SAM-PAY: A Location-Based Authentication Method for Mobile Environments

electronics

MDPI

Article

SAM-PAY: A Location-Based Authentication Method for Mobile Environments †

Diana Gratiela Berbecaru

Department of Control and Computer Engineering, Politecnico di Torino, Corso Duca degli Abruzzi 24, 10129 Torino, Italy; diana.berbecaru@polito.it

† This paper inherits ideas and some implementation details from a paper previously published by the authors in 2011 at the 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing, Ayia Napa, Cyprus, 2011, pp. 141–145, https://doi.org/10.1109/PDP.2011.32. New ideas have been drawn based on the author's experience gained in the ROOT (Rolling Out OSNMA for the secure synchronization of Telecom networks) project (https://cordis.europa.eu/project/id/101004261).

Abstract: Wireless, satellite, and mobile networks are increasingly used in application scenarios to provide advanced services to mobile or nomadic devices. For example, to authenticate mobile users while obtaining access to remote services, a two-factor authentication mechanism is typically used, e.g., based on the ownership of a personal mobile phone, device, or (smart)card and the knowledge of a (static) username and password. Nevertheless, two-factor authentication is considered roughly "adequate" for security problems encountered today on the Internet and even less for ubiquitous or mobile environments. To increase the authentication level, several authentication methods of different classes may be combined to achieve more reliable user identification. In particular, location technologies allow ubiquitous applications to better exploit the (physical) location information in the authentication process. Consequently, in security applications based on multiple authentication factors, an additional authentication factor could be the location information protected for integrity against undesired modification. We present the SAM-PAY authentication method, which combines different authentication factors to obtain a more reliable user identification. The mechanism is based on the use of a (location-aware) device, the location information certified by a trusted external party, such as a component or element in a telecom network, and the knowledge of data, like a static PIN and a dynamically generated one-time password. We also describe the design and implementation of a real case scenario exploiting our SAM-PAY method, namely the refueling service at a self-service gas station. The test-bed put in place for this service demonstrates the feasibility and effectiveness of the SAM-PAY method in open mobile environments.

Keywords: authentication; location-based services; mobile payment

Academic Editor: Aryya Gangopadhyay

Received: 13 December 2024
Revised: 21 January 2025
Accepted: 30 January 2025
Published: 5 February 2025

Citation: Berbecaru, D.G. SAM-PAY: A Location-Based Authentication Method for Mobile Environments. *Electronics* **2025**, *14*, 621. https://doi.org/10.3390/electronics14030621

1. Introduction

Authentication is considered the most important security service, being at the basis of security solutions for systems and networks. To perform authentication in online and ubiquitous computing environments, users authenticate themselves using various methods with a variable reliability degree. These methods can be classified into three main classes or factors: what the user knows, e.g., a static password or a one-time code), what the user is, e.g., a fingerprint, retinal scan, voice-recognition pattern, or other biometric data), and what the user has, e.g., an ID card, a security token, or a personal cell phone or tablet. When speaking about authentication, we observe that there is no "one-size-fits-all" solution:

the number and types of authentication methods supported in the security products and services depend on the service provided and on the costs required for their implementation and deployment [1]. There is no unique authentication method that can fully protect against all types of security attacks. For example, the challenge-response one-time codes or application-level digital certificate-based authentication render phishing and malicious software attacks useless, but they do not fully protect against Man-In-The-Middle (MITM) attacks [2], even though both methods could be extended to achieve this protection too [3,4].

Nevertheless, the more services or data are security-sensitive, the more they are appealing to the attackers, who would definitely employ various methods to obtain access to them, such as token/notes theft, hidden code, worms, e-mails with malicious code, smart-card analyzers or a reader card manipulator, brute-force attacks, web page obfuscation, session hijacking, security policy violation, or website manipulation [5–7]. Obviously, the type of security attacks executed depends also on the authentication mechanism employed by the authentication system, and it becomes clearer that, especially in "remote" usage scenarios, there is a need for stronger authentication methods. The term "remote" is used here to refer to any infrastructure in which the clients and the service providers are connected via some potentially insecure network channel, like the mobile network or a data connection using the short-message service (SMS).

Considering the incredible advance of location sensing [8] and social-networking technologies, researchers have proposed even newer authentication classes, such as where the user is and when [9] or somebody you know [10], which should be used in combination with the classical authentication classes to protect (on one side) the service providers against the security attacks, and to have (at the same time) an attractive, transparent and usable service offered to the users. For example, the new types of authentication classes could be used in the mobile payment (m-payment) systems—like PayPal, PayCircle, or MobiPay—which are still considered "not secure enough", "too difficult and slow to use" [11], or available only for a limited variety of goods or a small selected clientele. Mobile payment systems have emerged in recent years, allowing users to pay with their devices (especially mobile phones) wherever they go.

Contribution. Many authentication solutions have been improved to guarantee high-assurance user identification. Even if a user enters the right username and password, there is still a probability that we might not deal with the legitimate user because the username and password could have been stolen. Some national systems or frameworks, like the electronic identity systems in Europe [12,13], have addressed this concern by deploying identity cards to citizens that can also be used to perform authentication when accessing some public services, such as for tax declaration or to register children at schools. Even though such cards are useful for enabling smoother administrative procedures asking for user identification, they are not (typically) used for payments. Even the use of biometric identification solutions is not 100% secure because there is always a chance for a false positive or negative.

Other proposals introduced the idea of combining several authentication methods in order to obtain a more reliable user identification [9,14–16]. Potentially, several factors should be employed to authenticate the user, including username/password, biometrics, behavioral characteristics, and location information, which must be protected for integrity against intentional attacks aimed to forge or spoof it. For instance, in [9], the probability that a user is at a certain location is used as a measure to parameterize the authentication level of the user. To combat identity theft, [17] proposed in 2005 an authentication architecture and system combining a physical location cross-check, a method for assuring uniqueness of location claims, and a centralized verification process. The above mentioned work extensively discusses necessary checks regarding the personal device used in the

authentication process, like device irregularities, theft, and cloning, and proposes that all identity verifications be funneled through a centralized point. This component allows to check that no "irregularities" have occurred for the personal device in question (based on ongoing device monitoring). Moreover, determining and securely asserting that a user is at a certain location is not trivial, as no single location-sensing technology has emerged as a clear winner in all kinds of environments. The Global Positioning System (GPS) is the de facto location technology for wide outdoor areas, but it does not work in covered areas or indoors, and it can be spoofed (as explained in Section 2). For indoor environments, many technologies have been proposed, but the data obtained from the different technologies should be combined to obtain a more complete picture of the physical environment and to determine the location with higher accuracy [18]. To mitigate these problems, a possible solution would be to use a specialized ground component, such as the Galileo Local Element (LE). These LEs are part of the overall Galileo definition, and the Galileo Program has foreseen the development of some selected experimental local elements [19]. Alternatively, for some critical services, the Open Service Navigation Message Authentication (OSNMA) could be employed. OSNMA is a data authentication function for Galileo Open Service worldwide users and is freely accessible. It provides (satellite) receivers with the assurance that the received Galileo navigation message is coming from the system itself and has not been modified. Even though OSNMA has been tested in some recent projects, e.g., in the ROOT project [20,21], it is still not widely exploited on a large scale because not every (user) device can be equipped with an OSNMA-aware receiver.

To authenticate remote users, we propose a method—named SAM-PAY (Secure Authentication Method for Payments)—which combines the usage of "classical" authentication methods (like static passwords and one-time passwords) with the location information provided by the GPS/EGNOS (European Geostationary navigation Overlay System) satellite networks and certified by a terrestrial component, namely the Galileo Local Element (LE).

SAM-PAY is based on three authentication factors: where a person is and when, i.e., the location of the user associated with the time information; something the user has, i.e., a specialized device used for localization and security purposes named User Terminal (UT); and something the user knows, i.e., a static PIN (Personal Identity Number) used to obtain access to the UT and a one-time password used to perform payment operations. The location/positioning information used in SAM-PAY is calculated by the UT and is certified by the ground component named Local Element.

We used the SAM-PAY authentication mechanism to design and implement a prototype self-service at gas stations. As noted in [22,23], although gathering and maintaining a rich profile of an individual and his or her transactions might seem antithetical to privacy interests, in some transactions or contexts (such as for m-payments), it might actually help protect the individual's privacy by raising a red flag about suspected identity theft. In our case, if the UT used to perform payments in the service at a gas station is suddenly being used to make purchases in other locations (e.g., cities) where it has not been used before, this could indicate that an attacker is fraudulently using the identity of a legitimate individual.

Organization. The paper is organized as follows. In Section 2, we present the related work and the location-authentication problem. In Section 3, we present the architecture and the functionality of its main components, in Section 4 we describe our SAM-PAY authentication method, and in Section 5 we present the design and implementation of the proposed SAM-PAY-based service at the self-service gas stations. In Section 6 we present the test-bed used to experiment with the proposed SAM-PAY-based service at the self-service gas stations. Finally, in Section 7, we indicate possible future developments and extensions for our work, and we conclude our paper in Section 8.

2. Related Work

Authentication is the act of establishing or confirming something (or someone) as authentic, such as confirming the identity of a person. Often, a combination of authentication factors is employed for user authentication. For example, using a card and a PIN, we have a two-factor authentication. Bruce Schneier noted in [24] that two-factor authentication is not adequate for security problems encountered today since "it won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had ten years ago, not the security problems we have today". Historically, biometric identification (such as fingerprints) has been used as the most authoritative method of authentication, but court cases in the US and elsewhere have raised fundamental doubts about fingerprint reliability. Moreover, they can be used only locally, such as to unlock devices used for authentication supporting asymmetric cryptography, as in FIDO [25]. Other biometric methods are promising (such as retinal and fingerprint scans) but have shown themselves to be easily spoofable in practice.

M. Alexander notes in [26] that new, cost-effective technology tools should be in every bank's online security arsenal to protect their customers against security fraud. Geolocation information has been used in the past in several location-based services, such as emergency and information services [27,28], tracking and monitoring systems [29], or even for establishing pairwise keys in the sensor networks [30]. Sensor networks are the ideal candidate for a wide range of applications like military operations, health monitoring, and data acquisition in hazardous environments, and sensor location plays a fundamental role in fulfilling their task. In the presence of attackers, most localization protocols for sensor networks are vulnerable to hostile environments [31]. In such contexts, some schemes like [32], also have methods for location estimation that tolerate malicious attacks against beacon-based location discovery. The beacon nodes are assumed to know their location, e.g., through GPS receivers, while the non-beacon nodes receive radio signals called beacon signals from the beacon nodes. Without protection, an attacker can mislead the location estimation at sensor nodes and subvert their normal operation. Thus, each beacon packet should provide authentication with a cryptographic key only known to the sender and intended receivers, while a non-beacon node should accept a beacon signal only when the beacon packet (carried by the beacon signal) can be authenticated. Other works have also considered insider attacks in wireless sensor networks [33] and proposed solutions for providing location-aware end-to-end data security in such networks. In the security field, some location-authentication schemes have been proposed [34,35], but location authentication is still considered a novel security service [36], mainly because location data need to be authenticated or certified by a trusted third party in order to be considered reliable [37]. Prominent among those tools is geolocation technology that determines the true geographic location (the country, state, or even city) of an online customer when they log into a bank website. When access to the account is made from a mismatched or unknown location, the bank's website could apply additional authentication measures. Thus, geolocation would not be just a fancy feature but may prove beneficial in a multifactor authentication strategy. This fact is also indicated in the guidance document released by the Federal Financial Institutions Examination Council (FFIEC) on authentication in the Internet-banking environment [38]. Moreover, in the past, some research proposals have explored the possibility of enhancing server authentication with location verification. For example, Yu et al. [39] explored the use of the Location Service (LCS) proposed by the telecommunication industry to achieve location-enhanced server authentication, which typically relies on public-key certificates in the X.509 format. This solution, named SALVE, defends against server impersonation by attackers with bogus certificates or exploiting stolen private keys of the legitimate server. Table 1 compares some selected location-

based authentication methods, their main characteristics and whether the method has been prototyped in a real context or in an environment with hardware specific to the service provider.

Table 1. Comparison of some location-based authentication methods and related works, underlining the main features of each proposal/scheme and whether the proposed scheme was deployed in a practical use case.

Scheme/Paper	Year	Short Description	Practical Test-Bed Implementation
[17]	2005	Proposes an authentication architecture and system to combat identity theft. The system combines a physical location cross-check (every user has a personal device, e.g., a cell phone or PDA, which can be used to securely detect location), a method for assuring the uniqueness of location claims, and a centralized verification process. Discusses extensively device cloning, theft, and device uniqueness.	No
[39]	2016	Location-based server authentication using secure Domain Name System (DNS) resolution and by leveraging Location Service proposed by the telecommunication industry.	yes (lab prototype)
[40]	2015	Proposes a mechanism to verify whether a mobile device currently resides within a geographical area at a given time, enabling the use of the location as an additional authentication factor. Addresses extensively trustworthiness, privacy, and practicability (uses the location of the phone as detected by the mobile network operator).	yes (lab prototype)
[41]	2016	Presents a framework for a sensor-based smartphone authentication system that continuously verifies the presence of a smartphone user. Location information is not employed.	Yes (lab prototype)
[42]	2023	method leveraging geolocation to verify the user's identity and prevent fraudulent transactions. Additionally, it allows controlling the ownership of transactions in a convenient way (e.g., allowing users to deactivate/reactivate authentication at any time, block the card in case it is stolen or lost, and set up a withdrawal limit). To obtain the exact user location via mobile, the solution relied on the Google Maps API, which employs a combination of GPS, cell tower triangulation, and various data sources.	yes (simulation environment with an ATM testing solution)
[43]	2022	Authentication protocol executed in RFID then NFC communication between a server, an ATM, and a smartphone equipped with a secure element (SE).	No
Our work	2025	Practical, user-friendly mechanism enabling an SP to verify whether the UT of a given user (previously registered at the SP via an IMEI and a phone number) currently resides within a certain geographical reference area at a given time. Moreover, the SP must be able to authenticate the user through a dynamic password (or One-Time Code) and a static password registered by the user at the SP.	Yes (simulation environment with ATM testing solution and specific hardware available at gas stations—service proposed)

Short discussion on location authentication. When speaking about location, one could think that the Global Positioning System (GPS) is the key to enhancing some of the authentication mechanisms already in place. GPS is a US space-based radio-navigation system that provides positioning, navigation and timing services to civilian users on a continuous worldwide basis, freely available to all. For anyone with a GPS receiver, the system provides accurate location and time information in all weathers, day and night, anywhere in the world. However, from a security point of view, obtaining secure (that is

authentic) location information using just a GPS receiver and civil GPS signal is (still) not possible [44]. In practice, the authenticity of the GPS signal cannot be guaranteed because the signal can be spoofed, i.e., a false signal could be generated by a dedicated GPS signal simulator, and a typical (GPS) receiver would not be able to detect that. Some "advanced" GPS receivers have been enhanced with antispoofing modules in order to detect whether the GPS signal comes from the satellite or a fake GPS simulator. However, in recent years, more and more advanced GPS simulators have also become readily available (e.g., they can be hired relatively cheaply), and thus, it is not possible to guarantee that a GPS signal really comes from the "right" source or not.

Some security solutions have tried to overcome a GPS signal authentication problem using additional components to certify the location information. For example, Denning & Doran defined in [34] a "location signature sensor" (LSS) tamper-proof device whose role is to create (and verify) a location signature (LS). An LS contains a geodetic position and is valid for a short time, like, for example, for 5 ms. Thus, an LS acts more or less like an unpredictable one-time password. Nevertheless, Kuhn notes in [45] some critical points of this solution, such as "this system only provides symmetric authentication and anyone able to verify the output of an LSS in a geographical region will also be able to fake the output of such a sensor from anywhere within the same region". Other solutions, like [46], propose to exploit the location-positioning capabilities of a wireless network to check out the location information. Specifically, the wireless network is instructed to determine whether the GPS position supplied by the node (directly or encrypted) is consistent with the network's own internal signal measurements. The return of low consistency would imply that the node has tampered its position identifier, and likely represents a malicious threat. Other solutions proposed to guarantee the authenticity of location information against the most common location-related attacks are briefly presented in [36].

Concerning the security of mobile banking, some security shortfalls in mobile-banking implementations [47] include authentication problems with GSM network, SMS/GPRS protocols, and security problems with the current bank's mobile-banking solutions [48–50]. Chikomo et al. [51] proposed, for example, a secure SMS message, in case a secure messaging protocol is used, and a secure GPRS (SGP) protocol used to create and conduct secure connections between mobile devices (acting as clients) and the bank servers (acting as servers). In the secure SMS solution, the authentication is performed by simply validating the message PIN with the receiver's stored PIN. The PIN has been previously selected by the user when he registered for a mobile-banking account. Thus, the authentication strength depends on the password policy (stating PIN length and syntax) used. For the confidentiality of the messages, the scheme employs symmetric cryptography. The key used for encryption is generated from the one-time password entered by the user. The one-time passwords are only known by the server and the user. The server stores the one-time password in its database. The password is indexed by the account identifier and the sequence number. Thereafter, the server uses the retrieved password as the decryption key to decode the encrypted contents. If the decryption is successful, the used OTP is discarded, and the server sequence counter for that account is incremented by 1.

In the SGP protocol, mutual authentication is established using certificates: each mobile application is packed with the server's certificate, and in this certificate, there is the server's public key, which is used to authenticate the server. The server also uses the client's SGP certificate to authenticate the clients. We think both approaches have intrinsic drawbacks: using just PIN-based authentication might not be secure enough because the users are often not cautious with their password selection [52], while in the second case, it is necessary to use SGP certificates, which are not available on most mobile devices. In our solution, we try to exploit data that are already available on most platforms (such

as the location data provided by the GPS receivers) or that can be easily configured or generated (such as static passwords or one-time passwords) in order to obtain an adaptive security solution.

Kim et al. [53] proposed, instead, a geolocation-based QR-code authentication scheme using mobile phones, which is resistant to ART (Active Real-Time) MITM phishing attacks. In this attack, an attacker collects authentication data (e.g., OTP, ID/password, a two-channel number from a user in plaintext) and then forwards this information to log into a web server. This solution combines the login history of the user's computer and location-based mutual authentication by assuming that the user already has an account on the web server and that the user and the web server share a (secret) key. Camenish et al. [40] designed and implemented an authentication mechanism that uses the location of a mobile phone as detected by the mobile network operator instead of relying on the location detected by the phone itself. Their approach has used an anonymous credential system to follow the privacy-by-design principle to ensure that sensitive information, e.g., location and subscriber data, are only revealed to parties that need to know. The exploitation of ground components for localization purposes has been explored extensively in the vehicular ad hoc networks (VANETS). For example, CARAVAN [54] describes a system aimed to locate and track a vehicle based on its transmissions during communication with other vehicles or with the road-side infrastructure, in particular with the Road-Side Units (RSU), which are connected to a location server by the wired network. The location server saves all the location information provided by the RSUs and processes the data together with the information from other sources, e.g., vehicle manufacturers, weather information centers, or traffic management centers. The location server also provides an interface for the location-based service providers, while a trusted Registration Authority provides authentication and authorization services to both vehicles and LBS providers. We see in the CARAVAN system some common points with our proposed system (exploitation of ground components for location services) and additional interesting features to be further analyzed for potential integration in SAM-PAY, like the possibility of achieving location privacy (unlinkability) (reviewed and discussed largely also in [55] in mobile environments) between two or more locations of a vehicle, and in our case, of a UT, in the presence of a global adversary.

Finally, it is worth mentioning that several patents have been proposed for improving the security of user authentication on devices via multiple factors and location techniques, e.g., [56–59].

3. Architecture and Components

The GNSS (Global Navigation Satellite System) acronym has been introduced within the European Galileo program to provide users with an alternative satellite system that is independent but interoperable with the US GPS. The system refers to any satellite constellation that provides global positioning, navigation, and timing services, including Galileo (EU), GPS (US), GLONAS (Russia), BeiDou (China). Galileo is a satellite navigation system specifically for civil purposes, generating new opportunities for the market and pushing the advance in technology for Europe. It became operational in 2013 with a constellation of 30 satellites placed in Medium Earth Orbits (MEO), over three circular planes inclined at 56° to the equator, and about 23,222 km altitude for a global coverage of the Earth.

In the architecture that we consider for the implementation of the service, all target applications are based on a common technological infrastructure (shown in Figures 1 and 2), which includes the GNSS-enabled User Terminals, the Local Element (LE), the middleware platform, and the Service Provider (SP). The middleware platform is a distributed software

layer that allows different SPs (for example, providing road, emergency, or finance services) to benefit from common functionalities, such as obtaining certified position information or exchanging data with user terminals. The LE is an element of the ground infrastructure of Galileo, which can be used for certifying the location information. The User Terminal (UT) is an advanced navigation device of rather small size that can support various communication technologies and that can be profiled based on the application service in which the UT is used. For example, in services based on Global System for Mobile (GSM) communication, such as road and/or finance services, the UT exchanges data with the LE over a GPRS communication channel, and communicates with the SPs via Unstructured Supplementary Service Data (USSD) technology. The SP interacts with the UT and with the LE by means of a set of web service adapters implemented in the middleware platform. Emergency and crisis-management applications instead are not necessarily based on the GSM network (which could not be reachable in certain zones, like mountains), but they typically use professional networks like the Very High Frequency (VHF) network, the TErrestrial Trunked RAdio (TETRA), or the innovative Digital Mobile Radio (DMR) technologies. In this case, a dedicated front end manages these professional networks from the service provider side, as shown in Figure 2.

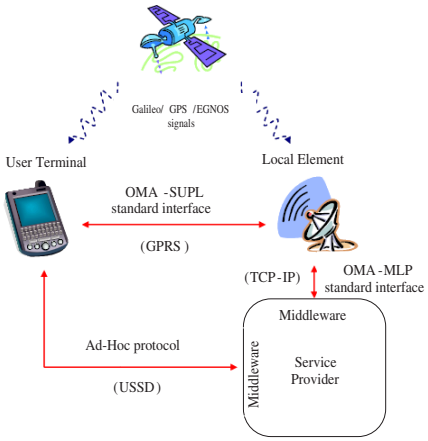

Figure 1. Possible architecture in the case of a GSM network.

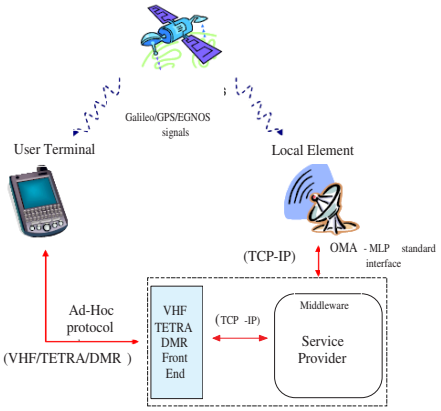

Figure 2. Possible architecture in the case of professional communication networks (VHF, TETRA and DMR).

General security requirements. In the considered architecture, we aim to define a practical, user-friendly mechanism enabling an SP to verify whether the UT of a given user previously registered at the SP via an International Mobile Equipment Identifier (IMEI) and a phone number currently resides within a certain geographical reference area at a given

time. Moreover, the SP must be able to authenticate the user through a dynamic password (or One-Time Code) and a static password registered by the user at the SP.

User Terminal. The UT is a technological platform that holds the hardware, software, and firmware elements to create an embedded, power-safe, and easily customizable system that combines localization functionalities with professional and standard communication capabilities. In particular, the UT is a Galileo-ready embedded system that integrates Assisted GPS (A-GPS) and DPGS/EGNOS functionalities enhanced with the possibility of combining GSM, VHF, TETRA, and DMR communication channels. An early prototype of a UT (along with a detailed description of its components) can be found in [60]. Nevertheless, the proposed SAM-PAY method can also be used with more recent Galileo-enabled user terminals. For example, the HAUT project [61] defined a Galileo HAS User Terminal, which is a light, small, portable, configurable, and autonomous device powered by a triple-frequency Galileo and GPS receiver. This UT provides free-of-charge, high-accuracy Precise Point Positioning (PPP) corrections (orbits, clocks) and code biases for Galileo and GPS to achieve real-time improved user-positioning performance. From a security point of view, we considered UT to be a trusted tamper-proof device that can store sensitive data (like secret keys), which can be further used in the authentication process.

Local Element. The Local Element (LE) is in charge of delivering enhanced performance in terms of accuracy, integrity, availability, and continuity by combining GALILEO/GPSIII satellite-only services with additional information coming from external sources.

In particular, the LE provides augmentation and certification features using data from GNSS and GSM cellular networks. The LE accesses the GNSS data via a dedicated connection to the GPS/EGNOS reference station, and it can exploit at the same time all the functions and data available in the mobile operator network.

According to the description given in [60], the Local Element provides two important functionalities: Assisted GPS and Certification. Assisted GPS allows the UT to improve its GNSS receiver performance in terms of Time-To-First-Fix (TTFF) and sensitivity. Certification guarantees the reliability of position and time information. This feature is obtained by integrating the GNSS integrity data with the data calculated using cellular-network positioning techniques. Moreover, the cross-check between GNSS and cell-based positions allows the isolating of unexpected high-GNSS errors and acts as an effective anti-fraud mechanism by detecting possible illegal alterations of the GNSS data collected from the user device. Moreover, according to the LE description in [60], an integrity-processing strategy was also defined, which has been optimized for difficult operating conditions. For example, in light-indoor or urban canyons, the GNSS signals may be strongly attenuated and affected by multiple reflections generated by the surrounding environment, such as buildings and trees. In these scenarios, a monitoring technique (which is an extension of the Receiver Autonomous Integrity Monitoring—RAIM—technique) is used for the GNSS signal-integrity check in order to detect and isolate the observations that are degraded (with the Fault Detection Estimation—FDE technique). If a certified position is needed, the system must guarantee that the probability of an outlier being used in the solution is below the so-called "integrity risk". In these cases, the Protection Level (PL) may be provided as an upper bound that a position error shall not exceed without being detected. The PL size may be determined as a function of the application requirements (e.g., integrity risk) and other parameters, such as the measurement error model, number of visible satellites, and external aiding. The PL parameter, together with the position estimation, may be used in liability-critical LBS services, such as in commercial applications, in order to guarantee a more reliable certified service and to minimize the probability of performing incorrect actions. e.g., an incorrect service charge.

4. Design of the SAM-PAY Authentication Method

As stated in the introduction, to defend themselves from attackers who falsely identify themselves as legitimate users, many security services and applications have started to implement stronger user-authentication methods based on more authentication factors or behavioral characteristics, especially when executing critical operations, like commercial transactions. For example, SwipePass [62] authenticates a smartphone user by examining the distinct physiological and behavioral characteristics embedded in the user's pattern-lock process. SwipePass is a two-factor authentication system that can sense the entire unlocking process and extract discriminative features to authenticate the user from the signal variations associated with hand dynamics.

In this work, we have used multiple authentication elements in our mechanism: the UT device, which can be used as a localization and security device, and the position of the UT, which is certified by the LE ground component. In addition, the third authentication factor used in our approach is the "classical" one-time code (OTC), referred to in some contexts also as a one-time password (OTP). Remote authentication with one-time codes is based on the idea that both the prover (the entity whose identity is verified) and the verifier share a secret: the client either presents the secret to the server as is (in this case, the shared secret is the OTC), or in a form derived according to some algorithm, like, for example, the OTC generated with an RSA SecurID authenticator. Typically, the OTC has a limited validity lifetime, e.g., 60 s for the codes generated by an RSA SecurID, because time is used for OTC generation. Moreover, to protect from replay attacks, the prover can use an OTC to authenticate themself to the verifier only once, i.e., an OTC cannot be re-used a second time.

The OTC can be generated independently by the user (for example, with an RSA SecurID token), or it can be generated by the verifier and sent to the user (if some previous relationship has been established between the user and the verifier). The latter method is used by several banks to offer advanced services, such as mobile banking or fund transfers to non-registered third-party accounts. In some security products, like in the Clavister MFA [63], the users authenticate with a mobile app Clavister Authenticator and an SMS-based One Time Password (OTP) service.

4.1. OTC Usage in SAM-PAY Authentication Method

In our approach, the OTC is generated by the SP (acting as a verifier) and is sent to the UT, which will be used transparently in the authentication phase. Since the SP needs to be aware of some important data related to the UT (such as user or terminal identification data), the user must register first with an SP. In the registration phase, the client provides the SP with several data, like personal data (name, surname, birthplace, fiscal code), phone number, and the IMEI code of the UT, uniquely identifying the UT device in the cellular network, the username and the password used by the user to authenticate to the SP, contract expiry date, bank account number (if a payment operation needs to be performed in the service) and other optional data like the subscription type (silver, gold), etc. In addition, in the registration phase, the user also sets two secret keys: key KS_e and key KS_a, which will be used, respectively, for encryption and authentication purposes. Furthermore, we assumed that when certifying the location of the UT, the "legitimate" user controls the device when (or immediately before) the evidence about the location has been acquired. In practice, we do not separate the location authentication (that assures the truthfulness of the claimed or presumed location) from the entity authentication, which helps corroborate the veracity of a claimed or presumed party's identity.

Since the UT (and implicitly the user controlling the UT) is authenticated based on the knowledge of the OTC, the ownership of the UT, and the location (of the UT), we looked

for a solution aimed at combining these authentication factors. In practice, in SAM-PAY, the user will be able to "recover" the OTC only if they are in a certain location (within the range of the Toleration Distance) and have access to the UT. To combine the location information and the OTC, we used a modified LDEA geo-encryption algorithm, described further below.

4.2. Modified LDEA Geo-Encryption Algorithm

The term "geo-encryption" or "location-based encryption" refers to a security algorithm that limits the access or decryption of some information content to specified locations and/or times [64,65]. The algorithm does not replace any of the conventional cryptographic algorithms, but it adds instead an additional security layer. By using a geo-encryption algorithm, the sender can restrict the location of the receiver for data decryption. Several geo-encryption algorithms have been proposed so far, such as [64]. Some of them are public, whereas others are protected by patents. One public geo-encryption algorithm is the location-dependent data-encryption algorithm (LDEA) published in [66], then in [67] and also used in [68] to enhance the security of a mobile information system by allowing the mobile clients to transmit a target latitude/longitude coordinate for data encryption to the information server. The client can only decrypt the ciphertext when the coordinate acquired from the GPS receiver matches with the target coordinate.

LDEA uses latitude/longitude coordinates to derive a key called LDEA-key, which is further combined (using an XOR operation) with a random session key to calculate the Final-key. This key is used to encrypt the plaintext data. When a target coordinate is determined for data encryption, the ciphertext can only be decrypted at the expected location. The LDEA algorithm uses public-key cryptography to ensure the authenticity and integrity of the session key.

In our approach, we retained from the LDEA algorithm [67] the technique used to derive the LDEA-key. For example, in Figure 3, E 12134.5971 means 121° and 34.5971 min east longitude. N 2504.7314 means 25° and 4.7314 min north latitude. Combine and hash means that the results of transforming the latitue/longitude coordinates into an integer part are further combined by performing a bitwise exclusive-OR operation. Then, a hash algorithm is utilized (note: MD5 was used in the original LDEA algorithm, but nowadays MD5 algorithm is considered obsolete and algorithms from SHA2 family are appropriate, such as SHA-256) to generate a digest for the combined result. If the digest is 256-bit long, the digest is split into two 128-bit values, called LDEA-keys. Additionally, we used a symmetric key (named KS_e) to generate the Final-key [23], which is composed of a 128-bit key (that can be used with the AES algorithm) and an 128-bit initialization vector (IV). The latter key (and IV) are used by the SP to encrypt the OTC with a symmetric algorithm (like AES-128 in CBC mode), obtaining thus the TOKEN that will be sent to the user (as shown in Figure 4). The resulting scheme is shown in Figure 4. Since the OTC is changed at each session, it is not necessary to use a random session key to protect the TOKEN from dictionary attacks. The resulting TOKEN, obtained by encrypting the OTC with the AES algorithm and the Final-key, will be different at each session. Since the position determined by the GPS receiver of the UT terminal could be inaccurate and inconsistent depending on how many satellite signals are received, the LDEA algorithm uses an additional parameter named Toleration Distance (TD), which must be known both by the sender and the receiver. The sender uses the TD (e.g., 0, 5, 10, 15, or 20 m) when calculating the LDEA-key, and the receiver can recover the OTC if it is within the TD range.

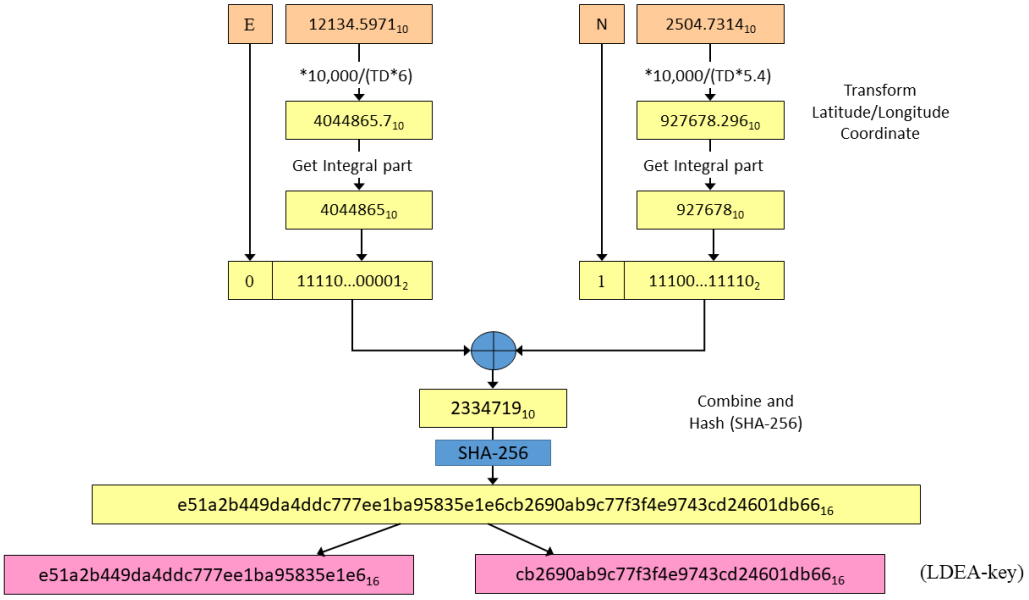

Figure 3. Generation of LDEA-key, where (*) means multiplication.

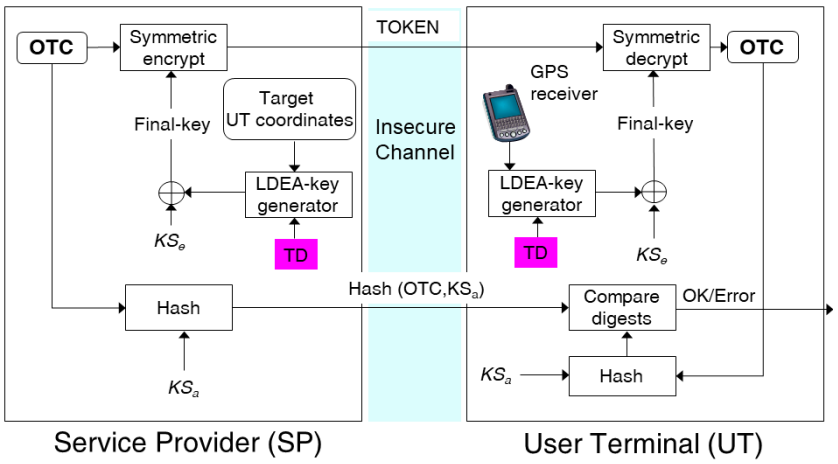

Figure 4. Modified LDEA geo-encryption algorithm used in the SAM-PAY authentication method.

5. Service Exploiting the SAM-PAY Method for Mobile Authentication

This section describes the design and implementation of a refueling service at a self-service gas station that uses the SAM-PAY method for authenticating remote clients. The payment operations are performed with the UT communicating with a Point-of-Sale (POS) device, which is typically available at any gas station providing such a service.

5.1. Traditional Refueling Service at Self-Service Gas Stations

In small towns and rural areas, gas stations sometimes allow customers to pump gas first and pay afterward. Due to the higher incidence of crime in large urban areas, customers must generally pay before pumping fuel. To allow customers to perform payments, modern gas stations have pay-at-the-pump capabilities: in most cases, credit, debit, ATM cards, fuel cards, and fleet cards are accepted. Occasionally, a station will have a pay-at-the-pump-only period per day when attendants are not present, often at night, and some stations are pay-at-the-pump-only 24 h a day. The following steps are typically executed when a customer performs self-service at the gas station: the user inserts money (or a payment card supported by the fuel dispenser) in the fuel pump that incorporates a pay-at-the-pump device, such as a Point-Of-Sale (POS) device. Subsequently, the user selects a pump number

(if several pumps are serviced by the same fuel dispenser) and waits for the pump to be unlocked. In practice, in the case of payment with a card, the pay-at-the-pump device typically communicates with the server of the customer's bank (via a dedicated payment circuit) in order to check the eligibility of the customer, i.e., to check the availability of the amount required in the customer's bank account. Once the customer has finished using the fuel dispenser and if no error has occurred during the whole operation, a receipt is returned by the pay-at-the-pump device to the user.

One of the most common frauds regarding fuel pumps is theft of credit or debit card data, as described in [69]. In this case, the thieves installed hard-to-detect electronic devices at the gas stations (also named skimming devices) in order to steal credit and debit card data. The skimming devices are typically small. They can be installed outside or inside the pump and are molded and painted to match the machine. Subsequently, the skimmed data are used to create cards used at the victims' expense. Skimming devices have been used for several years, most often at ATMs. Thieves increasingly target pumps because it is a cheap, easy way to steal credit and debit card information. With this method, the thieves managed, for example, to take more than $200,000 from up to 180 victims by stealing card data at a gas station in California (USA). Other types of fraud have been encountered, too. For example, in suburban Detroit, bandits climbed onto the roofs of at least seven gas stations and disabled satellites that send credit information [70]. The sabotage allowed drivers to fill tanks for hours at a time and steal millions in fuel simply by swiping plastic cards at the pump. The above paper also mentions another fraud scenario in which the thieves swapped card readers with their own to wirelessly send PINs and credit card numbers to a remote receiver. The scheme netted USD 4 million from 18,000 bank accounts. Credit and debit cards are the real honeypot for criminal bees because they typically carry key bank details that do not change over time. Thus, if an alternative payment method, such as using one-time codes (and restricted for use in a limited area), is used instead of the card itself, a card-cloning attack can be mitigated.

5.2. SAM-PAY Based Refueling Service at the Self-Service Gas Stations

Starting from the SAM-PAY authentication method, we designed a secure self-service at the gas stations in which the customers do not use cards for payment operations but rather dedicated UT devices (as briefly described in Section 3) and OTC codes. Moreover, the usage of an OTC code is limited both in time—because an OTC expires after a time interval, e.g., 15 min, and in space—because an OTC can be known only if the UT (and implicitly the customer) is localized in a restricted area at the gas station, and their position is certified by the LE acting as a trusted third party. The architecture and the workflow of the refueling service exploiting the SAM-PAY method for mobile client authentication are illustrated in Figure 5. In our current approach, the SP is part of a Private Payment System (PPS), which can manage both the payments performed with the UT device as described in this section, as well as the payments performed with traditional methods in which the clients use traditional credit or debit cards. However, in the tested scenario, we developed procedures to accept and manage only the first type of payment, i.e., the one performed with the UT.

In a PPS, both the issuer of the payment cards (like credit cards) and the acquirer, whose role is to provide and manage the POS machines used during payment operations, are part of the same system. In this way, the PPS is able to manage all payment transactions performed with the cards (or e-wallets) issued and recognized by himself (named "on-us" payments) without involving external circuits like Visa or Mastercard. Nevertheless, the PPS is also connected to external card circuits via a communication gateway so that it can manage payments performed with cards issued by external card issuers, which are typically referred to as "non-on-us payments".

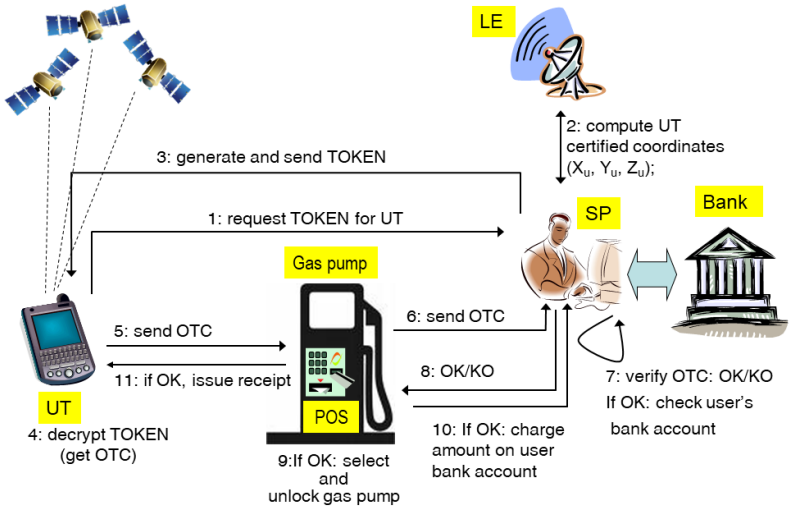

Figure 5. Architecture and workflow of the SAM-PAY-based refueling service at self-service gas stations.

During the design phase of the proposed refueling service, we considered several components:

(i). The user performing a payment operation has a personal UT (as described in Section 3), which is used together with the human–machine interface (HMI) for controlling the operations related to the transaction. The UT is certified by the PPS so that any payment operation originating from the UT can be considered an "on-us" payment, and it can be managed without requiring interaction with external circuits.

(ii). The UT is considered "trusted" by the owner to perform payments, and any other considerations on storing the secret information (i.e., the KS_e key) in a tamper-resistant security module on the UT is out of scope in this work. If the UT device is lost or stolen, the user must have the possibility to promptly inform the SP about this event via an emergency phone number, as happens presently with green numbers made available by any bank or credit card issuer. We also assume that it should be impossible for a malicious application to copy the sensitive data stored on a UT, even if the user presents the correct PIN code.

(iii). The HW/SW architecture of the UT allows the receipt and processing of signals of the GPS and EGNOS systems (and in the future of Galileo) by performing measurements on two distinct levels: (a) at a high level, where the coordinates (X, Y, Z) and the time information are processed; (b) at a low level, where the pseudorange measurements between the UT and each of the satellites reachable by the UT are processed.

(iv). The UT can manage two types of communication channels: (a) short-range communication, e.g., Zigbee, used for exchanging data with the POS of the gas-station provider; (b) long-range (GPRS)—used for exchanging data with the LE group component and the SP of the Payment System.

(v). The LE is a server with GPRS communication capability and navigation functionality, which determines (upon request from the SP) the certified position of a UT.

(vi). The SP is either a trusted third party that communicates with the PPS or with a bank for payment operations management (as shown in Figure 5), or it can even be part of the PPS or the banking system.

The proposed SAM-PAY-based service is composed of two phases: the user registration phase and the (service) operational phase. In the registration phase, both the gas-station provider and the clients provide data to the SP to obtain access to the SAM-PAY-enabled refueling service at the self-service gas-station. In particular, the client needs to create a profile holding the authentication credentials (username and password) required to log into

the service portal, the contact (name, surname, address), fiscal data, the unique identifier (i.e., the IMEI code) of the UT device, the bank coordinates required for the payment operations, and the consent for being localized during service provision. Moreover, the client also sets the symmetric keys KS_a and KS_e used for authentication and encryption in the modified LDEA algorithm.

The operational phase of the proposed refueling service is composed of 11 steps, shown in Figure 5, consisting of interactions among the main components. First, the user needs to unlock his UT by inserting an 8-character secret PIN. We note that this functionality is available for almost any cellular mobile phone, though more modern phones allow local unlocking of the phone via biometric data or by swiping on a 3 × 3 grid of contactable points. Subsequently, the user exploits the UT to retrieve from the SP the data (TOKEN) required for the payment operation. To complete the above operation, the user must have registered at the SP for this and they need to be located in the proximity of the gas pump. Next, the UT asks for a TOKEN from the SP to be used for the payment operation. The SP checks first whether the UT has been declared lost or stolen (and thus, it cannot be used to complete the transaction). If this is not the case, it queries the LE to obtain the certified position (expressed in terms of X_U, Y_U, Z_U coordinates) of the UT at a given time t1. Next, the SP issues a TOKEN with the modified LDEA algorithm (illustrated in Figure 5), and that has a limited time validity, e.g., 5–10 min. From the TOKEN, the UT can recover the OTC data, which can be used for payment purposes (Step 5). Finally, the SP verifies the OTC's correctness (in Step 7) and unlocks the gas pump if the validation of the OTC has been completed successfully (Step 9).

5.3. Service Provider Implementation Details

Since the Service Provider is a core element of the proposed service, we provide more details on its internal architecture and functionality. The SP system is based on a 3-tier model and is composed of the following modules: the SP Front End, the SP Application Server, and the SP Database Server.

The SP Front End consists of a service portal accessed via a web interface by the users (in this use case, the customers and the gas-station managers) to access customer information and details on the functionalities of the provided service. The service portal is composed of two logical–functional areas: (i) the public area, which contains the description of the service provided and of the types of users that can register to access it, general information about the contracts that can be subscribed, contact information, such as the phone number, e-mail address, etc.; and (ii) the private area, which can be accessed only by the users who registered for the service. Three types of users can obtain access to the private area via a login operation: the service portal administrator, the managers of the gas station providing the proposed SAM-PAY enabled-based service, and the customers who want to use the SAM-PAY-based refueling service.

The SP Application Server (AS) is composed of several software components, each of which is in charge of performing a dedicated task. For example, the Service Handler is the core of the AS and implements the finite state machine of the system controlling all the transactions involving the main actors (UT, LE Payment System, Database). The Service Handler implements the logic for verifying the UT credentials and the validity of the user contract. It generates the OTC and the TOKEN, verifies the temporal validity of the TOKEN in a payment operation, verifies the user eligibility, etc. The Service Handler communicates with the database via a dedicated DB Services module, with the UT via a dedicated UT subsystem module, with the LE via a dedicated LE subsystem module, and with the Payment System via a specialized Payment subsystem module. The UT subsystem implements the interface between the Service Handler and the Web Services

exposed by the Message Adapter of the middleware platform (TELECOM infrastructure) required for the UT–SP communication. The SP Application Server is configured with data required by the Service Handler when it exchanges data with the Message Adapter as part of the UT–SP communication, such as (i) the URL of the web service on the middleware portal, (ii) the type of messages exchanged (i.e., USSD), (iii) the authentication method (e.g., username and password), and (iv) other information such as the maximum number of retry attempts to be performed in a UT–SP communication if an operation (e.g., connect, authenticate) fails.

USSD (Unstructured Supplementary Service Data), unlike the asynchronous SMS service, opens a session, which may induce other network operators or a USSD response before releasing the connection. Almost 90% of the worldwide GSM network infrastructure and nearly 100% of mobile phones available today support the transport of USSD messages via the MAP (Mobile Application Part) protocol.

Mobile phones send USSD messages when the user chooses a function from a phone's menu, like call diversion to the subscriber's Voice Mailbox. Those "simple" applications tend to hide an aspect of USSD messages that allows the implementation of much more powerful applications on top of the USSD technology. A USSD session can remain active for some minutes. During this period (or session), the mobile phone and the HLR of the mobile network operator can exchange as many messages as they like, and this feature has been exploited in our proposed solution. In practice, the SP and the UT exchange the following USSD messages in the proposed SAM-PAY-enabled workflow:

- UT_SP_CONNECT (IMEI, phone number): is the message sent by the UT to connect to the SP. The Service Handler accepts the incoming connection when the UT (identified by its IMEI—International Mobile Equipment Identity) and the associated phone number are successfully found with success in the SP Database. When the connection has been established with success, the Service Handler returns to the UT a session ID, which will be used in the subsequent steps. If the connection establishment fails, the SP returns to the UT the failure reason, such as "user contract expired/not active" or "phone number not registered".
- UT_SP_AUTHENTICATE (session ID, username, password): is the message used by the UT to authenticate it to the SP using the username and the password set by the user in the registration phase. In case of authentication failure, an error message is returned to the UT, such as "UT not connected", "user not active", or "Uname/PW not valid".
- UT_SP_GETTOKEN (session ID): is the message used to retrieve the 32-byte-long TOKEN from the SP. If the operation is completed with success, the Service Handler returns to the UT the token together with the token lifetime (expressed in seconds). Otherwise, an error message is returned, such as "UT not connected", "UT not authenticated", "connection with LE failed", or "Token generation failed".
- UT_SP_PAYINFO (IMEI, phone number, username, password): is the message sent by the SP to inform the user about the status of the last "n" payment operations.

Each message is at most 80 bytes long and contains several (data, length, value) tuples, like the numeric code of the command—such as request session ID or request token—recognized by the SP, the current date and time, and the message checksum.

Similar messages are also exchanged between the LE and the LE subsystem module of the SP via a dedicated adapter provided by the middleware platform. Besides the SP_LE_CONNECT, SP_LE_AUTHENTICATE, and the SP_LE_DISCONNECT messages, we also encounter the SP_LE_GETPOSITION message, which is sent by the SP to the LE to obtain the certified position of a UT.

The Payment subsystem is divided into two submodules: the SP–POS module is in charge of the management of the transactions between the POS and the SP, whereas the SP–ABS module manages the transactions between the SP and the e-wallet ABS Card system. In both cases, a TCP/IP connection is established between the communicating parties. To interact with the POS device, the SP's Payment subsystem communicates internally with a dedicated HGEPOS Adapter, which is a software infrastructure implementing the interface between the SP–POS module of the Payment subsystem and the POS device. The messages exchanged between SP and the SP–POS module are: POS_SP_OPEN (POS SIA Code, operation number), which is the message sent by POS to the SP for the opening of the accounting transaction; POS_SP_PREAUTO (POS SIA Code, Operation number, OTC, max amount), which is the message sent by POS to the SP for the execution of the preauthorization operation; POS_SP_NOTIFY (POS SIA Code, Operation number, OTC, effective amount), which is the message sent by POS to the SP for the execution of accounting notification; and POS_SP_CLOSE (POS SIA Code, Operation number), which is the message sent by POS to the SP to indicate that the accounting transaction has been closed.

The transactions among the various actors are grouped in operational flows, each of which is composed of several phases. Each phase can be associated with a status (in progress, completed with success, or failed). The Service Handler keeps track of all the phases executed inside an operational flow, and all the relevant log trails are stored in the SP Database.

The SP Database Server is based on an Oracle database and contains the objects (Tables, Views, Procedures, etc.) required for the storage and management of the information of the Service Provider. The communication between the SP Application Server and the database server is implemented via the Oracle JDBC driver connection.

6. Test-Bed Description

This section provides details of the test-bed put in place in the frame of a concluded research project to demonstrate the functionality of the proposed refueling service exploiting the SAM-PAY method. The test-bed was aimed at validating the main phases expressed in the proposed service and evaluating the time required to complete the SAM-PAY-enabled transaction (about 10 s). The test-bed was installed in a controlled environment inside a research institute, and a test LE was situated at a Telecom provider in Italy. The test-bed was not, however, thought to be available to large-scale users until additional tests (e.g., against potential malicious users) were performed. However, we note that some components (e.g., the POS and the SP) can be easily adapted in other use-case scenarios, like hospitals, universities, or public administration offices. Figure 1 shows the test-bed, where the four screenshots depict the core components of the system described in Section 5.2. On the right-hand side of the picture, a fuel dispenser is clearly visible. A dispenser from a leading Italian company supplying electronic and computer science technology services for automated oil distribution has been used. This dispenser can deliver up to 2 products and is configured to manage two nozzles. The unit, containing the electronics, which is separated from the hydraulic part, allows the installation of different remote-control stations for pre- or post-payment solutions. In the test-bed, we integrated the fuel dispenser with the Maser Automation MAC Secure Plus remote-control station (i.e., the white tower shown in the middle of Figure 6), which is an Outdoor Payment Terminal (OPT) in line with the level of security requested for electronic payment transactions via smart-card. It implements an independent payment module that has obtained PCI (Payment Card Industry), PED (PIN Entry Device), EMV Level 1, and EMV Level 2 certifications. In particular, the payments can be performed both with credit cards (magnetic stripe and microchip) and debit cards through the panel POS (screenshot 1) developed by a multi-national company whose

business is focused on technology, telecommunications, security, and home automation. We customized this POS by integrating a Zigbee concentrator as a COM peripheral able to manage all the short-range connections coming from UTs (screenshot 2). In practice, we used a Texas Instruments CC2430 2.4 GHz IEEE 802.15.4/Zigbee chipset, the same one that we integrated in the UT prototype.

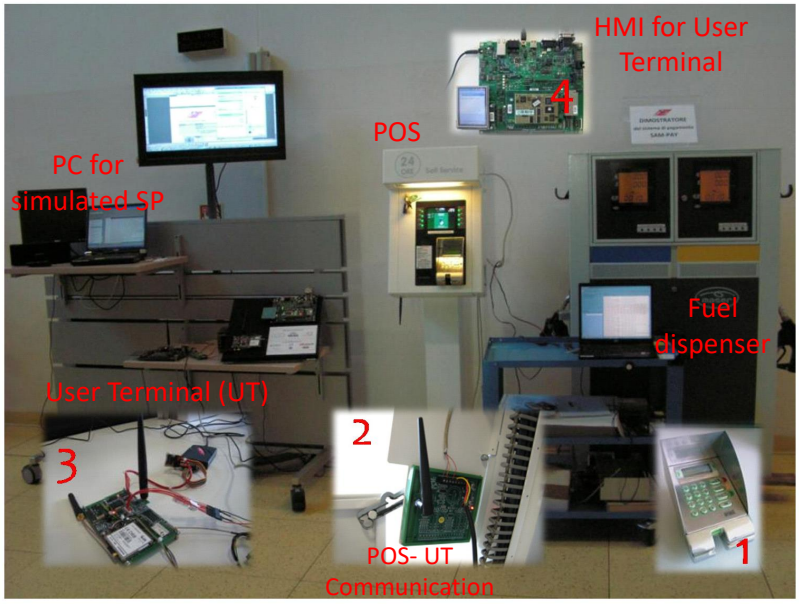

Figure 6. Test-bed for the self-service gas-station scenario exploiting the SAM-PAY authentication method.

As far as the UT prototype is concerned (screenshot 3), it was designed and developed to host both A-GPS and Galileo-ready chipsets like SIRF Star III or ublox 5. It also integrates a communication unit for the management of short-range and wide-area professional and commercial communications technologies: GPRS/USSD/SMS, Wi-Fi, Bluetooth, Zigbee, VHF, TETRA, and DMR. The platform has some additional peripherals like a 3-axis accelerometer for the identification of crashes and falls, a USB connector for fast data transfer, and some RAM banks (2 Mbytes) for data storage. Finally, the UT integrates an HMI to allow user interaction during payment procedures. We used a Windows CE-based development platform (screenshot 4) accessible through a serial port connection. For cryptographic operations, the OpenSSL library [71] was employed in an application developed in C language for the logical implementation of the modified LDEA algorithm. All the above components have been integrated with the SP and the LE according to the architecture and workflow described in Section 5.2.

7. Discussion and Future Work

The proposed SAM-PAY method was designed with usability in mind. It allows users to use simple one-time codes generated by the SP based on the user's location (as calculated via the GNSS system and certified by an LE ground element run by an MNO) and keys shared between the SP and the user in the registration phase. The work can be further extended in several directions: for example, in highly sensitive/critical scenarios, to mitigate GNSS spoofing attacks, the UT could be replaced with an UT integrated with a receiver supporting OSNMA [72], such as the ones manufactured by Septentrio and prototyped in the ROOT project [20]. Architecture and workflow could be further enhanced with anonymous credentials (as in [40]) to support service unlinkability and location privacy. Service unlinkability means that the mobile network operator should not be able to link

location-certification requests for a user to a particular Service Provider. Location privacy means that the SP, on the other hand, should not be able to learn location information for users identified with real identities, but pseudonyms should be used instead. Alternatively, the SP could merely learn whether the user of the UT is within a (larger) area where they are expected to be, thus enlarging the Toleration Distance to a wider reference area. Unfortunately, in this case, we increase the attack surface because the location information (used in the SAM-PAY method) is not accurate. Thus, potential attacks could occur if the attacker is placed within the reference area. Future work could address the extension of the SAM-PAY method to integrate behavioral factors and methods for countering device theft or cloning (i.e., assurance that the legitimate owner controls the device at transaction time). Last but not least, the work can be further extended to better protect sensitive symmetric keys (KS_e and KS_a) both on the user side and the SP side. In particular, a Trusted Execution Environment (TEE) could be exploited for this purpose since many phones on the market already include a TEE or parts thereof, e.g., ARM TrustZone or a Secure Enclave, in order to execute the trusted code. Additional tests are needed for this part because executing such a trusted code incurs a management burden and time requirements similar to those involved in running applications on Secure Elements [73]. Finally, the work could be extended to integrate additional authentication elements into the SAM-PAY method, like, for example, behavioral authentication, providing assurances that the mobile device is being used by its owner. Interesting proposals in this sense may be found in some research papers, e.g., [41,74].

8. Conclusions

In this paper, we have discussed several aspects that make designing context-enhanced authentication based on three or more authentication factors more challenging than their Internet counterparts. Our approach, named SAM-PAY, enables users to authenticate using a combination of contextual information, such as the geographical position (as determined through GPS/GNSS signals and certified by a ground telecommunication network component), and traditional authentication factors, such as based on what the user has and what the user knows. Certifying the location itself is a challenging task since various location-sensing technologies have emerged and can be used depending on the operation environment and the application scenario. Our contribution is three-fold: (i) we exploited an LE component used for certifying a UT's location within an acceptable "integrity risk", and a UT that supports various location-sensing technologies, which makes it suitable for use in various location-based applications; (ii) we proposed the SAM-PAY authentication method that makes use of both traditional and contextual (i.e., location) authentication factors; (iii) we designed and implemented a proof of concept for the SAM-PAY method, in the form of a case scenario that allows users to perform payments at self-service gas stations, without the need to use credit or debit cards. Our experimental test-bed shows that the method proposed also proves to be resistant to some attacks like card-number theft or MITM attacks, but future works could investigate the service resilience in various attack scenarios including external attackers, compromised components (e.g., the LE, UT) and malicious users.

Funding: Preliminary parts of this work (including the exploitation of a prototype LE for location certification and integration) have been performed in a concluded project "ANTICIPANDO GALILEO: PRODOTTI E SERVIZI A SUPPORTO DELLA MOBILITÀ E DELLA SICUREZZA" financed by Regione Piemonte (Italy). Part of the work related to the user authentication and identification in the SAM-PAY method has been performed by Dr. Diana Gratiela Berbecaru within the Ministerial Decree no. 1062/2021 and received funding from the FSE REACT-EU-PON Ricerca e Innovazione 2014-2020.

Data Availability Statement: No data is available for this research.

Acknowledgments: Author thanks Massimilano Spelat for his past collaboration in the concluded GAL-PMI Project (in Italian: ANTICIPANDO GALILEO: PRODOTTI E SERVIZI A SUPPORTO DELLA MOBILITÀ E DELLA SICUREZZA) for integrating the SAM-PAY method into the tested service and setting up the test-bed.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Fan, C.-I.; Shih, Y.-T.; Huang, J.-J.; Chiu, W.-R. Cross-Network-Slice Authentication Scheme for the 5th Generation Mobile Communication System. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 701–712. [CrossRef]
2. Ni, T.; Lan, G.; Wang, J.; Zhao, Q.; Xu, W. Eavesdropping Mobile App Activity via Radio-Frequency Energy Harvesting. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; USENIX Association: Berkeley, CA, USA, 2023 ; pp. 3511–3528. Available online: https://www.usenix.org/conference/usenixsecurity23/presentation/ni (accessed on 31 January 2025).
3. Weigold, T.; Kramp, T.; Baentsch, M. Remote Client Authentication. *IEEE Secur. Priv.* **2008**, *6*, 36–43. [CrossRef]
4. Dostálek, L.; Ledvina, J. Strong authentication for internet mobile application. In Proceedings of the 2015 International Conference on Applied Electronics (AE), Pilsen, Czech Republic, 8–9 September 2015; pp. 23–26.
5. Dimitriadis, C.K. Analyzing the Security of Internet Banking Authentication Mechanisms. *Inf. Syst. Control. J.* **2007**, *3*, 34–41.
6. Lee, K.; Lee, S.Y.; Yim, K. Classification and Analysis of Security Techniques for the User Terminal Area in the Internet Banking Service. *Secur. Commun. Netw.* **2020**, *2020*, 7672941. [CrossRef]
7. Hsu, C.-L.; Le, T.-V.; Hsieh, M.-C.; Tsai, K.-Y.; Lu, K.-Y.; Lin, T.-W. Three-Factor UCSSO Scheme With Fast Authentication and Privacy Protection for Telecare Medicine Information Systems. *IEEE Access* **2020**, *8*, 196553–196566. [CrossRef]
8. Hightower, J.; Borriello, G. Location systems for ubiquitous computing. *IEEE Comput.* **2001**, *34*, 57–66. [CrossRef]
9. Hulsebosch, R.J.; Bargh, M.S.; Lenzini, G.; Ebben, P.W.G.; Iacob, S.M. Context Sensitive Adaptive Authentication. In Proceedings of the European Conference on Smart Sensing and Context (EuroSSC) 2007, LNCS 4793, Kendal, UK, 23–25 October 2007; pp. 93–109.
10. Brainard, J.; Juels, A.; Rivest, R.; Szydlo, M.; Yung, M. Fourth Factor Authentication: Somebody You Know. In Proceedings of the ACM Conference on Computer and Communications Security (CCS), Alexandria, VA, USA, 30 October–3 November 2006; pp. 168–178.
11. Kadhiwal, S.; Zulfiquar, M.A.U.S. Analysis of mobile payment security measures and different standards. *Comput. Fraud. Secur.* **2007**, *2007*, 12–16. [CrossRef]
12. Berbecaru, D.G.; Lioy, A.; Cameroni, C. On Enabling Additional Natural Person and Domain-Specific Attributes in the eIDAS Network. *IEEE Access* **2021**, *9*, 134096–134121. [CrossRef]
13. Berbecaru, D.; Lioy, A.; Cameroni, C. Electronic Identification for Universities: Building Cross-Border Services Based on the eIDAS Infrastructure. *Information* **2019**, *10*, 210. [CrossRef]
14. Zheng, H.; Kwak, J.; Son, K.; Lee, W.; Kim, S.; Won, D. Confidence Value Based Multi Levels of Authentication for Ubiquitous Computing Environments. In Proceedings of the International Conference on Computational Science and its Applications (ICCSA) 2006, LNCS 3981, Glasgow, UK, 8–11 May 2006; pp. 954–963.
15. Al-Muhtadi, J.; Ranganathan, A.; Campbell, R.; Mickunas, M.D. A Flexible, Privacy-Preserving Authentication Framework for Ubiquitous Computing Environments. In Proceedings of the International Conference on Distributed Computing Systems Workshops (ICDCSW), Vienna, Austria, 2–5 July 2002; pp. 771–776.
16. Liu, Y.; Huang, W.; Zhuo, M.; Zhou, S.; Li, M. Mobile Payment Protocol with Deniably Authenticated Property. *Sensors* **2023**, *23*, 3927. [CrossRef]
17. van Oorschot, P.C.; Stubblebine, S. Countering Identity Theft Through Digital Uniqueness, Location Cross-Checking, and Funneling. In *Financial Cryptography and Data Security*; Patrick, A.S., Yung, M., Eds.; FC 2005. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005. [CrossRef]
18. Ranganathan, A.; Al-Muhtadi, J.; Chetan, S. MiddleWhere: A Middleware for Location Awareness in Ubiquitous Computing Applications. In Proceedings of the Middleware 2004, LNCS 3231, Toronto, ON, Canada, 18–20 October 2004; pp. 397–416.
19. Antonini, M.; Ruggieri, M.; Prasad, R. Communications within the Galileo locally assisted services. In Proceedings of the IEEE Aerospace Conference, Big Sky, MT, USA, 6–13 March 2004; Volume 2, pp. 1312–1321.
20. Pini, M.; Minetto, A.; Vesco, A.; Berbecaru, D.; Murillo, L.M.C.; Nemry, P.; De Francesca, I.; Rat, B.; Callewaert, K. Satellite-derived Time for Enhanced Telecom Networks Synchronization: The ROOT Project. In Proceedings of the 2021 IEEE 8th International Workshop on Metrology for AeroSpace (MetroAeroSpace), Naples, Italy, 23–25 June 2021; pp. 288–293. [CrossRef]

21. Berbecaru, D.G.; Sisinni, S.; Lioy, A.; Rat, B.; Margaria, D.; Vesco, A. Mitigating Software Integrity Attacks with Trusted Computing in a Time Distribution Network. *IEEE Access* **2023**, *11*, 50510–50527. [CrossRef]
22. Hansen, M.; Schwartz, A.; Cooper, A. Privacy and Identity Management. *IEEE Secur. Priv.* **2008**, *6*, 38–45. [CrossRef]
23. Berbecaru, D. LRAP: A Location-Based Remote Client Authentication Protocol for Mobile Environments. In Proceedings of the 2011 19th International Euromicro Conference on Parallel, Distributed and Network-Based Processing, Ayia Napa, Cyprus, 9–11 February 2011; pp. 141–145. [CrossRef]
24. Schneier, B. Two-Factor Authentication: Too Little, Too Late. *Commun. ACM* **2005**, *48*, 136. [CrossRef]
25. FIDO Alliance. FIDO Attestation: Enhancing Trust, Privacy, and Interoperability in Passwordless Authentication. 2024. Available online: https://fidoalliance.org/wp-content/uploads/2024/06/EDWG_Attestation-White-Paper_2024-1.pdf (accessed on 12 December 2024).
26. Alexander, M. Keeping Online Banking Safe: Why Banks Need Geolocation and Other New Techniques Right Now. May 2005. Available online: https://www.bankersonline.com/articles/106833 (accessed on 24 February 2009).
27. Becker, C.; Durr E. On Location Models for Ubiquitous Computing. In *Personal and Ubiquitous Computing*; Springer: London, UK, 2005; Volume 9, pp. 20–31. [CrossRef]
28. Toye, E.; Sharp, R.; Madhayapeddy, A.; Scott, D. Using Smart Phones to Access Site-Specific Services. In *IEEE Pervasive Computing*; Springer: London, UK, 2005; Volume 4, pp. 60–66.
29. Gruteser, M.; Liu, X. Protecting Privacy in Continuous Location-Tracking Applications. *IEEE Secur. Priv. Mag.* **2004**, *2*, 28–34. [CrossRef]
30. Liu, D.; Ning, P. Location-based pairwise key establishments for static sensor networks. In Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, Fairfax, VA, USA, 31 October 2003; pp. 72–82. [CrossRef]
31. Wu, Y.; Li, C.; Hou, Y.T.; Lou, W. A Real-Time Super-Resolution DoA Estimation Algorithm for Automotive Radar Sensor. *IEEE Sens. J.* **2024**, *24*, 37947–37961. [CrossRef]
32. Liu, D.; Ning, P.; Du, W.K. Attack-resistant location estimation in sensor networks. In Proceedings of the IPSN 2005—Fourth International Symposium on Information Processing in Sensor Networks, 2005, Boise, ID, USA, 25–27 April 2005; pp. 99–106. [CrossRef]
33. Ren, K.; Lou, W.; Zhang, Y. LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks. *IEEE Trans. Mob. Comput.* **2008**, *7*, 585–598. [CrossRef]
34. Denning, D.E.; MacDoran, P.F. Location-based authentication: Grounding cyberspace for better security. *Comput. Fraud. Secur.* **1996**, *1996*, 12–16. [CrossRef]
35. Wullems, C.; Pozzobon, O.; Kubik, K. Trust Your Receiver? Enhancing Location Security. *GPS World* **2004**, *15*, 23–30.
36. Ferreres, A.I.G.-T.; Alvarez, B.R.; Garnacho, A.R. Guaranteeing the Authenticity of Location Information. *IEEE Pervasive Comput.* **2008**, *7*, 72–80. [CrossRef]
37. González-Tablas, A.I.; Kursawe, K.; Ramos, B.; Ribagorda, A. Survey on Location Authentication Protocols and Spatial-Temporal Attestation Services. In Proceedings of the Embedded and Ubiquitous Computing—EUC 2005 Workshops, Nagasaki, Japan, 8–9 December 2005; Enokido, T., Yan, L., Xiao, B., Kim, D., Dai, Y., Yang, L.T., Eds.; EUC 2005. Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2005; Volume 3823. [CrossRef]
38. Federal Financial Institutions Examination Council. Authentication in Internet Banking Environment. Available online: https://www.ffiec.gov/pdf/authentication_guidance.pdf (accessed on 13 December 2024).
39. Yu, D.-Y.; Ranganathan, A.; Masti, R.J.; Soriente, C.; Capkun, S. SALVE: Server authentication with location verification. In Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom '16), New York, NY, USA, 3–7 October 2016; Association for Computing Machinery: New York, NY, USA, 2016; pp. 401–414. [CrossRef]
40. Camenisch, J.; Ortiz-Yepes, D.A.; Preiss, F.-S. Strengthening Authentication with Privacy-Preserving Location Verification of Mobile Phones. In Proceedings of the 14th ACM Workshop on Privacy in the Electronic Society (WPES '15), Denver, CO, USA, 12 October 2015; Association for Computing Machinery: New York, NY, USA, 2015; pp. 37–48. [CrossRef]
41. Shen, C.; Yu, T.; Yuan, S.; Li, Y.; Guan, X. Performance Analysis of Motion-Sensor Behavior for User Authentication on Smartphones. *Sensors* **2016**, *16*, 345. [CrossRef]
42. Alabdulatif, A.; Samarasinghe, R.; Thilakarathne, N.N. A Novel Robust Geolocation-Based Multi-Factor Authentication Method for Securing ATM Payment Transactions. *Appl. Sci.* **2023**, *13*, 10743. [CrossRef]
43. Chabbi, S.; Araar, C. RFID and NFC authentication protocol for securing a payment transaction. In Proceedings of the 2022 4th International Conference on Pattern Analysis and Intelligent Systems (PAIS), Oum El Bouaghi, Algeria, 12–13 October 2022; pp. 1–8.
44. Berbecaru, D.G.; Lioy, A. Attack Strategies and Countermeasures in Transport-Based Time Synchronization Solutions. *In Intelligent Distributed Computing XIV. IDC 2021*; Camacho, D., Rosaci, D., Sarné, G.M.L., Versaci, M., Eds.; Studies in Computational Intelligence; Springer: Cham, Switzerland, 2021; Volume 1026. [CrossRef]

45. Kuhn, M.G. An Asymmetric Security Mechanism for Navigation Signals. In Proceedings of the 6th Int'l Workshop Information Hiding (IH), LNCS 3200, Toronto, ON, Canada, 23–25 May 2004; pp. 239–252. [CrossRef]
46. Malaney, R.A. A location enabled wireless security system. In Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), Dallas, TX, USA, 29 November–3 December 2004; Volume 4, pp. 2196–2200.
47. Yildirim, N.; Varol, A. A Research on Security Vulnerabilities in Online and Mobile Banking Systems. In Proceedings of the 2019 7th International Symposium on Digital Forensics and Security (ISDFS), Barcelos, Portugal, 10–12 June 2019; pp. 1–5. [CrossRef]
48. Bellare, M.; Garay, J.A.; Hauser, M.; Herzberg, A.; Krawczyk, H.; Steiner, M.; Tsudik, G.; Van Herreweghen, E.; Waidner, M. Design, implementation, and deployment of the iKP secure electronic payment system. *IEEE J. Sel. Areas Commun.* **2000**, *18*, 611–627. [CrossRef]
49. Al-Fuqaha, A.; Al-Ibrahim, O.; Baird, J. Geo-encryption: Using GPS to enhance data security. In Proceedings of the Global Telecommunications Conference 2005 (GLOBECOM '05), St. Louis, MO, USA, 28 November–2 December 2005; Volume 3, pp. 1721–1725.
50. Zhu, J.; Wu, P.; Wang, X.; Zhang, J. SenSec: Mobile security through passive sensing. In Proceedings of the 2013 International Conference on Computing, Networking and Communications (ICNC), San Diego, CA, USA, 28–31 January 2013; pp. 1128–1133. [CrossRef]
51. Chikomo, K.; Chong, M.K.; Arnab, A.; Hutchison, A. Security of Mobile Banking. University of Cape Town, South Africa, Technical Report, 1 November 2006. Available online: https://www.academia.edu/67750990/Security_of_Mobile_Banking (accessed on 31 January 2025).
52. Shay, R.; Bhargav-Spantzel, A.; Bertino, E. Password Policy Simulation and Analysis. In Proceedings of the ACM Workshop on Digital Identity Management (DIM), Fairfax, VA, USA, 2 November 2007; pp. 1–10. [CrossRef]
53. Kim, S.H.; Choi, D.; Jin, S.H.; Lee, S.H. Geo-location based QR-Code authentication scheme to defeat active real-time phishing attack. In Proceedings of the 2013 ACM Workshop on Digital Identity Management (DIM '13), Berlin, Germany, 8 November 2013; Association for Computing Machinery: New York, NY, USA, 2013; pp. 51–62. [CrossRef]
54. Sampigethaya, K.; Huang, L.; Li, M.; Poovendran, R.; Matsuura, K.; Sezaki, K. Caravan: Providing location privacy for VANET. *Int. J. Ad Hoc Ubiquitous Comput.* **2012**, *10*, 219–229.
55. Asuquo, P.; Cruickshank, H.; Morley, J.; Ogah, C.P.A.; Lei, A.; Hathal, W.; Bao, S.; Sun, Z. Security and Privacy in Location-Based Services for Vehicular and Mobile Communications: An Overview, Challenges, and Countermeasures. *IEEE Internet Things J.* **2018**, *5*, 4778–4802. [CrossRef]
56. Krishnamurthi, G. Method and Apparatus for Using a Multi-Factor Password or a Dynamic Password for Enhanced Security on a Device. U.S. Patent 9,659,164B2, 23 May 2017. Available online: https://patents.google.com/patent/US9659164B2/en (accessed on 31 January 2025).
57. Cohen, G.K.; Green, M.D.; Smith, C.P.; Stuart, C.; Wright, K.L.; Young, M.M. Systems and Methods for Location-Binding Authentication. U.S. Patent 11,132,425B1, 28 September 2021. Available online: https://patents.google.com/patent/US11132425B1/en (accessed on 31 January 2025).
58. Bharghavan, V.; Gangam, A.; Maram, P.K.; Gunasekaran, B. System and Method for Authorizing a Transaction Based on Dynamic Location Updates from a User Device. U.S. Patent 11,636,489B2, 25 April 2023. Available online: https://patents.google.com/patent/US11636489B2/en (accessed on 31 January 2025).
59. Bharghavan, V.; Han, S.-W.; Zhang, Z. Enriching Transaction Request Data for Improving Fraud Prevention Systems on a Data Communication Network with User Controls Injected to Back-End Transaction Approval Requests in Real-Time with Transactions. U.S. Patent 20210166237A1, 3 June 2021. Available online: https://patents.google.com/patent/US20210166237A1/en (accessed on 31 January 2025).
60. Dominici, F.; Mazzocchi, D.; Mulassano, P.; Spelat, M.; Boiero, G.; Lovisolo, P. NAV/COM Hybrid Architecture for Innovative Location Based Payment Systems. In Proceedings of the 2009 6th IEEE Consumer Communications and Networking Conference, Las Vegas, NV, USA, 11–13 January 2009; pp. 1–5. [CrossRef]
61. González, E.; Pintor, P.; Senado, A.; Dhital, N.; Ostolaza, J.; Hernández, C.; Vázquez, J.; de Blas, J.; Lagrasta, S. Testing the Galileo High Accuracy Service User Terminal (HAUT) in Static Scenarios. *Eng. Proc.* **2023**, *54*, 17. [CrossRef]
62. Chen, Y.; Ni, T.; Xu, W.; Gu, T. SwipePass: Acoustic-based Second-factor User Authentication for Smartphones. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* **2022**, *6*, 1–25. [CrossRef]
63. Clavister Launches Strong Authentication Solution with Clavister Multi Factor Authentication (MFA). Available online: https://www.businesswire.com/news/home/20160607006861/en/Clavister-Launches-Strong-Authentication-Solution-with-Clavister-Multi-Factor-Authentication-MFA (accessed on 31 January 2025).
64. Qiu, D. Security Analysis of Geoencryption: A Case Study Using Loran. In Proceedings of the 20th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS), Fort Worth, TX, USA, 25–28 September 2007; pp. 1146–1154.

65. Berbecaru, D.G.; Pintaldi, L. Exploiting Emercoin Blockchain and Trusted Computing for IoT Scenarios: A Practical Approach. In Proceedings of the 2023 IEEE Symposium on Computers and Communications (ISCC), Gammarth, Tunisia, 9–12 July 2023; pp. 771–776. [CrossRef]
66. Liao, H.C.; Chao, Y.H.; Hsu, C.Y. A Novel Approach for Data Encryption Depending on User Location. In Proceedings of the Tenth Pacific Asia Conference on Information Systems (PACIS 2006), Kuala Lumpur, Malaysia, 5–9 July 2006. Available online: https://aisel.aisnet.org/pacis2006/ (accessed on 13 December 2024).
67. Liao, H.C.; Chao, Y.H. A New Data Encryption Algorithm Based on the Location of Mobile Users. *Inf. Technol. J.* **2008**, *7*, 63–69. https://scialert.net/abstract/?doi=itj.2008.63.69 (accessed on 31 January 2025) [CrossRef]
68. Liao, H.C.; Lee, P.C.; Chao, Y.H. A Location-Dependent Data Encryption Approach for Enhancing Mobile Information System Security. In Proceedings of the 9th International Conference on Advanced Communication Technology (ICACT 2007), Phoenix Park, Republic of Korea, 12–14 February 2007; pp. 625–628.
69. Jackson, C. How to Spot and Avoid a Credit Card Skimmer at the Gas Pump, 16 February 2023. Available online: https://www.snbonline.com/about/news/fraud-alert-how-to-detect-a-card-skimmer- (accessed on 13 December 2024).
70. Fuel Card Fraud Is Rampant in 2023. Available online: https://www.multiservicefuelcard.com/news/fuel-card-fraud-is-rampant-in-2023-here-are-seven-ways-truckers-can-fight-back/ (accessed on 13 December 2024).
71. OpenSSL Library. Available online: https://openssl-library.org/ (accessed on 31 January 2025).
72. OSNMA: The Latest in GNSS Anti-Spoofing Security. Available online: https://www.septentrio.com/en/learn-more/insights/osnma-latest-gnss-anti-spoofing-security (accessed on 31 January 2025).
73. Ekberg, J.-E.; Kostiainen, K.; Asokan, N. The Untapped Potential of Trusted Execution Environments on Mobile Devices. *IEEE Secur. Priv.* **2014**, *12*, 29–37. [CrossRef]
74. Qin, L.; Guo, M.; Zhou, K.; Chen, X. An Identity Authentication Method Based on Inertial Sensors and Pressure Insoles. In Proceedings of the 2024 39th Youth Academic Annual Conference of Chinese Association of Automation (YAC), Dalian, China, 7–9 June 2024; pp. 630–634. [CrossRef]