits
I/NAV + SoL	Idem as without SoL	Verification every 30 seconds Digital signature: DSA 320 bits

Summary of authentication design for different signals

Criteria	Symmetric	Asymmetric
Key management	Very difficult or unsecure	Easy
Computation time on satellite	Expensive	Very expensive
Signal Spoofing	Still possible	Still possible

Main concerns on message authentication

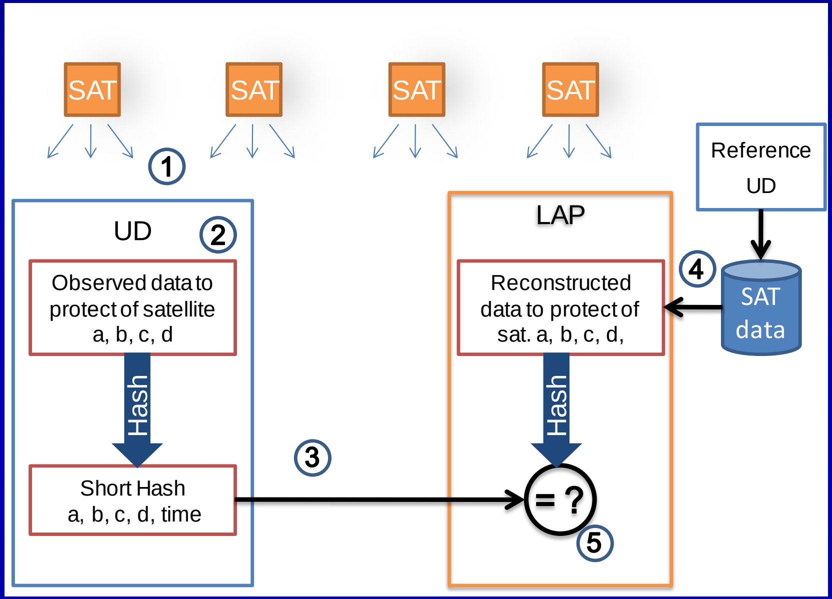
Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

5. Missing Galileo navigation message authentication

Solution 2

Simply comparing the input data of the localisation algorithm with a secure data reference.



SAT
SAT
SAT
SAT
1
Reference UD
UD
2
Observed data to protect of satellite a, b, c, d
Hash
Short Hash a, b, c, d, time
3
LAP
4
SAT data
Reconstructed data to protect of sat. a, b, c, d,
Hash
= ?
5

Central Message Authentication (CMA) architecture

Reference UD:

User Devices distributed over earth surface capturing and sharing Galileo signals received to the LAP.

Advantages if combined with LAP:

- Fast authentication verification rate (any time)
- Does not require to modify Galileo signal specifications

Disadvantages:

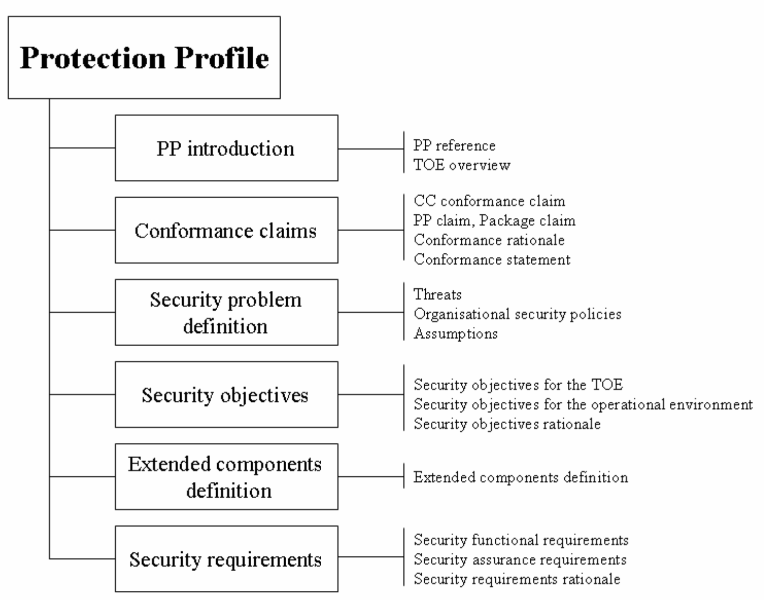
- But only as commercial service
- Depend on availability of the LAP

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

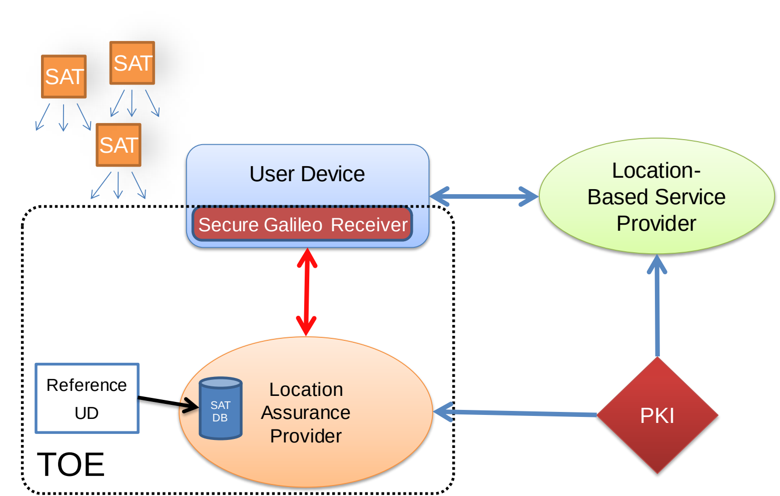
6. Security requirements with ISO 15408

We defined a protection profile for the LAP:



Protection Profile

- PP introduction
  - PP reference
  - TOE overview
- Conformance claims
  - CC conformance claim
  - PP claim, Package claim
  - Conformance rationale
  - Conformance statement
- Security problem definition
  - Threats
  - Organisational security policies
  - Assumptions
- Security objectives
  - Security objectives for the TOE
  - Security objectives for the operational environment
  - Security objectives rationale
- Extended components definition
  - Extended components definition
- Security requirements
  - Security functional requirements
  - Security assurance requirements
  - Security requirements rationale



TOE = Target of Evaluation

Protection profile (PP): allows creation of generalised and reusable sets of security requirements. The PP can be used by prospective consumers for specification and identification of products with IT security features which will meet their needs.

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

6. Security requirement with ISO 15408

Examples of threat:

T.TAMPER_RUD

Reference UD are configured to capture Galileo signals and send them to a centralised server. An attacker could try to tamper the behaviour of reference UD (e.g. fake software update, spoofing) in a manner enabling to change centralised Galileo signal content as for a spoofed Galileo receiver..

T.GNSS_MEACONING

An attacker uses a receiver/sender to replay Galileo signals.

	T.TAMPER_RUD	T.TAMPER_SATDB	T.LOSSDATADB	T.RUD_LAP_MAN_IN_THE_MIDDLE
O.CHANNEL_SECURE				X
O.CRYPTO	X			X
O.DETECT_RUD_ATTACK	X			
O.LAP _RECOVERY			X	
O.LAP _SECURE		X	X	
O.LAP_PROTECT_ACCESS		X	X	

Example of Security Objectives:

O.DETECT_RUD_ATTACK

The TOE shall detect attempts at physical tampering on the RUD and directly stop collecting satellite signal data. Each RUD should have anti-meaconing measures (e.g. using a LAP service for itself). Redundancy of RUD should be used to prevent attack of the RUD at the same time. Comparing the data of the RUD with data of real UD also allows detecting inconsistent data of a RUD.

Example of Security Requirements:

FIA_AFL.1.1

The LAP shall detect when unsuccessful authentication attempts occur related to the authentication of the SGR.

FIA_AFL.1.2

When the defined number of unsuccessful authentication attempts has been met or surpassed, the LAP shall restrict access to the LAP services for the SGR user.

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

9. Conclusion

Central Provider of Location Assurance is an innovative idea !

It enhances security of Galileo localisation and enables use of Galileo in high-secure applications.

No modification requirements of Galileo signals, as our architecture is based on LAP, PKI, Secure Galileo Receiver, GPRS or UMTS technologies…

Could be adapted to provide Location Assurance for all existing GNSS (GPS, GLONASS…).

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion

10. Questions and Answers

Thank you for your attention !

Dr Carlo Harpes
Benoît Jager
Brian Gent

Agenda

1. Context and objectives
2. Threats on Galileo
3. Security measures
4. LAP architecture
5. Missing authentication
6. Common Criteria
7. Conclusion