Authentication Considerations for Mobile e-health Applications

John A. MacDonald
Information Security Group
Royal Holloway, University of London,
Egham, England TW20 0EX
john@madgo.com

***Abstract*—This paper identifies serious user privacy concerns with the 3GPP Generic Bootstrapping Architecture protocol when used as the basis for security for certain e-health applications.A possible alternative approach avoiding these concerns is also outlined.**

I. Introduction

Marti et al. describe [17] e-health services that incorporate the use of mobile technologies to communicate with a Body Area Network (BAN) comprising diagnostic sensors and treatment dispensing actuators. Security attacks on any e-health system could have serious consequences not only to the patient's privacy but quite possibly also to their survival prospects. If, in the interest of cost economies and ease of introduction, the mobile component of an e-health system is to utilise standard, commercially available and perhaps pre-issued mobile devices (indeed ideally the patient's own device), then it is necessary to subject the security standards of mobile technology to critical analysis. Only if these standards satisfy the application's security and privacy requirements should they be adopted as the basis for securing a mobile e-health service.

Securing identity is fundamental for e-health applications. This paper investigates the choice of authenticated key agreement (AKA) protocol to be deployed for mutual authentication in such situations. Section 2 overviews the Generic Authentication Architecture (GAA) [4] standard as a basis for mutual authentication, whilst section 3 identifies how the derived security credentials could be incorporated within a typical mobile e-health system. Section 4 identifies potential weaknesses in the GAA standard, whilst section 5 identifies an alternative approach. Finally, Section 6 summarises how the derived session keys from either GAA or the proposed alternative AKA may be incorporated into the various options for an application layer protocol of an e-health service.

II. GAA, GBA & GBA_U

The Third Generation Partnership Project (3GPP) has proposed the GAA [4] framework for mutual authentication of users and network applications in third generation mobile networks. In application scenarios, such as mobile e-health, where end users are remote from the application provider, preloading the user equipment with a (public, private) key pair and certificate may not be practical. In this scenario, irrespective of whether the final application protocol uses a public key infrastructure or not, the relevant GAA mutual authentication proposal that requires critical analysis for suitability in mobile e-health applications is GBA [2].

GBA uses the 3GPP network authentication algorithm [1] to create a shared GAA master session key K_S and transaction identifier (B-TID) between a user equipment and an external application server, building on the existing keying relationship between the mobile operator and the user equipment. In the 3GPP mobile architecture, security and trust reside in two locations: the Home Subscriber System (HSS) and the Operator issued tamper resistant USIM card. The GBA process for mutual authentication [13] may be summarised by referring to the reference model of figure 1 where the User Equipment (UE) is presented as comprising two elements: mobile equipment (ME) and a tamper resistant USIM card. The GBA procedure calls for the Bootstrapping Server Function (BSF), a Network element under the control of the Mobile Operator, to fetch 3G AKA authentication vectors from the HSS over reference point Zh. Reference point Ub provides Mutual authentication between the User Equipment (UE) and the BSF by execution of the cellular authentication procedure in accordance with [1], performing predefined cryptographic processing on the authentication vectors using the shared cellular secret contained in the USIM card. From this cellular authentication process, the BSF and the GBA Boostrapping client in the UE derive GAA credentials that are made available to secure a connection between a Network Application Function (NAF) server and its corresponding UE application client over reference point Ua. In general the NAF and the UE application client need not be under the control of the Mobile Operator.

A UE consists of two elements: a mobile equipment (ME) and a tamper resistant USIM card. The GBA standard identifies two implementation options, termed GBA_ME and GBA_U, depending on where the GBA procedure is conducted within the UE.

GBA_ME requires only that the ME is compliant with the GBA standard; i.e. the GBA procedure is conducted wholly within the ME. In this scenario the derived GAA security credentials which include the master session key K_S and (B-TID), are determined by the GBA Bootstrapping Client of the

ME. The ME GBA Boostrapping Client provides a derived session key $K_S\_ext\_NAF$ to the UE application client, which is then used to secure the subsequent exchange between application server and client. In situations where the ME user device is considered potentially hostile by the application provider then GBA_U is the preferred implementation.

GBA_U requires that both the ME and the USIM card are compliant with the GBA standard, i.e. that both ME and USIM are GBA aware. This scheme uses the GBA Boostrapping Client resident on the tamper resistant USIM card to determine and store the GAA master session key K_S and related security credentials. GBA_U ensures that both the shared secret K_S and the derived session key $K_S\_int\_NAF$ remain in the USIM, exposing only the $K_S\_ext\_NAF$ to the application client in the ME.

III. GBA_U IN E-HEALTH APPLICATIONS

As shown in Figure 1, the e-health application is assumed to consist of a centralised application server interacting with application clients resident on UEs distributed to remote end users. The UE application client manages a BAN containing diagnostic sensors and treatment dispensing actuators. The GBA_U process for this scheme may be summarised as follows:

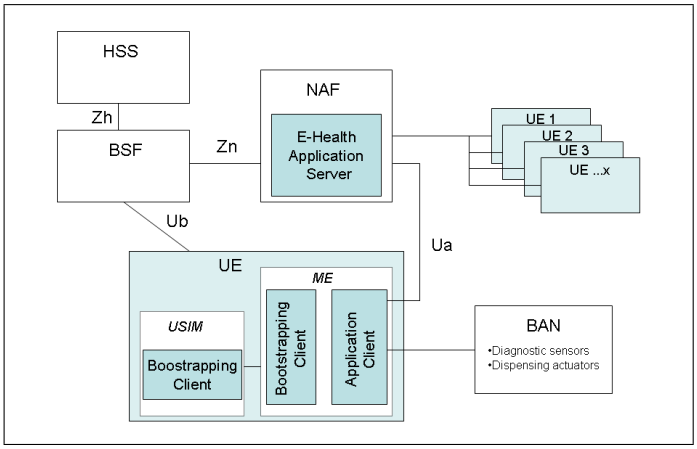

Fig. 1. Scheme Description

1) The e-health application, either in response to an external event or on execution of a scheduled treatment routine, will initiate the bootstrapping procedure. This may be launched either by the cenralised NAF application or by the UE application client.
2) The BSF fetches 3G AKA authentication vectors from the HSS via reference point Zh.
3) Reference point Ub provides mutual authentication between the UE and the BSF.
4) The USIM GBA Boostrapping Client calculates K_s and provides the GBA Boostrapping Client on the ME with the application security credentials ($K_s\_ext\_NAF$). The key K_s always remains in the USIM.
5) The corresponding security credentials are calculated in the BSF and communicated via Zn to the NAF.
6) The GBA Bootstrapping Client on the ME provides the security credentials, including ($K_s\_ext\_NAF$), to the UE application client.
7) The application client makes contact with the NAF via reference point Ua, using the now shared service credentials for authentication, confidentiality and integrity security services, as required by the application.

This simple model can be extended to incorporate the mobile end point within a Service Orientated Architecture (SOA) using web service technologies, by adopting the combined Liberty & 3GPP GAA model, as defined in [5]. In this specific case the identity of the end user within the web services environment is provided by a co-located Liberty Identity Provider IdP and NAF [14].

Adopting the GBA process allows e-health service providers to deliver identity consuming web services direct to the End User, without securely provisioning the initial credentials – a costly, time consuming and inconvenient process for end users. GBA is therefore a standardised technique that allows application providers to reuse the already widely deployed mobile credentials [13].

IV. POTENTIAL CONCERNS WITH GBA

There are a number of concerns which arise when applying the 3GPP GBA protocols to privacy and cost sensitive applications such as e-health. These concerns fall into the category of security/privacy and deployment. The primary security and privacy concerns are:

1) The mobile operator must be considered as a trusted third party. The derived GAA credentials used to secure the application are always known to the mobile operator's BSF. Indeed it is possible for the mobile operator to relate the specific application session key to the users MSISDN.
2) Both GBA_ME and GBA_U require a GBA Bootstrapping Client within the ME for operation. This client is a native software object within the ME; it is neither implemented by, nor under the control of, the application provider. The ME has total access to the derived GAA credentials when GBA_ME is implemented.
3) Although with GBA_U the master session key K_s remains within the tamper resistant USIM card, the derived session key $K_S\_ext\_NAF$ is nevertheless provided to the GBA Boostrapping Client of the ME, introducing a potential, albeit reduced, risk of attack.

GBA is a new standard; as such adopting GBA may introduce the following constraints when deploying an application:

1) GBA mandates that the ME must support both GBA_ME and GBA_U, whilst GBA_U requires that the USIM is also GBA aware. Any application wishing to deploy GBA, must ensure that all UEs are compliant.
2) The BSF is a network operator service. Any application wishing to deploy GBA must ensure that all participating mobile operators implement a compliant BSF service.

Deploying GBA requires the application provider to accept the above risks and constraints arising from GBA's dependency

on both the mobile operator and the UE vendor. Requiring the application provider to trust the operating procedures of participating mobile operators to perform the role of trusted third party is a potentially major issue. Similarly, GBA requires the application provider to trust the GBA implementation on the ME, and its ability to resist attack. The ME is unlikely to be tamper resistant, and the ME GBA Bootstrapping Client may not be implemented in a manner to resist fraudulent manipulation. MEs are rarely trusted to hold components and functions that protect valuable assets. This lack of trust is likely to increase as devices move from traditionally closed proprietary operating systems to more open operating systems capable of performing the file manipulation required by advanced 3G services.

Healthcare institutions may consider these risks and constraints to be unacceptable.

V. A possible alternative to GBA

Any alternative should aim to reduce the security risk by eliminating the mobile operator as a trusted third party and the dependency on the ME's native GBA Boostrapping Client. To ease deployment constraints, any alternative to GBA should build on existing, well proven and widely available mobile technology, and be under the end to end control of the application provider.

It would appear possible to design an AKA scheme that satisfies these requirements by building on the dual capabilities of SMS Security [6] and USIM Application Toolkit (SAT) [10]. The former can be used to provide end to end security services for an SMS message sent to or from the USIM, card whilst the SAT API allows a USIM card application to communicate with the connected ME. In recent years Java enabled devices have also become increasingly popular. The ME typically provides a J2ME java runtime environment [18] complemented by additional classes from the Mobile Information Device Profile 2.0 specification [11]. Java applications that run on MIDP compliant ME's are known as MIDlets. The USIM [7] are Java Cards where the USIM application [8] is just one of the possible java applications [9]. Java applications that run on Java Cards are known as Applets.

The putative AKA scheme is assumed to implement a *Security Agent* function — an example of which is presented in [16]. The client application comprises a device executed MIDlet application for I/O and computationally intensive operations, together with a USIM Applet for secure storage and cryptographic processing. The MIDlet has the appropriate permissions to incorporate the SATSA-APDU and SATSA-PKI [12] packages, enabling the application client access to the tamper resistant USIM card using APDU communication, and providing support for digital signatures and credential management. Unlike GBA, the master key K_S is not bootstrapped from the mobile operator's cellular credentials, but securely copied from the application provider server to the USIM using the TS03.48 mechanisms to provide end to end security. The AKA scheme, under the complete control of the application provider, resides in java application space of the UE and uses the shared secret K_S to generate session security credentials. A full description of such an AKA protocol, and an approach to enable over-the-air deployment to pre-issued, but not pre-programmed, mobile stations, is being developed.

VI. Application layer protocol options

Both GBA_U and the proposed alternative scheme result in the master key K_S being shared between the e-health server and the USIM. Secondary keys are provided to the ME, for use in securing an appropriate application protocol that transfers BAN information between the application client and e-health Server. The AKA protocol, whether it is GBA or the proposed alternative, provides the shared secret necessary to secure the channel, either through the use of MACs and symmetric encryption, or by authenticating a certificate enrolment request and thereafter securely issuing a certificate and key pair [3], when the non-repudiation security service or creation of a http over TLS tunnel is required.

In many application scenarios, simply securing the channel is insufficient; it is also desireable to secure the message itself. In this way the message protects itself, and is secure even when it is at rest, irrespective of the route it has taken between source and destination. Message based security and the adoption of a service orientated architecture is particularly suited to the e-health scenario where there are multiple providers of healthcare services [19] registered with the e-health provider. Adoption of web service technologies require information to be moved around the network as structured XML messages. The application layer protocol and design of tokens to secure these web service based XML messages could be application-specific [15] to minimise the load on scarce mobile resources; alternatively they could adopt a standards based approach [14] to optimise interoperability and software reuse.

VII. Conclusion

This paper has identified concerns with the GBA architecture for bootstrapping credentials necessary to secure e-health applications. It outlines an alternative approach, and indicates how derived session keys may be incorporated into the application layer of an mobile e-health service.

Acknowledgment

This work was supported by sponsorship funding from Telefonica Móviles, España. The author wishes to thank the Information Security Group at Royal Holloway, University of London for their continued financial and academic support during the course of these studies.

References

[1] 3G security; security architecture. Technical report, ETSI European Telecommunications Standards Institution, Septemper 2005.

[2] Generic bootstrapping architecture. Technical report, ETSI European Telecommunications Standards Institution, June 2005. UMTS, Generic Authentication Architecture.

[3] Support for subsriber certificates. Technical report, ETSI European Telecommunications Standards Institution, June 2005. UMTS, Generic Authentication Architecture.

[4] System description. Technical report, ETSI European Telecommunications Standards Institution, March 2005. UMTS, Generic Authentication Architecture.

[5] Interworking of Liberty Alliance ID-FF, ID-WSF and Generic Authentication Architecture. Technical report, 3GPP 3rd Generation Partnership Project, July 2007. 3GPP TR 33.980; Technical Specification Group Services and System Aspect, Release 4.

[6] 3GPP TS 03.48. *Technical Specification Group Terminals; Security Mechanisms for the SIM application toolkit; stage 2*. http://www.3gpp.org, 2001.

[7] 3GPP TS 31.101. *Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics*. http://www.3gpp.org, 2003.

[8] 3GPP TS 31.102. *Technical Specification Group Terminals; Characteristics of the USIM application*. http://www.3gpp.org, 2003.

[9] ETSI TS 101 476. *Digital cellular telecommunication system (Phase 2+); Subscriber Identity Module Application Programming Interface (SIM API); SIM API for Java Card; Stage 2 (GSM 03.19)*. ETSI, http://www.etsi.org, 2000.

[10] GSM 11.14. *Digital cellular telecomunnications system (Phase2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface*. ETSI, http://www.etsi.org, 2001.

[11] JSR-118 JCP. *Mobile Information Device Profile, v2.0 (JSR-118)*. Sun Microsystems, http://java.sun.com, 2002.

[12] JSR-177 JCP. *Security & Trust Services API (SATSA) (JSR-177)*. Sun Microsystems, http://java.sun.com, 2004.

[13] P. Laitinen, P. Ginzboorg, N. Asokan, S. Holtmanns, and V. Niemi. Extending cellular authentication as a service. In *1st IEEE Conference on Commercialising Technology and Inovation, 2005*, pages 1–7. IEEE, 2005.

[14] John A. MacDonald, Kalid Elmufti, Dasun Weerasinghe, M. Rajarajan, Veselin Rakocevic, and Sanowar Khan. A web services shopping mall for mobile users. In *4th IEEE European Conference on Web Services*, pages 99–108, Los Alamitos, CA, USA, 2006. IEEE Computer Society.

[15] John A. MacDonald and Chris J. Mitchell. Using the GSM/UMTS SIM to secure web services. In *2nd IEEE International Workshop on Mobile Commerce & Services (WMCS 2005)*. IEEE Computer Society Press, 2005.

[16] John A. MacDonald, William G. Sirett, and Chris J. Mitchell. Overcoming channel bandwidth constraints in secure SIM applications. In *Security and Privacy in the Age of Ubiquitous Computing*. Springer Science and Business Media, 2005.

[17] R. Marti, J. Delgado, and X. Perramon. Security specification and implementation for mobile e-health services. In *EEE'04: Conference on e-technology, e-Commerce and e-Service*, pages 241–248. IEEE, 2004.

[18] K. Topley. *J2ME In a Nutshell*. O'Reilly, 2002.

[19] Dasun Weerasinghe, Kalid Elmufti, M. Rajarajan, and Veselin Rakocevic. XML security based access control for healthjcare information in mobile environment. In *Pervasive Health Conference and Workshops, 2006*, pages 1–6. IEEE, 2006.