*Journal of Global Positioning Systems (2004)*
*Vol. 3, No. 1-2: 200-207*

Journal of Global Positioning Systems
2004
© CPGPS

# Secure Tracking using Trusted GNSS Receivers and Galileo Authentication Services

**Oscar Pozzobon[1], Chris Wullems[1], Kurt Kubik[2]**

[1] Qascom, Via O.Marinali 87, 36061 Bassano del Grappa (VI), Italy
e-mail: o.pozzobon@qascom.com, c.wullems@qascom.com; Tel: + 39 0424-525-473; Fax: +39 0424-527-800
[2] University of Queensland, Brisbane QLD, Australia
e-mail: kubik@itee.uq.edu.au; Tel: +61 7-3365-8328; Fax: +61 7-3365-4999

Received: 08 December 2004 / Accepted: 03 February 2005

**Abstract.** This paper describes a secure framework for tracking applications that use the Galileo signal authentication services. First a number of limitations that affect the trust of critical tracking applications, even in presence of authenticated GNSS signals, are detailed. Requirements for secure tracking are then introduced; detailing how the integrity characteristics of the Galileo authentication could enhance the security of active tracking applications. This paper concludes with a discussion of our existing tracking technology using a Siemens TC45 GSM/GPRS module and future development utilizing our previously proposed trusted GNSS receiver.

**Key words:** Galileo, GPS, security, authentication, privacy, tracking

## 1 Introduction

In recent years there has been an increasing presence of real time tracking applications in the GNSS (Global Navigation Satellite Systems) market. It is possibly one of the fastest growing areas in GNSS, however, fast growth brings with it significant drawbacks such as the lack of standardization and security support for applications that require security for revenue protection or even safety critical services.

The emergence of low cost GSM GPRS (General Packet Radio Service) providing wireless communications throughout Europe has fuelled rapid growth in the development of embedded, application specific platforms, which provides low-cost telematic solutions that are easy to integrate. This rapid growth has happened at the expense of a suitable security framework for development of safety-critical or financially-critical applications. To date there are few telematic solutions on the market that even offer security services. Most rely on the flawed encryption and key establishment protocols of GSM. One of the most significant issues with GSM encryption is the lack of support for cryptographic integrity protection.

The increase of tracking applications has resulted in the emergence of a number of new applications including GPS based road toll payments, GPS based insurance policy, location-based access control, finance and tracking for security. A number of these applications will be introduced in the following sections.

### 1.1 GNSS based road toll collection

Future road toll collection systems are planned to be based on GNSS technology in order to reduce infrastructure costs and to achieve region based tax collection facilitating regional tolling variations such as pollution-tax for highly polluted areas. As taxes are calculated based on location data from a GNSS receiver, it is imperative that location data is trusted. An additional concern is management of privacy in these technologies. This issue is to a large extent sill unresolved, as location data obtained by operators of these schemes are hardly controlled by the user.

In mid-2003, the EC (European Commission) adopted a proposal (COM(2003) 488) to align the national systems of road tolling for heavy-goods vehicles in Europe. This directive does not impose a particular technical solution, but another EC communication (COM(2003) 123) proposes the use of GNSS positioning and GSM/GPRS mobile communications for new electronic toll systems from 2008 onward (for all vehicle types). In addition, it proposes that migration from legacy microwave systems

to GNSS / mobile communications should be complete by 2012. Authentication, availability and integrity of the location data will be the main technical problem for revenue protection of toll operators. From the user perspective, privacy continues to be the biggest concern, which will demand innovative solutions for the management of location data privacy.

### 1.2 GNSS based insurance policy

GNSS tracking systems can be applied to insurance in obtaining time usage and location travelled by insured vehicles. This will permit insurance companies to create pay per usage policies. For some users this would result in cost reduction, as the policy cost can be estimated by vehicle usage as total kilometres, risks of travelled regions, average speed, time usage and time based risk. The use of this type of information in insurance policies continues to be an active area of research. A number of experiments have been conducted by Norwich Union and IBM in this area to test the user responses and system reliability.

### 1.3 GNSS based aircraft tracking

The Future Air Navigation System (FANS) is an example of aircraft tracking using a system facilitating a free flight. In this technology, FANS is responsible for communications, navigation and surveillance. The Flight Management Computer (FMC) uses GPS, inertial measurements, air data, and other navigation radios if available to facilitate surveillance by a traffic management (ATM) center, such that aircraft can be tracked at all times. The security of this system is important where there is an absence of radar systems to verify the reported location of the aircraft. Security of the data transmitted to the ATM is particularly critical in this situation, as it can assist in preventing intentional location spoofing.

### 1.4 GNSS based access control and auditing

Location can be used for the enhancement of access control systems and auditing. There are many applications where location context information can supplement existing security. Such applications would utilize location from GNSS systems in providing location-based audit trails, or access control policy where resources are granted or denied based on the location of a user. Security and trust of location is particularly important in this type of application, as insecure location acquisition would not only result in serious security breaches, but a false sense of security.

## 2 Limitations of existing technologies

There a number of security issues with tracking systems which utilize existing GNSS and telematic devices. These issues limit the potential for development of critical applications. The most significant limitations are:

1. Lack of signal authentication: There is no civil method to authenticate the GPS signal;
2. Lack of framework or standardized methodology to verify the integrity of a device and assess its security;
3. Lack of standardized telematic protocols that provide communications security; and
4. Significant privacy issues, such that it is difficult to obtain the location and preserve privacy at the same time.

The following subsections discuss these limitations in terms of signal authentication, device integrity and telematic security.

### 2.1 Signal authentication

There have been a number of recent efforts to quantify the extent of vulnerabilities and limitations the GPS civil signal imposes on civil applications in the presence of malicious attacks. Perhaps the most prominent vulnerability analysis was the report on the vulnerabilities of GPS in transportation, performed by the Volpe center for the US Department of Transportation (Volpe 2001).

As the GPS civil signal is not authenticated, it is possible to simulate it. In recent years simulators have become readily available, such that a GPS simulator can be hired relatively cheaply and can be connected to the antenna of a GPS receiver in a vehicular tracking module for example. Because of the possibility of signal simulation, the current generation of GPS tracking modules poses a potential security risk for use in safety or financially critical applications, such as the tracking of hazardous materials.

The U.S. Senate has recently approved a measure providing funds for the Transportation Security Administration (TSA) to develop measures for tracking trucks carrying hazardous materials (HAZMAT). As stated by (Gibbons 2004) More than 800,000 shipments of hazardous materials take place in the United States every day, including flammable fuel products, potentially explosive fertilizers, and volatile chemicals. GPS signal authentication is necessary for secure tracking in order to prevent a hijacker from simply spoofing the reported location.

The risk of signal simulation attacks is significantly reduced where the cost of hiring a signal simulator

outweighs the potential cost savings in defeating a tracking system. An example of this is performing a simulation attack in order to avoid the payment of road tolls or to cheat an insurance company by falsely reporting the number of kilometers traveled.

In addition to GPS signal spoofing, there is the potential for spoofing of augmentation data. The most widely used augmentation systems are satellite based augmentation systems including the European Geostationary Navigation Overlay Service (EGNOS) and the American Wide Area Augmentation System (WAAS). Both these augmentation systems do not provide authentication or cryptographic integrity protection. Spoofing of the correction data provided by these systems can introduce small but significant errors, which may be problematic where a few meters of error is critical.

### 2.2 Device integrity

A typical tracking device is composed of a GPS module and a communications module such as a GPRS modem or radio modem. Some tracking devices additionally contain a microprocessor with software to process the data from the GPS module. There are a number of limitations of current GPS modules:

- There is no cryptographic authentication or integrity protection of NMEA position, time or velocity data sourced from the GPS module; and
- The NMEA location data from the GPS module can be trivially simulated.

In addition to the limitations of GPS modules, the lack of authentication and end-to-end communications security between the tracking device and the telematic server can exacerbate the possible attacks that can be performed, such as masquerading as the tracking device to spoof the location.

### 2.3 Privacy

The growth of GNSS tracking applications has also created significant privacy concerns. The first techniques for managing privacy where proposed by (Spreitzer and Theimer 1993). These techniques were based on a location broker residing in the middleware layer. In recent times, considerable research has been conducted in the specification of protocols and policy representations in the context of a cellular location. For tracking applications, privacy is an issue for both single purpose tracking devices and multipurpose ones. For single purpose tracking, a user may be concerned with the usage of the location data by the destination application. Where a tracking device is used in a multi-application context, such as a device supporting both toll-payment and insurance tracking applications, the user must be able to configure privacy policies such that only the absolute minimum required location data for a given application is provided.

The user in effect should be able to adjust the accuracy of the location observations depending on the intended use and identity of the recipient, and the compliance with user's privacy policy. The most prominent effort to create location privacy standards outside the cellular domain is seen in the Geographic Location/Privacy (Geopriv[1]) working group of the Internet Engineering Task Force (IETF). This group has developed a number of draft standards for representation of privacy policy data and protocols for management of location privacy.

## 3 Secure tracking using Galileo

There are a number of requirements for security and privacy in GNSS tracking applications. The following subsections discuss these requirements and possible implementations in terms of satellite navigation system security, tracking device security, communications security to the telematic server, and privacy.

### 3.1 Signal authentication

Signal authentication of satellite navigation systems is required in order to ensure that the source of the satellite signaling is not from a simulator, but is genuine. There are a number of existing and proposed signal authentication methods (Hein and al 2002), (Scott 2003) which are summarized below:

- *Signal Authentication through Authentication Navigation Messages (ANM):* The ANMs would include a digital signature authenticating the other navigation messages that contain data including ephemeris and almanac data. Using the digital signature, the certified receiver is able to authenticate the source of messages and verify their integrity. These authentication messages are created on the ground and transmitted to the satellites for broadcast. This method has a security limitation, in that the messages can be acquired by a certified receiver and modulated over a simulated signal in order to spoof the Galileo signal. This would require functionality that is not commonly found in commercial signal simulators, and would require the operation to be performed within a very small time window. Documents from the Galileo design consolidation indicates that the Galileo

[1] Refer to http://ecotroph.net/geopriv

Open Service may support this type of signal authentication (Galilei 2003).

- *Signal Authentication through Spread Spectrum Security Codes (SSSC) (Scott 2003):* SSSCs are synchronous cipher streams seeded by an unsent digital signature from an Authentication Navigation Message, interleaved with normal spreading sequences. The receiver stores A/D samples and once the digital signature is received, it is able to generate the security spreading code reference signal and correlate it with the stored samples. If the SSSC is detected at the correct power level, the signal is authenticated. This technique has the innovative advantage that permits authentication in a signal open to the public without the difficulties of key distribution; however it has the limitation that the spoofing detection is proportional to the antenna gain and that the authentication verification is not immediate. A more secure type of authentication based on SSSCs is also proposed by (Scott 2003), utilizing a Civil Antispoof Security Module (CASM) with a preloaded Red Key and the authentication navigation message for seeding of the cipher stream generator. This type of signal authentication does not have the drawbacks of the public SSSC version.
- *Signal Authentication through Spreading Code Encryption (SCE):* Spreading code encryption is one of the oldest signal authentication techniques, currently used by the GPS P(Y) code, an exclusively military service, and is projected to provide authentication of the Galileo CS and PRS signals. As the spreading code is secret, without knowledge of the spreading code, signal access is denied. For this reason, the spoofer cannot simulate the signal, and hence authentication of the signal is achieved when the user possesses the correct spreading code. In GPS' P(Y) code, the P code is publicly known, and the secret spreading code is obtained using P code with a Red Key, or a Black Key and the Selective Availability Anti-spoofing Module (SAASM) (Callaghan and Fruehauf 2003). The Black Key is the Red Key encrypted with the public key of a given SAASM. , allowing the Red Key to be decrypted inside the tamper-resistant SAASM which contains its private key. The Black Keying infrastructure allows for electronic key distribution and does not compromise the classified Red Key.

Civil signal authentication is a challenge for next generation satellite systems. As detailed above, there are a range of different strength security solutions and proposals. The suitability of a particular signal authentication mechanism is dependant on the cost to defeat the mechanism; balanced against the possible gain should the mechanism be successfully defeated.

The Galileo signals and corresponding authentication schemes to date have not been decided. Based on generally available information, it is evident that Galileo will provide a number of different services, the following of which are projected to provide signal authentication: (Hein and al 2002)

- *Open Service (OS):* Based on available literature (Galilei 2003), encryption may be provided to the open service on the E5b-I data channel. This service will provide authentication through Authentication Navigation Messages (ANM);
- *Safety of Life Service (SOL):* This service will provide satellite and signal integrity messages and Authentication Navigation Messages (ANM);
- *Commercial Service (CS):* This service will provide access restriction and authentication through spreading code and data encryption (SCE); and
- *Public Regulated Service (PRS):* This service will provide access restriction and authentication through spreading code and data encryption (SCE).

Of particular interest to consumer applications such as insurance tracking and toll collection is the signal authentication provided on the Open Service. Fig. 1 illustrates a candidate navigation message authentication scheme as detailed in the Galilei Project Galileo Design Consolidation (Galilei 2003).

The authenticated navigation messages would be created by the Ground Control Centre and up-linked to the satellites. In theory a public key certificate certified by the Galileo certification authority would be included in the navigation messages, and could be verified by the Galileo certification authority certificate stored on a certified receiver. Once the public key is verified, the receiver would be able to verify the signature included in the navigation messages, and hence authenticate the source of the navigation messages, and implicitly the integrity of the messages.

For applications with greater security requirements, the CS and PRS signals will provide signal authentication through encrypted ranging codes. While there is no literature on the key distribution schemes, it can be assumed that that the implementation would be similar to the declassified Black Key distribution framework used

with the P(Y) code of GPS. The key distribution and key storage problem in this scenario are similar to the Selective Availability Anti Spoofing Module (SAASM) (Callaghan and Fruehauf 2003), used in military applications.

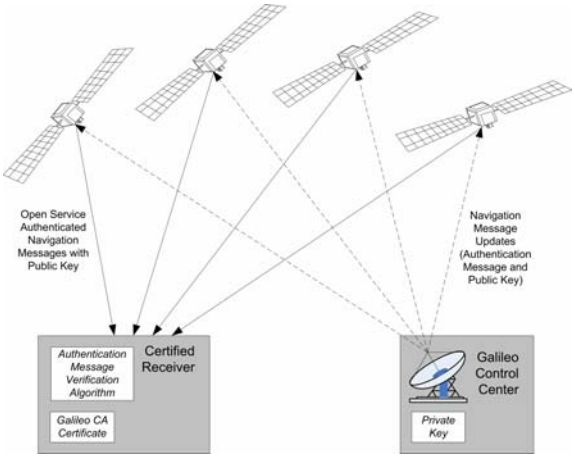


Fig. 1 Navigation authentication message

### 3.2 Receiver security for tracking applications

We have previously proposed the design for a trusted civil receiver in (Pozzobon et al. 2004). In this architecture a tamper resistant receiver uses public key cryptography to assure the chain of trust to the application, and provide authentication and cryptographic integrity of the data to the application. The tamper resistant receiver acquires and authenticates the signal, calculates the location and creates data authentication messages containing a digital signature of the location data, signal state and tamper-resistance state using the receiver private key. The data is sent to a telematic server via a wireless communications service such as GPRS.

The data is send using an extension to the National Marine Electronic Association (NMEA) protocol 0183 for GPS data navigation we have proposed (Pozzobon et al. 2004), which provides authenticated position, time and velocity information as well as signal state and tamper-resistance state of the receiver.

As integrity verification is a computation embedded in the device, the computation must be trusted. The device must implement all the necessary integrity verification algorithms and transmit to the telematic server any information regarding status, availability, integrity of the signal, and the results from the verification operations. Technology such as the Trusted Computing Platform (TCP)[2] can be used to build trusted systems, that is, systems where the application running can be trusted, with the assurance that it has not been compromised, or modified by an attacker.

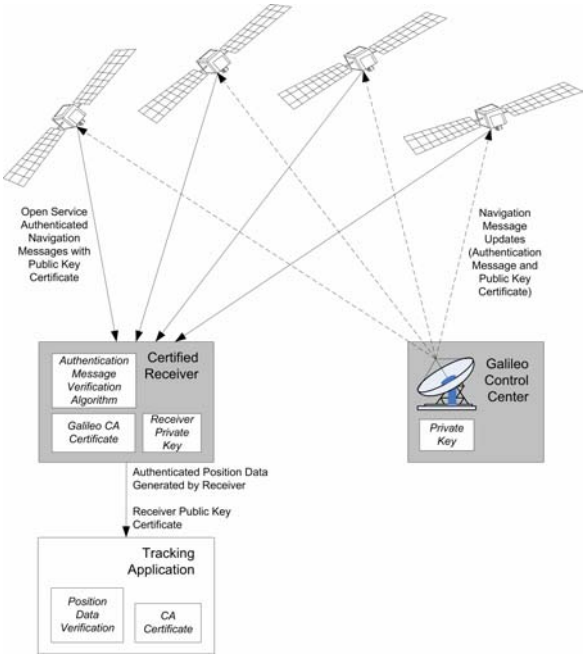


Fig. 2 Tracking with a certified receiver

The concept behind this technology is to build a computer with trusted building blocks (TBB). In TBB, the core root of trust for measurement (CRTM) is the Basic Input/Output system (BIOS) of the computer. The CRTM uses the trusted platform module (TPM) for cryptography operations (storage of keys, encryption) in order to trust the system boot[3] and verify the integrity of the subsequently executed applications. The whole "chain of trust" is based on public key infrastructure (PKI), RSA and 3DES algorithms.

### 3.3 Location privacy

As detailed in Section 2.3, there are a set of emerging standards for location privacy developed by the Geopriv working group of the IETF. A high level diagram of the interactions between architecture components in using Geopriv protocols for management of privacy between a GNSS tracking device and telematic server is illustrated in Fig. 3. The components of the architecture include:

- *GNSS tracking device:* The proposed tamper resistant GNSS device;
- *The Telematic Server:* The server that manages location and communications;

[2] Refer to https://www.trustedcomputinggroup.org/

[3] The procedure that starts all the necessary process of an operating system

- *Rule Holder:* The entity that provides the rules associated with a particular target for the distribution of location information; and
- *Rule Maker:* The authority that creates rules governing access to location information for a target.

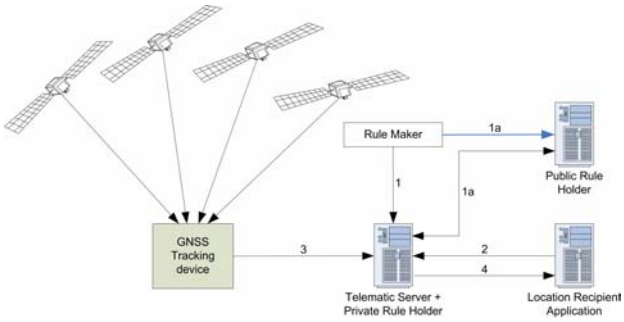


Fig. 3 Location privacy using Geopriv protocols

Fig. 3 additionally illustrated the process of privacy rule upload on the telematic server and how privacy is protected in the location acquisition process. This process, which complies with the RFC3693 requirements, consists of the following steps:

- *Rule Transfer:* The Rule Maker sends a Rule to the Telematic Server containing the privacy information;
- *(1a) Signed Rule:* the Rule Maker may write a Rule and place it in a Public Rule Holder as an alternative. The Telematic Server can access the Public Rule Holder to read the signed Rules;
- *Location Information Request:* The Location Recipient Application requests location information to the Telematic Server.
- *Locate:* The Telematic Server is either continuously receiving the location data from the GNSS tracking device or can request updates on the location. The communication is encrypted; and
- *Filtered Location Information:* The Telematic Server sends the location information to the Location Recipient Application. The information may be filtered in order to comply with the privacy policy and rules defined by the rule maker.

## 4 Secure tracking using current and emerging technology

The following subsections detail current and emerging technologies that have been developed or are currently under development.

### 4.1 Current tracking devices developed by Qascom

A number of tracking solutions have been developed using commercially available hardware such as the Siemens TC454 GSM module and SiRF5 GPS Receiver. Fig. 4 illustrates the components in the Qascom tracking blackbox. The location information is processed by a Java applet loaded into the flash memory of the TC45 GSM module. The java applet is responsible for processing GPS location, velocity and time data. The information is then processed according to the requirements of the application, such as insurance.

The applet signs the resulting information destined for the telematic server by invoking a sign function using the SIM Toolkit interface[6] of the SIM card. This functionality requires a SIM card with support for public key operations accessible through the SIM toolkit interface. The signature of the data provides cryptographic integrity protection of the data as well as authenticating the source of the data. The resulting information and signature are sent to the telematic server using one of two supported communication modes: SMS (Short Messaging Service) messaging or GPRS (General Packet Radio Service).

To ensure the privacy of the data communicated to the telematic server, appropriate security must be used. Where SMS is chosen as the mode of communication, no session cryptography is used. This is for three reasons:

- SMS is a point-to-point delivery service where the end point is another device on the GSM network. It is assumed that a destination on the GSM network cannot easily be spoofed. The tracking device can be authenticated using the source MSISDN (Mobile Station International ISDN Number);
- GSM provides data encipherment using the A5 algorithm from the mobile station to the base stations. The core network is assumed to be protected from intruders. Flaws in the encryption and key establishment protocols of GSM are overcome by the use of new protocols in 3G deployments; and
- A significant number of messages would be required for authentication and establishment of keys, resulting in a communications protocol that is too costly.

In this mode, the telematic server must have a mobile station present on the GSM network.

[4] Refer to http://www.siemens-mobile.com
[5] Refer to http://www.sirf.com/
[6] SIM Application Toolkit (SAT) is defined in GSM 11.14 standard for 2G networks, and 3GPP 31.111 for 3G networks.

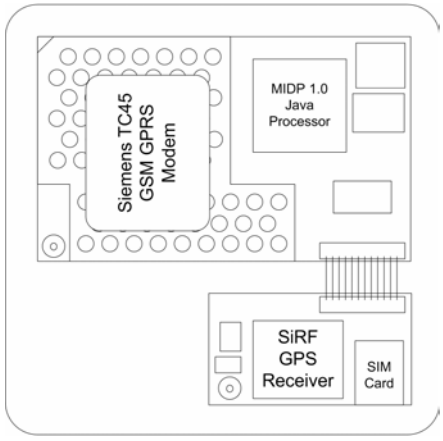


Fig. 4 Qascom GPS/GSM tracking box

Where GPRS is chosen as the mode of communications, the processed data and signature must pass through the GPRS Gateway (GGSN) and over the Internet to the telematic server as illustrated in Fig. 5. For this reason, the tracking device must be able to authenticate the destination telematic server, and establish session keys with this entity in order to transfer the processed data. This process is facilitated through a small implementation of SSL (Secure Sockets Layer) in the Java applet.

This implementation of SSL uses the SIM card to verify the public key certificate of the telematic server and perform public key operations for the exchange of keys. Computation of the pre-master-secret is performed in the Java applet, using the real-time clock in the GSM module for generation of random numbers. The pre-master-secret generated by the applet is then encrypted in the SIM card using the telematic server's public key. The master secret is generated from the pre-master secret as specified in (Dierks and Allen 1999). The master-secret is the key used for encrypting the session between the device and the telematic server. The processed data and signature can then be transmitted over the established security context. This mode of communications is significantly more secure than the SMS mode.

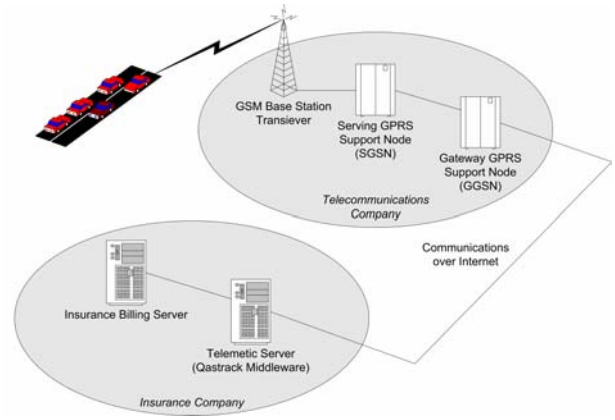


Fig. 5 GNSS tracking using GPRS

While the current solution provides protection from malicious attacks on the communications between the tracking device and the telematic server, the solution does not prevent an attacker from loading malicious firmware (Java applet) onto the tracking device. As the device has no mechanism to authenticate the firmware, the malicious software could generate data that minimizes the amount payable to an insurance company, for example. The software would still be able to use the cryptographic functionality of the SIM card, such that the telematic server would be unaware of such malicious activity.

In addition, the current GPS implementation provides no signal authentication or protection from spoofing. Thus, it is possible to attach a GPS signal simulator to the antenna and spoof the location.

### 4.2 Next generation devices being developed by Qascom

We are currently involved in development of a next generation tracking device that will fulfill the security requirements of applications such as insurance tracking. The proposed tracking device will contain a trusted GNSS receiver, which will be developed by a consortium of research institutions and companies including Qascom in Europe. The trusted GNSS receiver is described by Pozzobon, Wullems and Kubik in (Pozzobon et al. 2004). The proposed tracking device will contain a general purpose processor with tamper-resistant key storage and a cryptographic coprocessor (trusted platform module). In addition to supporting secure communications over GPRS, the tracking device will also provide the facility for authentication of firmware as well as support for trusted GNSS positioning. Fig. 6 illustrates the secure tracking box.

The verification of the data provided by the trusted GNSS receiver is performed by the authenticated software. This verification initially involves verification of the public key of the trusted GNSS receiver, before being able to verify the digital signatures contained within the authentication data.

This software not only verifies the GNSS position, time and velocity data, it additionally processes the data as required by the application. The resulting data to be sent to a telematic server contains the processed GNSS data, signal state and device compliance reports obtained from the trusted GNSS receiver, the public key certificate of the tracking device, and a digital signature of this data. The digital signature is calculated by the cryptographic co-processor using the private key stored in the tamper-resistant, secure key storage. The telematic server first must verify the public key certificate of the tracking device, after which it is able to verify the data received.

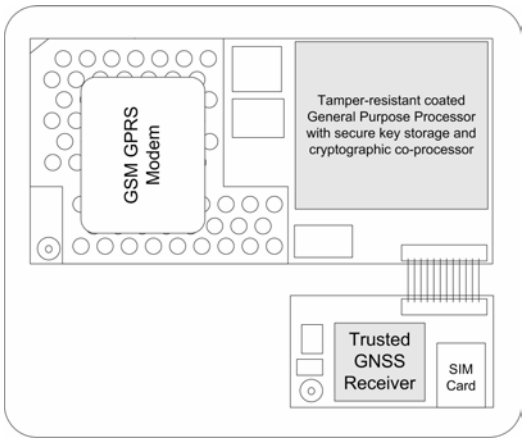


Fig. 6 Qascom secure tracking box

## 5 Conclusions

This paper has described a secure framework for tracking applications that use the Galileo Authentication Services. Requirements for secure tracking in both consumer and critical applications were introduced, detailing how the new signal characteristics of Galileo can be used to enhance the security of tracking applications. Requirements in terms of authenticated signaling, device security and location privacy were introduced. This paper concluded with a discussion of both existing and future tracking device developments and detailed the strategies used to mitigate the security issues in the presence of the Galileo security differentiators.

## References

Callaghan, S., and Fruehauf, H. (2003). ***SAASM and Direct P(Y) Signal Acquisition***, The Journal of Defense Software Engineering, 16(6), 12-16.

Dierks, T., and Allen, C. (1999). ***The TLS Protocol Version 1.0,*** Network Working Group, Internet Engineering Task Force, Request for Comments 2246.

Galilei. (2003). ***The Galilei Project: GALILEO Design Consolidation,*** European Commission.

Gibbons, G. (2004). ***HazMat Keeps on Truckin',*** *GPSWorld* (October), 6.

Hein, G. W. et al. (2002). ***Status of Galileo Frequency and Signal Design.*** Brussels.

Pozzobon, O., Wullems, C., and Kubik, K. ***Requirements for Enhancing Trust, Security and Integrity of GNSS Location Services,*** Institute of Navigation (ION ), 60th annual meeting, Dayton, OH, USA.

Scott, L. ***Anti-Spoofing & Authenticated Signal Architectures for Civil Navigation Systems,*** *ION GPS, GNSS 2003*, Portland, OR.

Spreitzer, M., and Theimer, M. ***Providing Location Information in a Ubiquitous Computing Environment.*** *Fourteenth ACM Symposium on Operating System Principles*, 270–283.

Volpe, J. A. (2001). ***Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System.***