Torben Kuseler; Ihsan Lami and Hisham Al-Assam, "Location-assured, multifactor authentication on smartphones via LTE communication", Proc. SPIE 8755, Mobile Multimedia/Image Processing, Security, and Applications (May 28, 2013); doi: 10.1117/12.2018027

Location-assured, multi-factor authentication on Smartphones via LTE communication

Torben Kuseler, Ihsan A. Lami, Hisham Al-Assam
Applied Computing Department
University of Buckingham
Hunter Street, Buckingham, MK18 1EG, UK
(phone: 44-1280-814080; email: first.last@buckingham.ac.uk)

ABSTRACT

With the added security provided by LTE, geographical location has become an important factor for authentication to enhance the security of remote client authentication during mCommerce applications using Smartphones. Tight combination of geographical location with classic authentication factors like PINs/Biometrics in a real-time, remote verification scheme over the LTE layer connection assures the authenticator about the client itself (via PIN/biometric) as well as the client’s current location, thus defines the important aspects of “who”, “when”, and “where” of the authentication attempt without eaves dropping or man on the middle attacks. To securely integrate location as an authentication factor into the remote authentication scheme, client’s location must be verified independently, i.e. the authenticator should not solely rely on the location determined on and reported by the client’s Smartphone. The latest wireless data communication technology for mobile phones (4G LTE, Long-Term Evolution), recently being rolled out in various networks, can be employed to enhance this location-factor requirement of independent location verification. LTE’s Control Plane LBS provisions, when integrated with user-based authentication and independent source of localisation factors ensures secure efficient, continuous location tracking of the Smartphone. This feature can be performed during normal operation of the LTE-based communication between client and network operator resulting in the authenticator being able to verify the client’s claimed location more securely and accurately. Trials and experiments show that such algorithm implementation is viable for nowadays Smartphone-based banking via LTE communication.

Keywords: Authentication, Location, LTE, mCommerce, Multi-Factor, Smartphones

1. INTRODUCTION

Smartphones are becoming a major part in everybody’s daily life. All kinds of mCommerce activities, including financial banking transactions and online shopping, are nowadays performed online via Smartphone applications whilst on the move. The wide availability of mCommerce applications on Smartphones creates new challenges in protecting these applications and the authentication process itself, and therefore demands secure and reliable remote client verification. In remote authentication, the authenticator does not have a direct knowledge about the “who, when, and where” of the remote client. Instead, only the remotely received client authentication factors are available.

Beside the classical authentication factors like PINs or passwords, location information becomes a more and more important factor in remote client authentication as location information grounds the client’s authentication attempt to a specific and clearly defined position on earth. However, the secure integration and verification of the client’s location information during the authentication process is difficult and should be performed independently from the client’s Smartphone to avoid manipulation. To achieve these aims, this paper proposes a novel scheme that combines LTE-based location provisions of Smartphones with a smart authentication process to assure secure mCommerce (e.g. bank transactions) with minimum overhead. LTE-location services are used to independently verify the client’s claimed location (based on the position determined by the Smartphone’s on-board GNSS receiver), i.e. the client based location information will be cross-checked with the location information independently determined via the LTE-location services provided by the mobile network operator.

The rest of this paper is organised as follows. Section 2 provides an overview about the current use of location information as an authentication factor and gives further background information about the LTE technology. Section 3 details the proposed location-based, multi-factor authentication scheme and explains the security and implementation enhancements resulting from the integration of LTE to establish and verify the client’s location. Section 4 concludes this paper and gives recommendations towards future work.

2. BACKGROUND AND RELATED WORK

2.1 Using Client’s Location Information to enhanced authentication security

Up until very recently, clients were authenticated in the majority of mCommerce applications via a combination of one or more classic (i.e. knowledge-, object-, or identity-based) authentication factors [1].

1) Knowledge-based authentication (or “something you know”) uses a piece of information memorised by the client, e.g. a password. This type of authentication offers very strong authentication security, if the chosen passwords are random and long. However, memorising these long and random passwords has been shown very difficult for many users in practical applications. This has often led to very short and consequently simple to guess passwords. Additionally, passwords are often re-used, which makes cross-application attacks easier [2].

2) Object-based authentication (or “something you have”) relies on the physical ownership of an object (token), e.g. an ATM card or a passport. This type of authentication has the advantage over knowledge-based authentication that the client does not need to memorise any information and that the authentication information stored within the object can be as complex as required without negatively effecting the client. However, object-based authentication has two main disadvantages when it comes especially to remote authentication scenarios. First, if the token gets lost or stolen, the security of the system is entirely vanished. Second, and this aspect is mainly relevant in remote authentication scenarios, the remote authenticator cannot verify the actual possession of the token. Instead, he can only verify the transmitted authentication information stored originally on the token. However, this might have been illicitly copied in a previous attack, e.g. via a manipulated ATM machine [3].

3) Identity-based / Biometric authentication (or “something you are”) relies on the unique and individual behavioural (e.g. gait, voice) or physiological (e.g. fingerprint, face) characteristics of a person. Biometrics offer the advantages over the other two classical authentication factors that the client does not need to memorise a password or might lose the token. However, biometric samples can be collected and re-used to fool the biometric verification sensor, e.g. the genuine client’s face can be used by an offender from a previously taken image.

To enhance the security and reliability of remote, multi-factor authentication systems further, additional authentication factors like time and location were added to such systems [4]. Adding time information that is tightly bound to the other authentication factors eliminates the risk that genuine authentication data can be illicitly re-used at later stages by an attacker, e.g. the risk of replay attacks with intercepted client data is minimised. Integration of location information grounds the remote authentication attempt to a clearly and uniquely defined position on earth [5], thus eliminating the possibility that an attacker can claim to be at a location, s/he actually is not, i.e. distance attacks are minimised.

To use location information as an authentication factor, the authenticator must be able to verify the correctness and actuality of the client’s claimed location [6]. To achieve this, two general approaches can be distinguished:

1) The client collects location proofs from trusted sources and submits these location proofs [7] to the authenticator for verification once the client’s current location needs to be verified, i.e. the client proactively submits his location claim to the authenticator for verification.

2) The authenticator determines the actual client location via a second resource that is independent from the technology used by the client, i.e. the authenticator independently requests the client’s current location and does not rely on the location information provided by the client.

Examples of the former approach are systems like APPLAUS [8] or Data-Location-Time (DTL) – certificates [9]. These systems depend on the widespread of trusted proof issuers, e.g. WiFi-Access Points, with known locations. Here, the main idea is that the client is only able to collect such location proofs from the proof issuer, if in communication range of the proof issuers. However, these systems introduce various requirements and limitations, which need to be carefully addressed to avoid that the authentication system security is undermined. The number of trusted senders needs to be high enough as well as adequately distributed to guarantee the necessary precision of the location information. It must also be guaranteed that the trusted senders cannot be modified in such a way that they generate wrong location proofs. The issued location proofs also have to be protected against modification. Because these proofs are stored on the client's Smartphone, they are subject to potential manipulation if not protected. Finally, such systems need to guarantee that the issued location proofs cannot be passed on to another person or be re-used at a later time.

In the later approach, the claimed client location is verified via a second, completely independent source. For example, the LocBiometrics system [4] uses GPS on the client's Smartphone to determine the client's current position. This location information is then tightly coupled with further authentication factors, e.g. a password and client's biometrics, and afterwards sent via a wireless communication link to the authenticator. Upon receiving the authentication information, the authenticator requests the current client location from the Mobile Network Operator (MNO, i.e. the second source) serving the client's Smartphone at that moment in time. The authenticator then uses his stored client credentials together with the location information received from the MNO to authentication the client and its location. A clear advantage of this independent location verification is that the location proof will never be available to the client, and accordingly cannot be directly manipulated. Also, the already existing cellular network infrastructure can be used to determine the client's location, no installation and observation of further trusted senders is necessary.

2.2 LTE-Location Services (LTE-LS) Architecture

Figure 1 shows the LTE-Location Service (LTE-LS) architecture used by the external LTE-LS user (e.g. the Bank, step 1) to determine/request the current location of the client (i.e. the LTE-User, step 8). Once the bank requires the location of the Smartphone used in the transaction for verification (step 1), the bank sends an LTE-LS request (step 2) to the Gateway Mobile Location Centre (GMLC, step 3), which acts as the first contact point for external location requests. The GMLC then determines the identity of the Mobility Management Entity (MME) currently serving the client's Smartphone from the Home Subscriber Server (HSS, step 4) and forwards the LTE-LS request to the determined MME (step 5). The HSS acts here as a central database for mobility management, call and session establishment support, and holds also LTE-User related subscription information. The MME then deputes the task of calculating the actual Smartphone location to the Evolved Serving Mobile Location Centre (ESMLC, step 6), which will use the Secure User Plane Location (SUPL, cp. section 2.3) protocol (step 7) to establish the current position of the client's Smartphone using the Evolved Node B (eNodeB). The eNodeB is a basestation connected to the mobile phone network. It controls the Smartphones in one or more mobile network cells, and communicates directly with the client's Smartphone. Once the client's position is securely established, the determined position information is returned to the GMLC. Finally, an LTE-LS response is generated and communicated back to the bank (step 9).

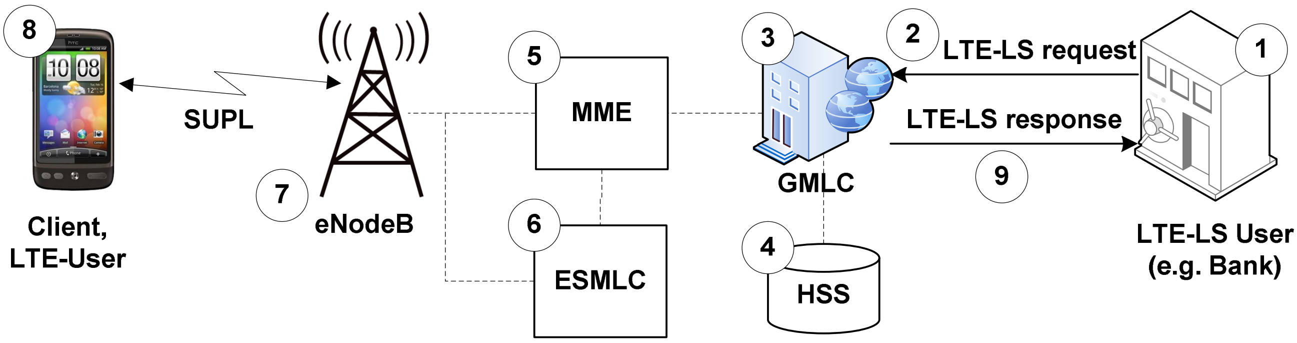

Figure 1: LTE Location Service Architecture (adopted from [10])

2.3 LTE Secure User Plane Location (SUPL) protocol

Since the initial FCC-E911 mandate, researchers have explored the use of a Secure User Plane Location (SUPL) protocol that is network technology (e.g. 2G-GSM or 3G-WCDMA) independent to carry the localisation information of any user and so enabling a solution for e911 and other Location Based Services (LBS). With the emergence of the LTE technology, since release 9, a SUPL has been included that will offer secure Smartphone based positioning based on one or more of the following four techniques:

1) Using Global Navigation Satellite System (GNSS, currently including GPS, Galileo & Glonass) where assistance-data (for GPS this data includes Almanac, ephemeris, time, error measurements that can help establish time and frequency) is supplied to the Smartphone's GNSS receiver(s) and associate position-fix is relayed back to any client via the ESMLC (Evolved Serving Mobile Location Centre, which also supply the assistance data). Accuracy of such fix can be within 10 meters.
2) Using Smartphone assisted positioning where the raw data from the on-board GNSS receivers are sent to the ESMLC to calculate the phone's position before passing it on to a client with an accuracy of 10meters
3) Using the serving towers/basestations to calculate the position of the Smartphone using the Observed Time Difference Of Arrival (OTDOA) technique. A special positioning sub-frames called "Positioning Reference Signals" has been included in release 9, to help accurately measure the time difference of arrival of neighbouring cells received signal, achieving accuracies to within 100meters
4) Using Enhanced cell-ID technique of measuring the distance between the Smartphone and the serving tower, based on the received signal round trip time (or the Angle of Arrival of the uplink signal) between the eNodeB and the Smartphone, and then calculating that the phone is within a circle of that distance radius.

Also, a new LTE Positioning Protocol (LPP) is available that will supports broadband, such as WiFi, based position techniques, too. LPP can therefore be used in the Control Plane (similar to RRC/RRLP in 2G/3G networks) or used in the User Plan enabled by SUPL. This makes LTE versatile in establishing the location of any user's Smartphone over any network via LPP on the Control Plane (commonly used by emergency services as only way in 2G/3G networks) and via SUPL with RRLP or LLP as used in the proposed location-based authentication scheme detailed in the following section 3.

3. LTE ENHANCED LOCATION-BASED MULTI-FACTOR AUTHENTICATION

3.1 Overview of the proposed scheme

The proposed LTE enhanced location-based multi-factor authentication scheme improves the security and reduces the overhead of authentication systems with independent location verification (e.g. LocBiometrics [4], cp. section 2.1) by integrating LTE-LS (cp. section 2.2) into the authentication process. Figure 2 shows how the GNSS-based (client side) and LTE-LS-based location information (authenticator side) is determined and combined with the further authentication factors (e.g. client's biometrics and PIN) during the authentication message generation as well as the verification process.

On the client side, the location-based, multi-factor authentication data is combined from freshly captured client biometrics, a client entered PIN as well as the current Smartphone location determined using the Smartphone's on-board GNSS receiver as detailed in [4]. On the authenticator side, this LTE enhanced authentication scheme requests the client's current location for independent verification via LTS-LS from the GMLC (cp. section 2.2). I.e. the MNO supplied LTE-LS location of the Smartphone, which is determined using the secured and unique to LTE Observed Time Difference Of Arrival (OTDOA) technique (cp. section 2.3), is compared to the GNSS (e.g. GPS) position obtained by the client's Smartphone.

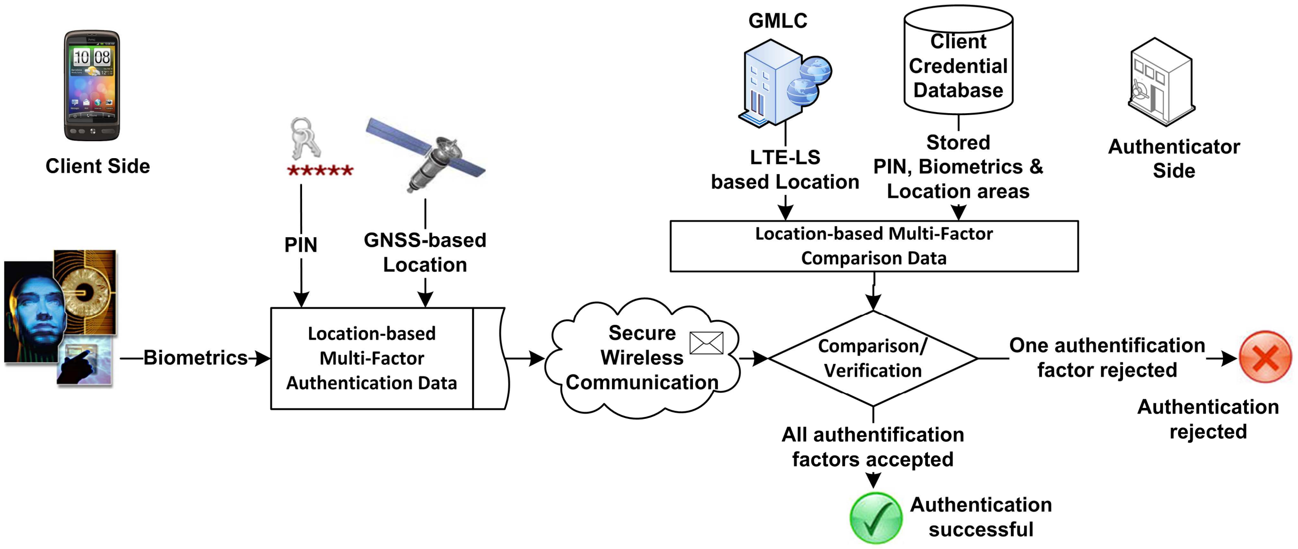
Client Side
PIN
GNSS-based Location
Biometrics
Location-based Multi-Factor Authentication Data
Secure Wireless Communication
GMLC
LTE-LS based Location
Client Credential Database
Stored PIN, Biometrics & Location areas
Authenticator Side
Location-based Multi-Factor Comparison Data
Comparison/ Verification
One authentification factor rejected
Authentication rejected
All authentification factors accepted
Authentication successful

Figure 2: Location-based, multi-factor authentication scheme

Figure 3 shows the verification process on the authenticator side in more detail. After the client provided authentication factors are extracted from the received authentication message (step 1), the provided location is compared to a set of pre-agreed areas, the client normally uses his/her Smartphone in (step 2). This optional step enables the authenticator in a quick and easy way to check if something unusual/suspicious is going on with this authentication attempt. Once this first check is successfully performed, the actual client location is requested by the authenticator via LTE-LS request (step 3). The received location information is verified (step 4). If the difference between the two locations is outside the pre-defined threshold, then the authentication attempt is rejected, otherwise the verification process continues. In the final verification step 6, the remaining client-based authentication factors (e.g. Biometrics and PIN) are compared to the stored client credentials retrieved from the corresponding database (step 5). Please note, that the client's credentials have been stored in the authenticator's database during an enrolment process executed prior to authentication. If the result of the verification process is also within a pre-defined threshold, then this scheme considers the client entire authentication data as genuine and the overall authentication attempt is successful. Otherwise, if one of the verification steps is not successful, then the entire authentication attempt is rejected.

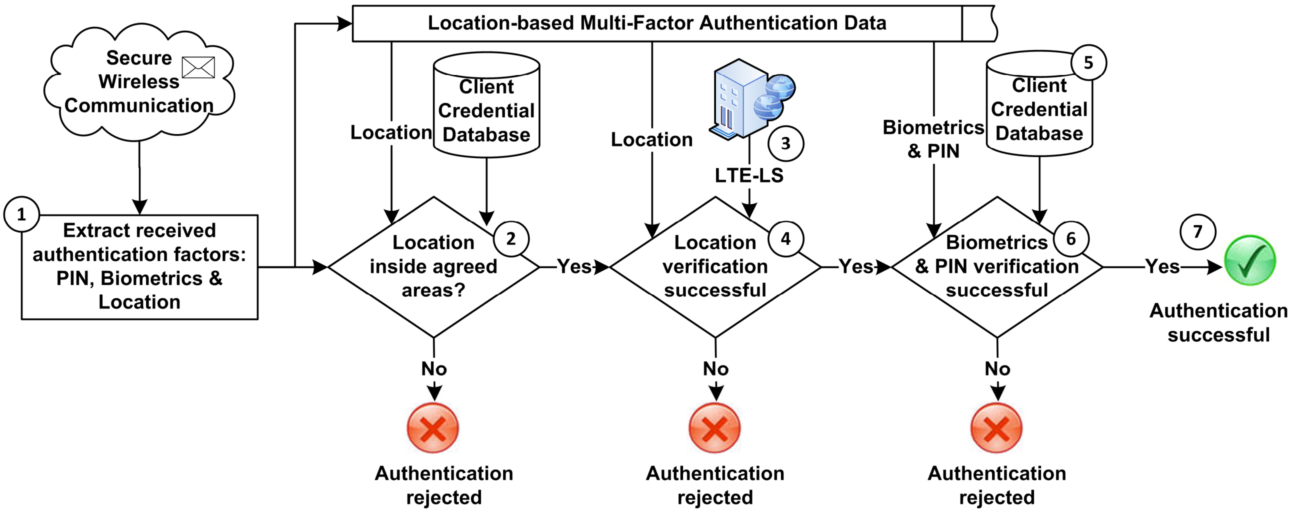
Location-based Multi-Factor Authentication Data
Secure Wireless Communication
1
Extract received authentication factors: PIN, Biometrics & Location
Location
Client Credential Database
2
Location inside agreed areas?
Yes
No
Authentication rejected
Location
3
LTE-LS
4
Location verification successful
Yes
No
Authentication rejected
Biometrics & PIN
5
Client Credential Database
6
Biometrics & PIN verification successful
Yes
No
Authentication rejected
7
Authentication successful

Figure 3: Verification process on authenticator side

3.2 Detailed LTE-LS location request procedure

Figure 4 details the steps executed by the MNO following an LTE-LS request from the authenticator (e.g. the bank) to establish the client's current location. This is done, once the supplied location-based multi-factor authentication data received from the Smartphone has been decoded (cp. step 1 in Figure 3) and the GNSS coordinates were recovered and checked to prove that the Smartphone is within the area supplied by the MNO OTDOA data (cp. step 2 in Figure 3). Now, the MNO is asked to supply the actual GNSS coordinate (step 1). The bank's request is passed on to the GMLC, which will retrieve the IMSI code of the Smartphone (step 2). Then the request is checked for validity and it is also validated if this client's privacy permissions allow determining his current location (step 3). This additional LTE-LS privacy feature can be used in combination with other privacy preserving authentication techniques, such as [11], to meet the privacy protecting aspects required in any remote authentication scheme. The GMLC will recover the ID of the serving MME from HSS (steps 4 and 5), using the basic Diameter (Diam) protocol [12], a standard IETF protocol for authentication, authorisation and accounting. In the following step 6, the GMLC forwards to location request directly to that MME to retrieve the location of the Smartphone.

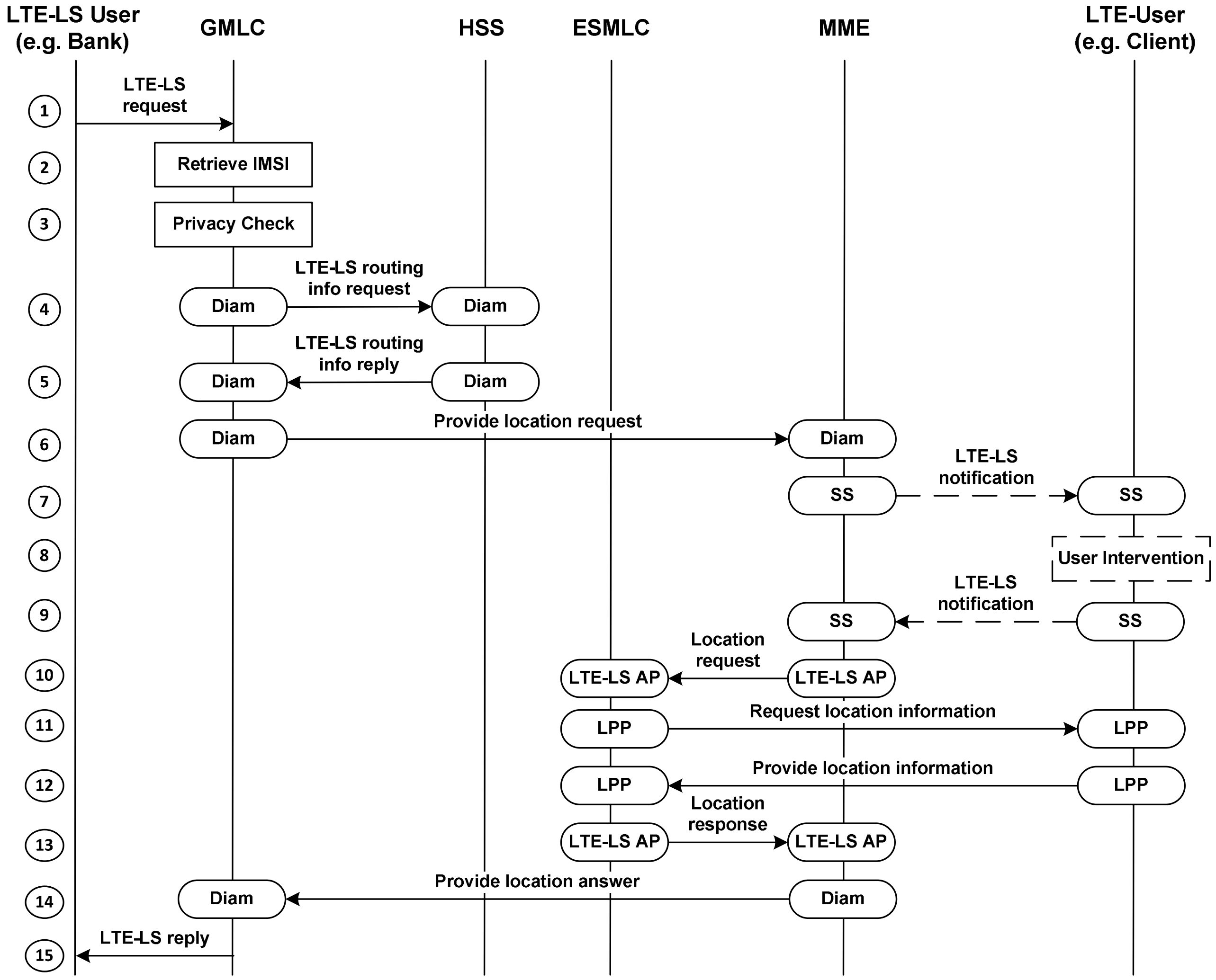

Figure 4: LTE-LS location request procedure (adopted from [13] and [10])

Before the actual location of the client’s Smartphone is determined, the MME can optionally ask the client for his/her permission (step 7) using the Supplementary Service (SS) protocol. If the client did not initiate the mCommerce authentication request in the first place, s/he can intervene at this point during the location determination process (step 8), and withhold his/her permission to continue the process (step 9). However, in the case that the initial authentication request was send from the client, permission will be granted and the MME will continue the process.

The MME forwards the location request to the ESMLC (step 10) using the LTE-LS Application Protocol (LTE-LS AP), which recovers the capabilities of the Smartphone from the information stored about the Smartphone in the ESMLC database. If the Smartphone has GNSS receivers on-board, then the GSMLC will provide aiding data (such as Almanac, Ephemeris, time, rough position and frequency for a GPS system) for these receivers’ technologies on-board the Smartphone and directly obtain the corresponding receiver’s coordinates. If instructed or the Smartphone has no GNSS receivers enabled on-board, then the ESMLC will use OTDOA, or enhanced-Cell-ID if the phone is in a remote location.

The LTE Positioning Protocol (LPP, cp. section 2.3) is used to exchange the actual determined location between the client’s Smartphone and the ESMLC in steps 11 and 12. Finally, the location is send via ESMLC (step 13), MME (step 14), and GMLC bank to the bank (i.e. the initial requester of the LTE-LS) in step 15.

4. CONCLUSION AND FUTURE WORK

Location has become an important authentication factor in remote authentication scenarios as for example required in financial transactions performed on Smartphones. Adding location information grounds the remote authentication attempt to a clearly specified position on earth, i.e. minimises the risk of distance attacks. To achieve the highest possible security and reliability of the location authentication factor within the authentication system, the location claimed by the client should be independently verified via a second source at the authenticator side.

The LTE-location service architecture provides a secure and trustworthy way to achieve these authentication requirements with minimal technical and time overhead. In addition, the privacy checks and user intervention stage integrated in the LTE-LS architecture can be efficiently used to address the high privacy demands of today’s authentication schemes. In tight combination with other authentication factors like PINs or biometrics as proposed in this paper, LTE verified location can be used to limit the fraud-attack possibilities and avoid certain distance attacks commonly existing in various identity theft scenarios with minimum overhead.

The work on using the new LTE-location services for secure authentication purposes is on-going. Currently, further schemes which combine the authentication factors with the LTE-LS provided location in a more robust ways are investigated. Also, the use of LTE-LS to securely and reliably generate location-based keys, for example to be used to protect mCommerce applications executed on Smartphones against illegitimate modification [14], are explored.

REFERENCES

[1] S.Z. Li and A.K. Jain, [Encyclopedia of Biometrics], Springer US (2009)

[2] D. Florencio and C. Herley, "Where do security policies come from?," Proc. Sixth Symposium on Usable Privacy and Security, New York, NY, USA, 10:1--10:14 (2010)

[3] Anneke Kosse, "Do newspaper articles on card fraud affect debit card usage?,” Journal of Banking & Finance, (2013)

[4] Ihsan A. Lami, Torben Kuseler, Hisham Al-Assam, and Sabah Jassim, "LocBiometrics: Mobile phone based multifactor biometric authentication with time and location assurance," Proc. 18th Telecommunications Forum IEEE TELFOR, (2010)

[5] D Denning and P MacDoran, "Location-Based Authentication: Grounding Cyperspace for Better Security," Computer Fraud and Security Bulletin, (1996)

[6] Torben Kuseler and Ihsan Alshahib Lami, "Using Geographical Location as an Authentication Factor to enhance mCommerce Applications on Smartphones," International Journal of Computer Science and Security (IJCSS) 6(4), 277-287 (2012)

[7] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," Proc. of the 10th workshop on Mobile Computing Systems and Applications, New York, NY, USA, 3:1--3:6 (2009)

[8] Z. Zhu and G. Cao, "Applaus: A privacy-preserving location proof updating system for location-based services," Proc. IEEE INFOCOM, 1889-1897 (2011)

[9] V. Lenders, E. Koukoumidis, P. Zhang, and M. Martonosi, "Location-based trust for mobile user-generated content: applications, challenges and implementations," Proc. of the 9th workshop on Mobile computing systems and applications, 60-64 (2008)

[10] Christopher Cox, [An introduction to LTE: LTE, LTE-advanced, SAE and 4G mobile communications], John Wiley & Sons, (2012)

[11] Torben Kuseler, Hisham Al-Assam, Sabah Jassim, and Ihsan A. Lami, "Privacy preserving, real-time and location secured biometrics for mCommerce authentication," Proc. SPIE 8063, Mobile Multimedia/Image Processing, Security, and Applications 2011, Bellingham, WA, (2011)

[12] IETF RFC 3588, Diameter Base Protocol, Internet Engineering Task Force, (2003)

[13] 3GPP TS 24.171, Functional stage 2 description of Location Services (LCS), 3rd Generation Partnership Project, (Dec 2012)

[14] Torben Kuseler and Ihsan Alshahib Lami, "dLocAuth: a dynamic multifactor authentication scheme for mCommerce applications using independent location-based obfuscation," Proc. SPIE 8406, Mobile Multimedia/Image Processing, Security, and Applications 2012, Bellingham, WA, 840605 (2012)