Privacy Protected Localization and Authentication of Georeferenced Measurements using Galileo PRS

Alexander Rügamer, Manuel Stahl, Ivana Lukčin, Günter Rohmer
Fraunhofer IIS
Nuremberg, Germany

***Abstract*—This paper describes two methods how ordinary users can profit from privacy protected localization and georeferenced measurements authentication using the Galileo public regulated service (PRS). The user does not need to care about any security related PRS-receiver issue and his localization privacy is inherently protected. A raw data snapshot, containing only Galileo PRS data, is combined with an artifact to be authenticated and forwarded to a PRS enabled agency server. All PRS and security related functions are implemented on this server located in a secured place. The server uses cross-correlation and snapshot positioning methods to authenticate or obtain a position information out of the raw data. The described methods will not provide any direct PRS information, like PRS position or time, to the ordinary user. Only the specific user request is responded. Having outlined the architecture of possible implementations, limits and applications of the idea are discussed. Possible attacks on the methods are described with mitigation measures. The paper concludes with a comparison to the state of the art and other publications and projects in this field of GNSS authentication.**

***Index Terms*—Satellite navigation systems, Global Positioning System, Authentication, PRS, Snapshot positioning**

I. Introduction

Position, velocity, and time (PVT) information, anywhere and anytime, thanks to the freely available global navigation satellite systems (GNSS), was a key opener for many applications, companies, and services. It is taken for granted that positioning and time information is available. Sometimes there are problems with accuracies or availability due to e.g. multipath or urban canyons but for most applications the standard GNSS PVT is still good enough.

Geolocation data can disclose significant information about someone's activities, but for many applications it is mandatory. An example of a positioning application entering everyone's life is the European eCall system. In case of an accident, the location of the incident is automatically forwarded to the emergency operators. Just recently, the European Parliament resolved upon a European Commission proposal that this automated emergency call system for road accidents shall be mandatory in every new car sold in Europe from beginning of October 2015 [1]. Of course, having a PVT device with communication interface in every car is also interesting for e.g. insurance or marketing companies. This is regarded as critical from a data protection point of view: with the help of the PVT data, accurate information about the user can be derived — with or without his knowledge and/or permission [2], [3].

The next generation of applications utilizes PVT for authentication purposes. Many location based services (LBS) rely on a trustworthy positioning and time information from GNSS. There are already some very big systems installed, e.g. toll collect systems in Europe, where the road fees are derived from the position of the vehicle. In these systems, it is crucial that the positioning solution can be trusted. If spoofed, the business model of the application is at stake.

Since more and more security related PVT applications are deployed, one also has to think about security issues. The timing information of the unprotected GPS C/A is currently used to synchronize critical infrastructure like telecommunication and energy networks [4]. There is a gradual change of mind ongoing, thanks to activities that generated a lot of media attention like the demonstration of drone and yacht capturing with a self-made spoofer [5], [6].

Consequently, a lot of research is done for spoofing detection and mitigation, but these methods alone are not enough for a reliable authentication solution. The security has to be embedded inside the GNSS signal. Different proposals for this have been made e.g. [3] but currently the only system already supporting such a secure, unspoofable, and non-military signal is Galileo with its public regulated service (PRS).

In this paper, we presented a method with possible applications for a secure tracking device, which protects the users' privacy with the help of Galileo PRS. This approach is then extended to be able to authenticate georeferenced measurements in general with their position and time information in a trustworthy way. Both methods do not disclose any direct Galileo PRS security, service, or positioning/timing information to the user. The user gets just a response to his request. The trustworthy answer to this request is ensured with the help of the Galileo PRS signal processed in a secure government controlled environment.

The paper is organized as follows: Section II briefly summarizes the Galileo public regulated service (PRS). In Section III the first method for using Galileo PRS for privacy protected localization is described with technical realization and application examples. Section IV extends this method with technical realization and applications for the authentication of georeferenced measurements using Galileo PRS. Possible attacks on the methods are described with feasible mitigation strategies. Finally, in Section V, the presented approaches are compared to the state of the art and conclusions are drawn.

978-1-4799-3320-4/14/$31.00 © 2014 IEEE

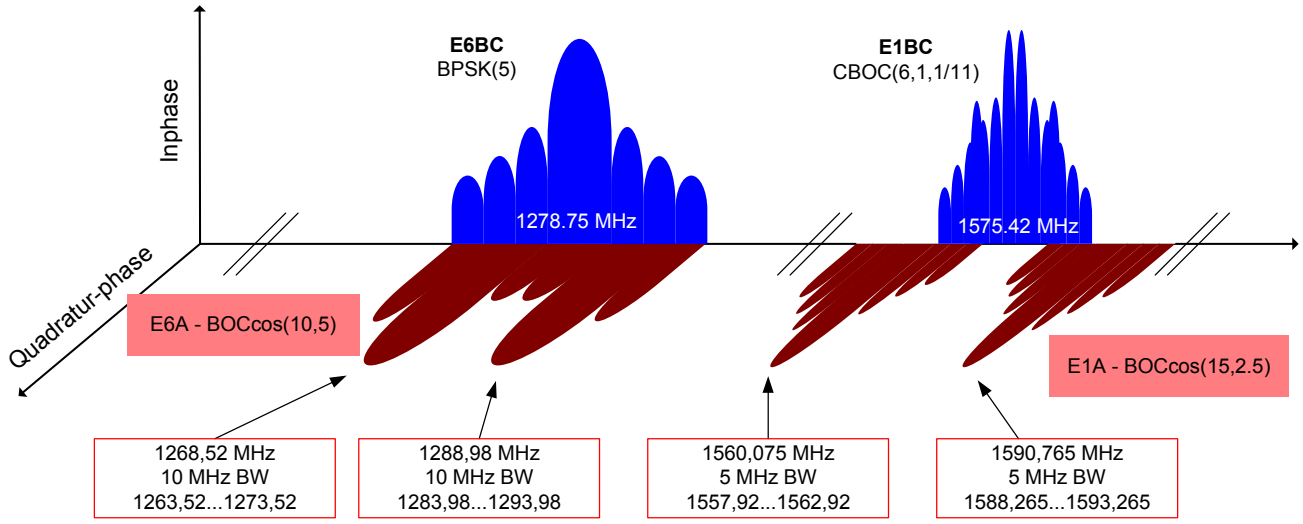

Fig. 1. Galileo PRS signals

II. Galileo PRS

The European GNSS Galileo will provide three different navigation services: Open Service (OS), Commercial Service (CS), and the Public Regulated Service (PRS). Galileo OS is similar to the free services of GPS and GLONASS. The Galileo CS is not yet defined. Ideas about providing additional correction data over an encrypted message for which the user has to pay for are currently discussed. Galileo PRS features two encrypted signals on two frequency bands and targets both governmental and authorized users, e.g. police, border control, emergency, armed forces, Search and Rescue, and also operators of critical infrastructures like telecommunication- and energy-networks as well as critical transports. It is important to highlight that in contrast to GPS and GLONASS, Galileo is a civil GNSS under civilian control. Consequently, PRS is not a military service, even though it is comparable to the military signals like the GPS PPS P(Y) in terms of access control and the strong encryption used.

As shown in Figure 1, the Galileo PRS signals are transmitted in a coherent way together with the OS and CS signals over the E1A and E6A frequency bands, using a binary offset carrier modulation denoted as BOCc(15,2.5) and BOCc(10,5), respectively. BOCc uses a cosine phased subcarrier resulting in higher frequency components than a sine phased subcarrier used in BOCs modulations of e.g. Galileo E1BC OS. As a result, more energy is shifted to the edges of the band. This improves the spectral separation with the coexisting OS and CS signals and the theoretical tracking performance [7].

Thanks to the strong encryption used, Galileo PRS can add a legal value on its PRS PVT solution since anti-spoofing is guaranteed. This property is a key opener to a lot of critical and demanding applications mostly in the security related areas. The disadvantage of the standard PRS service is that only certain user groups can profit from PRS and that handling of the security related PRS receiver is very demanding and cumbersome. The access to the PRS is controlled by the Galileo Member States through an encryption key system. The standard user will not be able to access any information of Galileo PRS. Although everyone can receive the PRS raw data, only someone having the decryption key is capable of generating the PRS pseudo-random-noise (PRN) sequences to despread the PRS signals and to process their messages. Without knowledge of the keys, the unknown PRN sequences used are like a one-time-pad, a type of encryption, which has been proven to be impossible to crack if used correctly.

The methods described in this paper show possibilities how also ordinary users can profit from Galileo PRS without having to take care about the strong security requirements of PRS or even jeopardizing the PRS security ring of trust. No PRS security related functions are needed on the user side. Not even the information directly obtained out of the PRS will be forwarded to the user. The methods require only from the server side — being a government authorized user — to deal with the real PRS signal structure and its security requirements. The additional use of PRS in the mass market leads to a wider acceptance of Galileo and its added value compared to GPS, since the PRS is a service that GPS cannot provide.

III. Privacy Protected Localization

This section describes how a privacy protected localization can be realized with the help of Galileo PRS. The block diagram for this method is depicted in Figure 2. The technical realization consists of a PRS snapshot recorder, which can e.g. be an external bluetooth device, connected to a conventional smartphone or any other end user's device. This device has access e.g. via mobile internet to a server for file uploading. A government authorized agency in charge of localizing the user in an emergency situation has also access to these files.

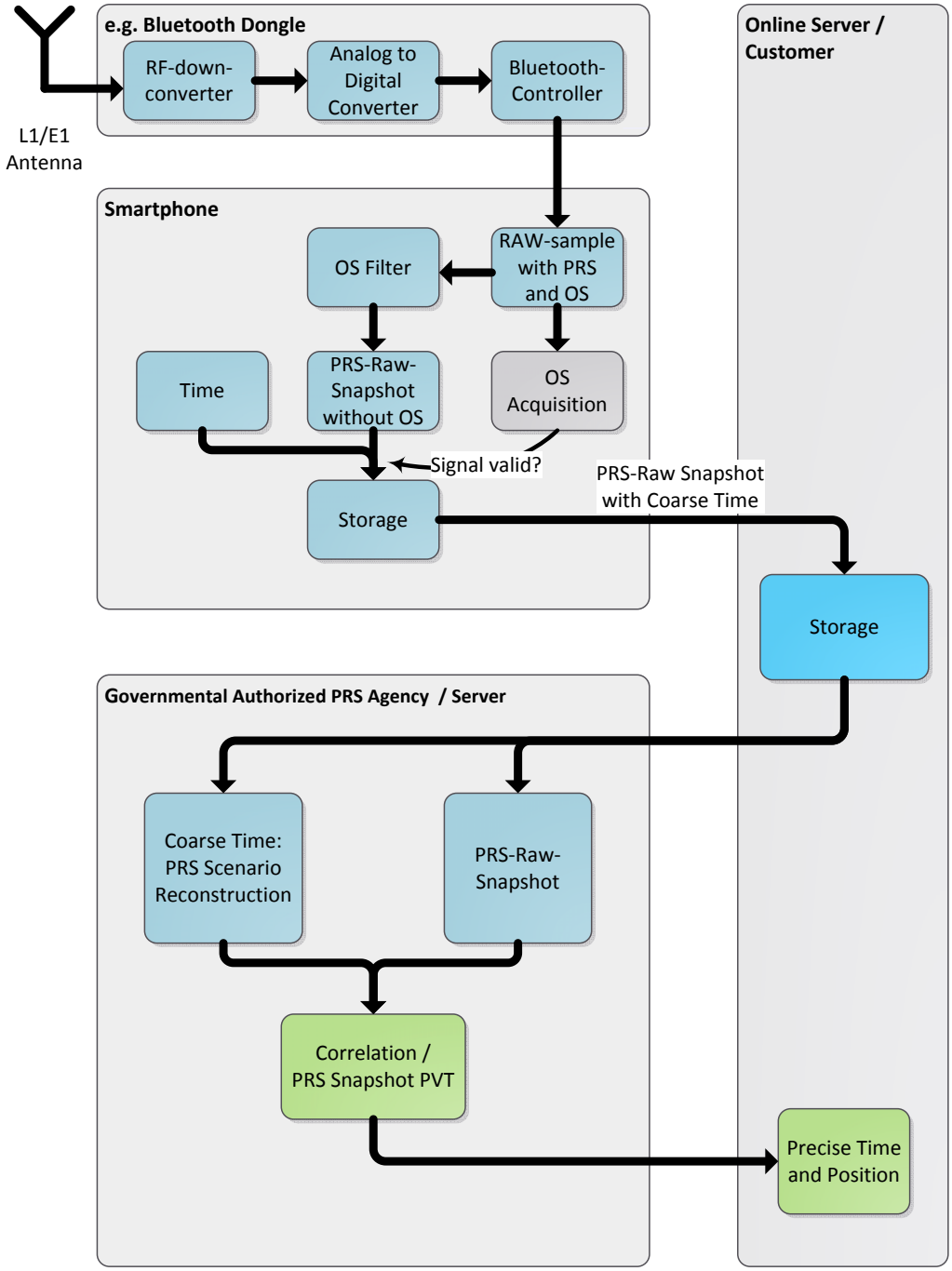

Fig. 2. Block diagram of a privacy protected localization

A. Method

The PRS snapshot recorder hardware comprises an integrated or external antenna, a radio frequency (RF) down converter chip, an analog to digital converter, and a data transmission controller (e.g. USB, Bluetooth or WiFi). The snapshot receiver records a few tens of milliseconds of raw-data on hard disk, wideband enough to include not only the Galileo OS but also the Galileo PRS. A software running on the client's computer or smartphone first acquires the Galileo E1 OS signals to check if the snapshot of raw data was successful. A successful OS acquisition guarantees that also PRS signals are present, since OS and PRS signals are transmitted together in a coherent way. Now, the Galileo OS components (including also the other open service signals like the GPS L1 C/A) are removed with a high-pass filter, leaving just the raw PRS-noise. The reason for the filtering is twofold. Firstly, the users' privacy is protected by removing the OS components since only institutions authorized to use Galileo PRS and having valid PRS keys are capable to obtain the actual position and (or) time of the taken snapshot. Secondly, having removed the OS components the file size of the snapshot can be significantly reduced.

This raw PRS snapshot can be uploaded to a server and processed by a government authorized PRS agency on specific request. Two methods are foreseen to obtain the actual position or time of the raw PRS snapshot. The first method uses a coarse time and location information transmitted together with the raw PRS snapshot. Using this additional information, the actual signal environment can be rebuilt with a special PRS simulator, using the actual ephemeris information and rebuilding the PRS signals with the valid key for the specified timeframe. Thus, the positioning and time information of the raw PRS snapshot is determined by a cross-correlation. The second method to get the positioning information out of the raw PRS snapshot is to use a snapshot positioning as has been already demonstrated for GPS L1 C/A [8]. For the raw PRS snapshot positioning again a PRS capable simulator / receiver is mandatory to generate the right PRS PRNs to be used for the pseudorange determination step. In contrast to GNSS snapshot positioning with GPS L1 C/A signals, the "PRS one-time-pad"-like sequences with quasi infinite length have no ambiguities. This facilitates the position determination and can lead to a higher accuracy.

B. Applications

One practical application for the privacy protected localization is the localization or tracking of elderly people e.g. suffering from dementia. The balance between the patient's privacy and the level of protection is floating. The described method of privacy protected localization helps these persons to age with dignity and respect even though their position is constantly made available with raw PRS snapshots uploaded to a server. Since only authorized personal can compute their position information in an emergency situation, the privacy is very well protected in contrast to the simple GPS trackers already available on the market that expose the position to everyone, leading to the abuse of patient's rights.

The same method can also be applied for prisoners' electronic tags used in minimal security or open prisons. The prisoner profits from the better protection of his privacy and is guarded with anti-spoofing and anti-jamming capabilities of Galileo PRS.

Another practical application, where privacy protected localization could be used, is the emergency call (eCall) system installed in more and more cars, as already mentioned in the introduction. To protect the position information of the driver, e.g. from abuse by insurance or marketing companies, raw PRS snapshots as described above will preserve the users' privacy without risking the lifesaving localization information in emergency situations. Another problem faced by the conventional eCall GPS localization systems is that the time to first fix of current GPS receivers is often too slow to provide an instant position, especially in obstructed areas. The eCall could be canceled before a position was transmitted. With transmitting only a snapshot of the received data, the emergency agency can use high processing power and invest more time to gain a position from this raw data snapshot. Moreover, the robust signal design of Galileo PRS enhances the position accuracy and reconstruction robustness.

IV. Authentication of Georeferenced Measurements with Galileo PRS

The raw PRS snapshot can be further used as a digital fingerprint on a measurement, file, or document to be authenticated with a georeference. The architecture for this application is depicted in Figure 3.

Depending on the intended application and the required security level, the raw signal snapshot device should be encapsulated together with the actual measurement device in a tamper proof housing. Such protected units are already standard for many devices like on-board units, electricity smart meters, etc.

A. Method

The first steps of this method are the same as explained in Section III to obtain a valid raw PRS snapshot. If the privacy of the data is of no concern, the OS components can also be included. The goal of this method is to cryptographically combine the raw PRS snapshot with the measurement to be signed and the positioning and time information of this measurement to be authenticated later on. One way of doing this combination is depicted in Figure 4 using a public/private key infrastructure. It is assumed that the user device incorporates a private key and has shared its public key with the customer. The private key is used to sign a hash value of both the raw PRS snapshot and the measurement. The public key, hash values, and the actual measurement with raw PRS snapshot are forwarded and stored on a server. The uniqueness of the hash functions signed with the user's device private key ensures that the raw PRS snapshot is cryptographically combined with the measurement.

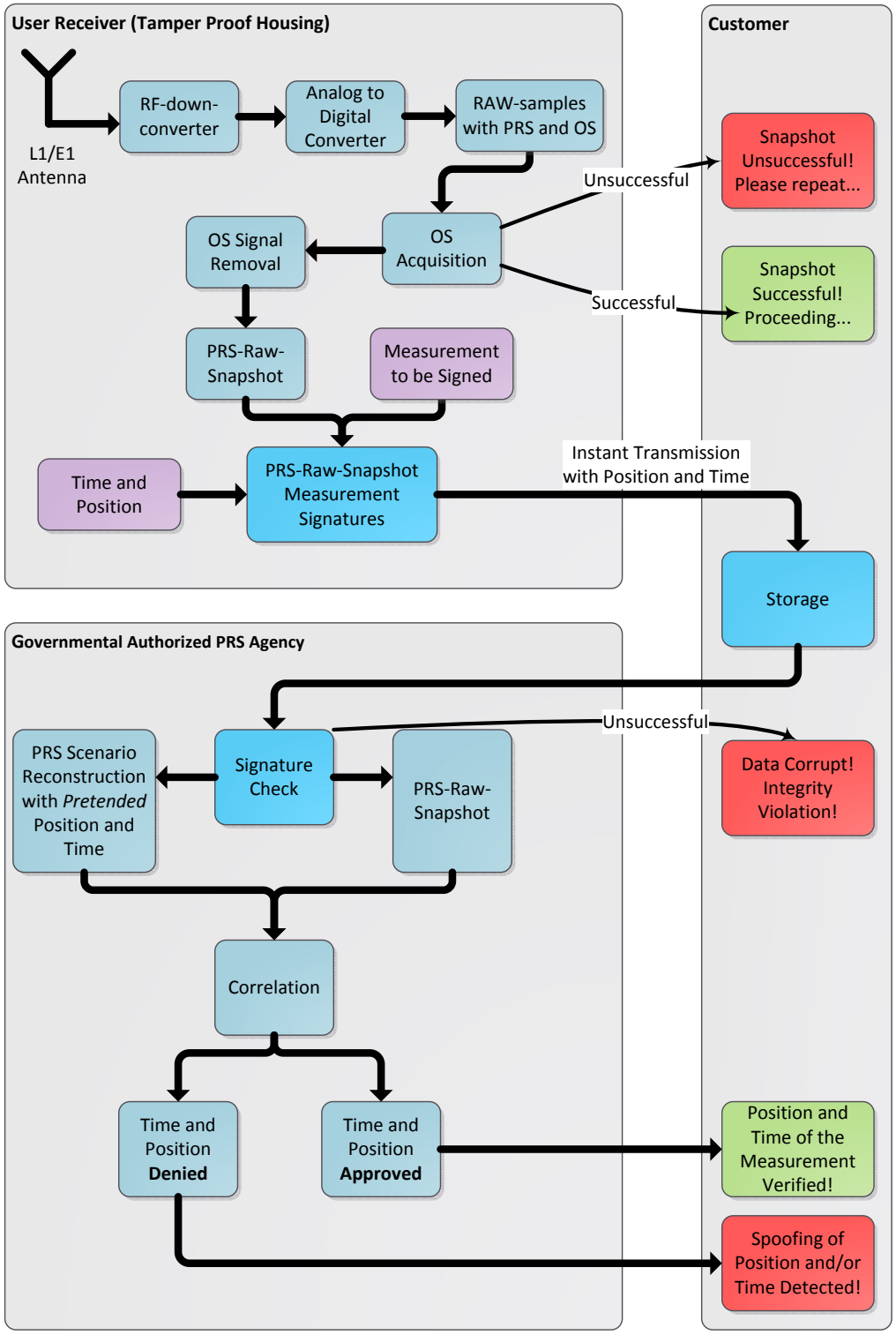

Fig. 3. Block diagram of authentication and combination of georeferenced measurements

To verify the measurement with its raw PRS snapshot a 3rd party can generate the same hashes out of the provided data and compare them to the transmitted hash sums. This is depicted in block diagram of Figure 5. The integrity of the hash sums provided can be verified using the user's device published public key.

When the customer or 3rd party is convinced that the measurement and the raw PRS snapshot are belonging to each other, the actual authentication process begins. Using the reported position and time, the government authorized PRS agency can recreate the given PRS scenario and do a cross-correlation to check if the pretended time and position match. Since a valid PRS key is necessary to do this check, only government authorized PRS agencies are capable of doing it. Then, the integrity of the file signed with the raw PRS snapshot can be decided. If a false position and/or time were provided, the correlation with the recreated scenario will not be successful. By extending the search space and with some more computational effort, it should even be possible for the authorized PRS agency to find out the actual position and time of the snapshot.

B. Applications

The "measurement" to be authenticated can be every digital artifact: a position, a digital file, a photo or video recording, documents, and so forth. Consequently, the applications for authentication of georeferenced measurements with Galileo PRS are very wide. A few practical examples are outlined in the following.

In Germany, larger cities have to do regular monitoring of environmental parameters like particulate matter, carbon dioxide emissions, and so forth. Therefore, some stationary equipment has been installed. Due to the high cost of this equipment and its maintenance, only a few sites per city are monitored. Until now, no mobile equipment is used, since the position and time of the measurement would have to be securely verified. With the concept of the authentication applications described in this section and the architecture depicted in Figure 3, it is possible to do this verification, even when the measurement equipment has no standalone PRS receiver. By uploading the recorded environmental data cryptographically combined together with a raw PRS snapshot on a server, the customer is able to verify the position and time of the measurements afterwards with the help of a government authorized PRS agency.

Furthermore, the presented method could also be used for a disposal of waste monitoring. When the waste is disposed, a system connected to the tailboard of the disposal truck could automatically initiate the collection of a raw PRS snapshot and transmit this to the responsible agency. Now this agency can check that a container of waste was disposed at a predefined location according to the rules.

Measurements like photos, audio files, videos, and also documents often have to be verified and/or authenticated where and when they were made. Typical examples are evidences used in a trial, e.g. photos of a crime scene taken by the police. This verification process can be realized with the presented idea using the raw PRS snapshot to sign such a measurement for adding certain legal information to the object. Afterwards, a government authorized PRS agency can be instructed to verify the location and time of the measurement. The procedure is basically the same as for the authentication applications depicted in Figure 3.

Already in 1996 an approach for an "authenticated camera" was presented using a certain interaction between the camera and its base station before and after its usage [9]. The biggest gap identified in their proposed architecture is the strong need for authenticated location data, which was not provided or even foreseen by any GNSS back then in 1996. The authentication of measurement method presented in this paper can provide exactly this required authenticated location data and time, thanks to the Galileo PRS service used in the proposed raw PRS snapshot way.

Another very interesting field of application for the verification of location and time of a measurement use case could be the adoption of the described technique for a toll collect system. A tamper proof on-board unit containing the user receiver is recommended for this. Also a combination of the PRS-raw samples with the OS samples could be useful in this case.

Finally, the verification of location and time of a measurement could be used as a skimming prevention system for bank transfers and credit card payments. The generation of the Transaction Authentication Number (TAN) or the usage of a credit card payment over the internet can be coupled to the location information provided by a transmitted and afterwards verified raw PRS snapshot.

C. Possible attacks on the system

Since such a PRS authentication process is mainly used to prevent fraud, attacks on the system are likely and have to be taken into account in the individual system application architecture and design phase.

Often a tamper proof housing is unavoidable to prevent that someone inserts e.g. digital raw PRS samples from another position and time into the system or inserts a fake measurement. Such attacks are similar applicable on other systems and can be successfully mitigated using the right technology for the tamper proof housing.

When the housing is shielded and the cryptographic combination holds, the only attack possible is via the RF signal entering the antenna. Galileo PRS signals are regarded as spoofing free due to the strong encryption used. This is the backbone of the methods described here and should be considered as inherently secure. Although spoofing is not feasible it is still possible to either replay a recorded RF signal or to reroute signals from another position and time to the RF input. One hardening strategy is to use a precise clock with a very high long term stability inside the tamper proof housing to have a reliable timing source. This independent time information can be used to detect replayed or rerouted

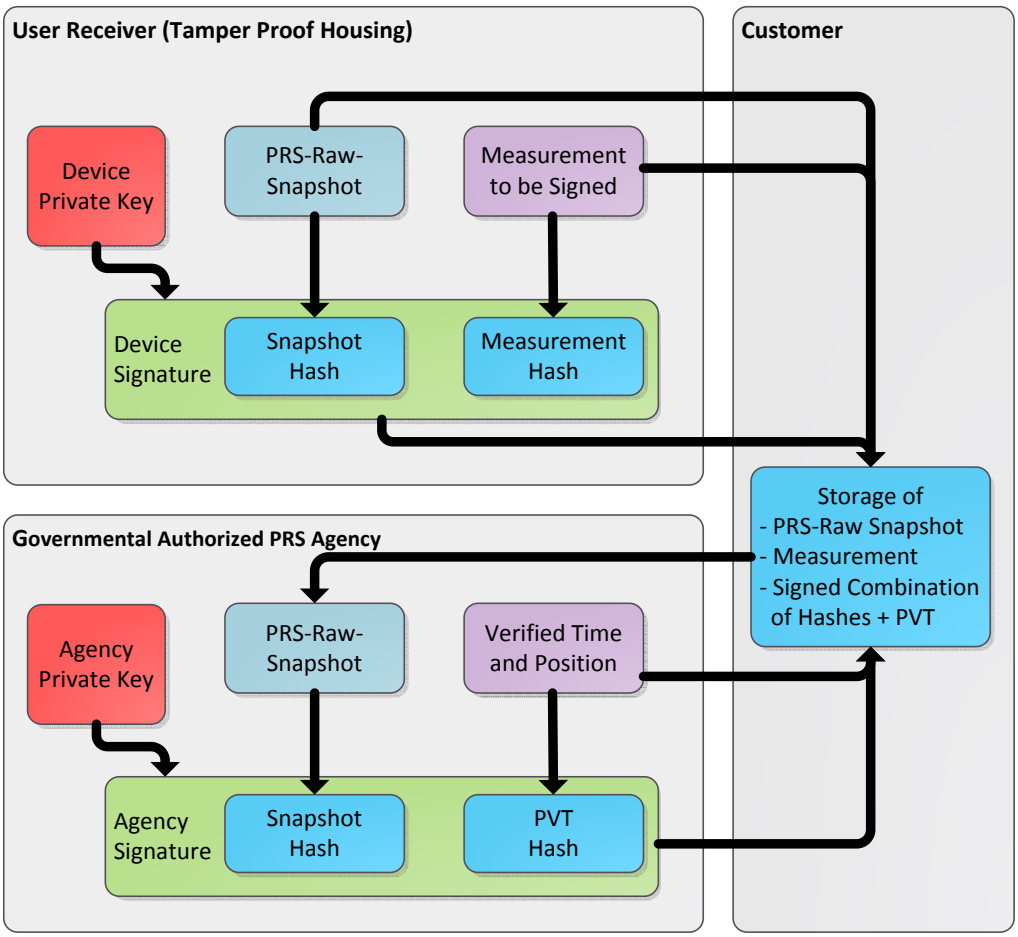

Fig. 4. Example of how to cryptographically combine a measurement to be authenticated with the raw PRS snapshot

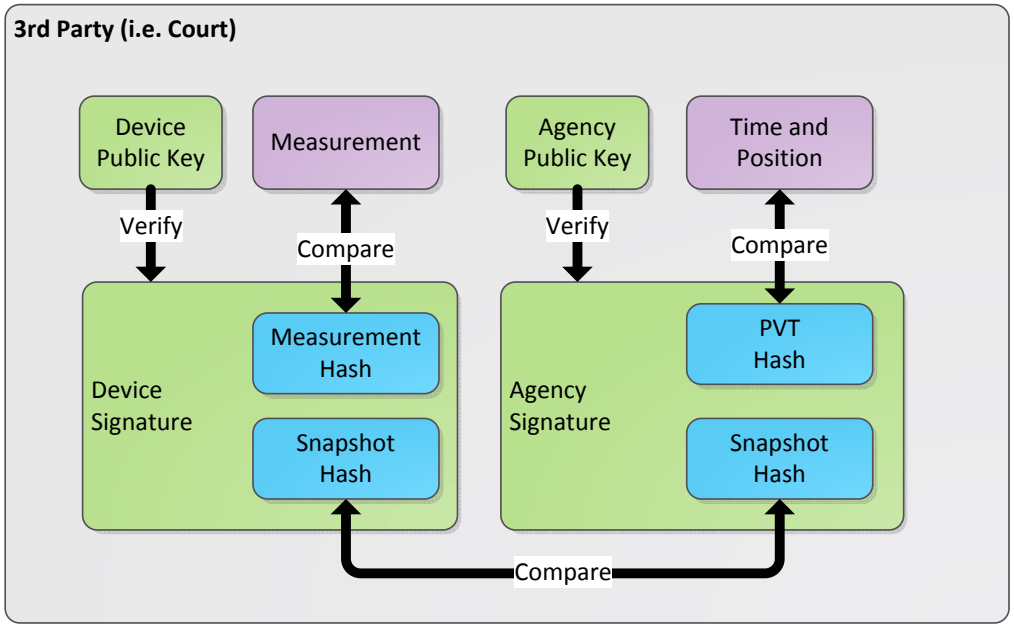

Fig. 5. Example of how a customer or 3rd party can validate the measurement/raw PRS snapshot combination

signals having a different timing information than predicted by the internal high precision clock [10].

Recently, different powerful spoofing detection techniques were introduced using only cheap and affordable standard commercial off-the-self (COTS) GNSS receiver. One applicable method was described in [11]. The idea is based on the fact that when the receiver is moved with respect to a static reradiator antenna, the carrier phases of different tracked satellites are correlated. In case of no spoofing/replay attack, the phases are uncorrelated. Instead of moving the receiver, it is also possible to either switch between two receiver antennas to get a similar effect or to use two antennas to take raw PRS snapshot from both of them. The actual anti-replay check can be done in the user receiver using an on-board COTS GNSS receiver. Still, an attacker could only replay Galileo PRS signals, which the COTS receiver cannot track and therefore check. In this case, the anti-replay check has to be carried out at the government authorized PRS agency. There, the PRS signals can not only be generated but also acquired and tracked to evaluate and check the phase responses when switching between antennas while recording the raw PRS snapshot.

V. Comparison with the State of the Art

As outlined in [3] one can generally distinguish between systems using classified signals as watermarks of opportunity and systems that are based on the incorporations of security and authentication signatures into the GNSS signal's message.

Our proposed method of using Galileo PRS with raw PRS snapshots and a dedicated authentication server is something in between. Galileo PRS is the first civil (but still classified) signal that has an authentication feature included in its signal structure. Since the PRS cannot be received and processed by someone unauthorized, the raw PRS snapshot is initially used as a watermark of opportunity. For a government agency controlled server, the raw PRS snapshot becomes a regular snapshot of processable signal data, since the server has the knowledge and authorization about the classified PRS signals.

In [12] and later extended in [13], a position and time authentication method using the military GPS PPS P(Y) signals as watermarks is described. According to their proposed concept, the raw data have to be recorded constantly by reference stations, to be able to prove the position and time later on using a cross-correlation between the snapshot signal and its reference received counterpart. In contrast to the Galileo PRS signals, the GPS PPS P(Y) signals cannot be regenerated for civil application authentication purpose. Consequently, a reference network sharing the same satellite visibility for several satellites to be used for the authentication is required. Such a reference network produces a considerable amount of raw data since the raw data has to be recorded continuously and saved for the span of time an authentication request might be necessary. Moreover, for a global coverage, a worldwide network of these trusted reference network stations is required. For mitigating false authentication results due to the C/A code transmitted together with the P(Y) signal, a high-pass filter is proposed. Since the P(Y) BPSK(10) is not spectrally isolated with the C/A BPSK(1) signal to be filtered away, a considerable power loss is the consequence. For the Galileo PRS raw snapshot methods, the Galileo OS signals are only high-pass filtered to ensure the privacy of the user. The OS/PRS signals are spectrally orthogonal as depicted in Figure 1. The high-pass filtering in our method does not affect the positioning and authentication ability.

In [14] a Galileo open service authentication system using Galileo PRS signals is described. Their proposal is to broadcast sections of the real PRS PRNs to a user receiver. These called "snippets" are then used in the user receiver to authenticate the user receiver's OS signal. It is stated that these snippets can be regarded as unclassified since their origin Galileo PRS PRNs were already transmitted and in principle could also have been received off-the-air with high gain antennas. Despite using also Galileo PRS signals for authentication purpose their method has elementary differences to the methods described in this paper. In the "snippets" solution, the end user device is doing the authentication, directly using parts of the classified Galileo PRS system. In our solution, the end user only gets a response to his request if something is trustworthy. Thus, all Galileo PRS relevant information are kept within a government agency controlled security boundary. No direct user interaction with the Galileo PRS system and its information is involved.

VI. Conclusion

In this paper we described an idea how ordinary people can profit from privacy protected localization and authentication of georeferenced measurements using the Galileo public regulated service (PRS). No security related PRS-receiver information or methods are needed on the user side. Everything security related is outsourced to a secure, government agency approved server.

Using the Galileo open service (OS) signals, recorded raw data snapshots are verified if OS and PRS signals were successfully recorded. Afterwards, the OS components are removed from the file to protect the privacy of the user and to shrink the snapshot size. Now, only authorities equipped with PRS keys and equipment are able to reconstruct time and position out of the modified snapshot signal. Moreover, the snapshot can also be cryptographically combined to a digital artifact just before it is transmitted to a server. This allows to authenticate georeferenced digital artifacts.

Different use cases with application examples for privacy protected localization and the authentication of georeferenced measurements were outlined. Moreover, possible attack scenarios were evaluated and appropriate mitigation strategies described.

Finally, we compared our methods to the state of the art. In contrast to the authentication using GPS military signals as watermarks, our method does not need a reference station network continuously recording the GPS military signals for later cross-correlation authentication. Instead, we propose a secure government approved PRS server reconstructing the pretended PRS signal scenario and using this input for cross-correlation

authentication. Moreover, with the help of a snapshot receiver processing technology, the position and time of the raw PRS snapshot can be obtained. In contrast to Galileo open service PRS authentication using "snippets", the authentication in our method is completely done within a save environment and not on the user side. Consequently, no Galileo PRS information is forwarded to the user. This prohibits abuse of Galileo PRS data with non authorized users or application since the government authorized server always retains control.

REFERENCES

[1] European Commission, "eCall: automated emergency call for road accidents mandatory in cars from 2015, http://europa.eu/rapid/press-release_IP-13-534_en.htm."

[2] J. E. Dobson and P. F. Fisher, "Geoslavery," *IEEE Technology and Society Magazine, Spring 2003*, pp. 47–52, spring 2003.

[3] L. Scott, "Proving Location Using GPS Location Signatures: Why it is needed and a way to do it," in *Proceedings of the 26th International Technical Meeting of the ION Satellite Division*, September 2013.

[4] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012, pp. 3591-3605*, 2012.

[5] D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Drone Hack: Spoofing Attack Demonstration on a Civilian Unmanned Aerial Vehicle," *GPS World, Vol. 23, August 2013, pp. 30-33*, 2012.

[6] "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea, http://www.utexas.edu/news/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/."

[7] A. Rügamer, I. Suberviola, F. Förster, G. Rohmer, A. Konovaltsev, N. Basta, M. Meurer, J. Wendel, M. Kaindl, and S. Baumann, "A Bavarian Initiative towards a Robust Galileo PRS Receiver," in *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), Portland, OR, September 2011, pp. 3668-3678*, September 2011.

[8] F. van Diggelen, *A-GPS: Assisted GPS, GNSS, and SBAS*, 1st ed. Artech House, 3 2009.

[9] J. Kelsey, B. Schneier, and C. Hall, "An authenticated camera," in *in Proceedings of the 12th Annual Computer Security Applications Conference, pp.24-30, 9-13 Dec 1996*, 1996.

[10] T. Mundt, "Location dependent digital rights management," in *Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005)*, 2005.

[11] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon, "GNSS spoofing detection using high-frequency antenna motion and carrier-phase data," in *Proceedings of the 26th International Technical Meeting of the ION Satellite Division*, 2013.

[12] S. Lo, D. de Lorenzo, P. Enge, D. Akos, and P. Bradley, "Signal authentication: A secure civil GNSS for today," *Inside GNSS*, pp. 30–39, september-october 2009.

[13] Z. Li and D. Gebre-Egziabher, "Performance Analysis of a Civilian GPS Position Authentication System," *Inside GNSS*, vol. 60, no. 4, pp. 249–265, Winter 2013.

[14] M. Turner, E. Chambers, E. Mak, L. Aguado, B. Wales, and M. Dumville, "PROSPA: Open Service Authentication," in *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013), Nashville, TN, September 2013, pp. 2992-2996*, 2013.