Novel framework for secure mobile financial services

Muttukrishnan Rajarajan
City University London, London, United Kingdom., r.muttukrishnan@city.ac.uk

Novel framework for secure mobile financial services

Dasun Weerasinghe[1], Fei Li[1], Ali Khayam[2] and Muttukrishnan Rajarajan[1]
Information Security Group
School of Engineering and Mathematical Sciences
City University London, Northampton Square,
London, EC1V 0HB, UK.
r.muttukrishnan@city.ac.uk

Abstract: The financial sector is always looking for new services delivery platforms to improve customer confidence and satisfaction. To achieve this, the banking service delivery platform must provide end-to-end security to safeguard the financial information exchanged between the bank and the customer. Today a number of banks offer mobile banking service to their customers. However, still banks have been adopting the generic user authentication systems that were developed for the desktop environment based on two-factor authentication with a number of user intrusive activities. This paper presents a novel authentication and authorization framework for secure mobile banking applications based on the user SIM and mobile credentials.

Keywords: Mobile banking, Parameter based access control, Mobile data security

1 Introduction

The wide penetrations of mobile phone usage and the availability of more powerful mobile handsets and network bandwidth have made mobile devices an attractive candidate for value added services. Today mobile users can carry out basic banking transactions such as transfer money, check balances or pay a bill or statement. Mobile banking services will be a value added service for mobile users due to the fact that the users can carry out banking from anywhere anytime at their convenience. It also gives the opportunity for people who do not have broadband connectivity to carry out mobile banking. According to the Juniper Research, by the end of 2011 more than 150 million subscribers worldwide will have used mobile banking services and this represents a growth of more than three fold since 2008 [1].

However, security is one of the main areas of concern when introducing banking services in mobile devices. During the recent past there has been a number of mobile banking solutions emerged in the market place that are complex and hence have slowed the adoption. This paper will review the existing mobile banking solutions and propose a novel security framework that will provide increased security and usability features.

The mobile banking association has recently highlighted the following main security issues that should be addressed in order to encourage the adoption of mobile banking [2].

(1) **Data transmission must be secured:** for the confidentiality, the connection between the bank and the device should be encrypted.
(2) **Application and data access must be controlled:** before users can receive any sensitive information related to their bank accounts, a certain degree of verification must be completed.
(3) **Data integrity must be provided:** Any critical data to the mobile phone must be protected against unauthorized modification.
(4) **Loss of device must have limited impact:** The mobile banking service should be designed so that there□s limited impact when customers lose their mobile phones.

2 Mobile Banking

Mobile banking is a term used for performing online banking services such as money transactions, view account balance, etc using a mobile device such as a mobile phone. Mobile banking today is most often performed using Short Message Service (SMS) communication or the Mobile Internet but can also use special programs called mobile applications downloaded onto the mobile device. We did a comparative study on security features in different banking applications in UK, USA and Asia. We have identified three main techniques in mobile banking and security features associated with each technique.

SMS Banking: The short message services in the mobile network are used to communicate between the mobile user and the bank. This is one of the most popular techniques and SMS banking offers features like check account balance, do micro payments and view mini statements. The user is registered with the bank using the mobile phone number and a password or PIN and those parameters are used to authenticate the user. The bank provides a set of SMS codes for different banking functions (e.g. „bank_balance□ to enquire the bank balance) or user has to send messages to different destination numbers for different services. Memorizing different SMS codes for different banking functions is cumbersome to the mobile users and there is no nationally or internationally accepted standard code of practice available to-date.

WAP-GPRS: Wireless application protocol (WAP) browser provides all the basic services of a web browser but simplified for a mobile phone. WAP banking in other terms is mobile Internet banking such as mobile user□s access banking websites designed to be accessed from mobile phones. This mobile banking would require all or a part of the authentication credentials used in Internet banking. Mostly, the users have to enter the username, password and account number. The extra security is added by some banks with introducing a One Time Password service. The bank issues a password that is valid for just single login or single transaction. So every time when user makes a new transaction the One Time Password is sent through SMS to the mobile phone. The user has to enter the password in the WAP site to authenticate.

However, entering all the security parameters using a mobile phone with restricted key pad (e.g. most of the mobile phones represent 4 letters by a single key in the key pad.) is not a user-friendly authentication method in mobile banking.

Mobile Application based Banking: Most banks are in the process of adopting this technology. The banking application is downloaded to the mobile device and then user is authenticated using username and password technique and the mobile number is used for the user identification in some of the existing applications. However, still the user entered password is required by the bank for the user authentication. This password is recommended to be strong characters to prevent security attacks. Meanwhile, Interactive Voice Response (IVR) calls are implemented in the mobile banking platform by some of the banks to improve the security features.

The Bank of America provides the mobile banking to their customers and it has three levels of security such as Online ID is entered by the user (Online ID is considered as a secure information), the site key is sent by the bank to the mobile device and it is identified by the mobile user and finally password is entered by the user. Barclays bank in the United Kingdom provides a WAP based mobile banking platform and users have to enter the complete login details such as username, membership number, passcode and memorable name from the mobile device. The HSBC and NatWest banks in the UK provide mobile application based banking services. The application is installed onto the mobile device and security is established using the phone number and the password. The HDFC bank in India provides WAP and SMS based mobile banking services. However, they do not provide more sensitive functions such as money transactions and the security is implemented using a user PIN.

Most of the mobile banking services inherit user authentication using one or more combinations of username, password, PIN, phone number and IVR calls [3]. Meanwhile, an extra PIN or password based authentication is required to authorize money transactions in mobile banking. However, according to the article [4], the number of user inputs to the mobile application using the mobile key pad should be minimized since it should be convenient for users to operate while on the move. Clarke and Furnell [5] presented security weaknesses in PIN and other user intrusive authentication systems in mobile devices. They highlighted the importance of non-user intrusive authentication methods for sensitive service access at mobile devices.

Merita Bank in Finland did a case study in mobile banking and they used the WAP technology with the username and password based authentication. The final outcome of the report was to setup a public key infrastructure in the mobile device to authenticate the mobile users to the banking services [3]. Horn G. *et al*. [6] evaluated the design of public key based protocols suitable for applications in 3G mobile systems. The protocols were considered for the authentication of a mobile user to value-added financial services. However, special Wireless Identity Module technology (WIM) is required in the mobile device or in the smart card to store long term secret keys in a mobile device [7]. Meanwhile, Dodis *et al.* [8] highlighted threats to cryptography when installing a private key in a device and especially when a user carries the mobile device which allows remote access from public or foreign domains. They recommended having a key as an output from a combination of different types of physical and logical cryptographic inputs.

The researches have investigated the use of mobile operator issued SIM card as an authentication unit for mobile banking. The SIM card is used by the mobile operator to identify the subscriber but the same SIM card was used for mobile banking by Radiomobil (today TMobile Czech) together with several Czech banks. These mobile SIM cards were specifically developed since then for mobile banking. Besides the GSM credentials they contained a collection of credentials (access keys) for mobile banking [9]. This security approach is not presently used due to the complexity of key management. CamWebSIM [10] is the platform for a variety of identification and security solutions. It is based on Windows for SmartCard and its integrated SIM functionality is combined with a small HTTP server on the card. By making the SIM accessible over HTTP, the phone and the SIM becomes a personal security server on the Internet. Meanwhile as specified in [11], the SIM can be used to generate a secure verifiable electronic consent of the mobile user using the electronic signature on SIM-created credentials that may contain information about time, intent and recipient.

The security framework proposed in this paper uses the SIM based authentication at the mobile operator to authenticate the mobile users to the mobile banking services. Then identity and attribute (parameter) based key generation functionality is proposed to authorize more sensitive banking services at the mobile device. The combination of SIM authentication and parameter based authorization generates a simple security framework for mobile banking.

3 Architecture

The mobile service environment has three main actors such as the consumer, mobile operator and the bank. The consumer is the mobile user with a mobile device and the mobile device has a SIM card connected to a mobile network. The proposed security framework allows mobile users to use the SIM based authentication mechanisms at the bank to access the mobile banking services. The authentication functionality is based on Federated Identity Management (FIM) technologies with the standard 3G authentication techniques [12] at the mobile operator. The FIM is an extended version of the Single-Sign-On (SSO) technique and it enables a single authentication system to be shared across multiple trust domains. The mobile operator and the bank are in two trust domains but the user authentication is linked using the FIM technology. This proposed environment is implemented based on the guidelines of Liberty Identity Federation Framework (ID-FF) [13]. The mobile users and the bank are connected to the mobile operator to access the outsourced SIM based credentials for authentication in the proposed model as shown in Figure 1.

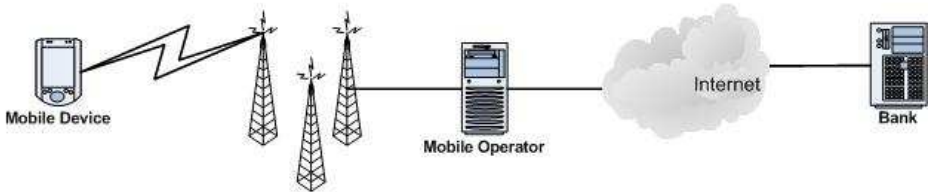

Figure 1: Mobile Banking Environment

The implementation of security framework for mobile banking is based on Web service architecture such as;

- The mobile device has an over-the-air installed application that uses the SIM card as one of its security elements. This application is named as the ***Security Capsule***.
- The banking services content is provided by the services provider in accordance with the Web services standard over the SOAP messaging.
- The mobile operator provides the authentication service using the Generic Bootstrapping Architecture (GBA) architecture of Generic Authentication Architecture (GAA) as specified by the 3GPP specification [12], and the bank establishes a trust relationship with the mobile operator and implements the Federated Identity Management technology.

The banking services are available to mobile users from the bank and the service must be capable of being set-up using over-the-air techniques. The actors interface to the system using the standard and the internationally agreed protocols such as SOAP and HTTP over the Internet or mobile network.

The Security Capsule is a mobile application and it establishes the mobile device communication with the bank. The bank uniquely identifies the mobile device for authentication and authorization before the service delivery and the bank issued security tokens to the Security Capsule to confirm the valid authentication and authorization activities at the mobile device. The unique identity is derived in the Security Capsule using the logical and physical identity parameters at the mobile device. Meanwhile, the Security Capsule maintains the key credentials for the authentication at the mobile operator and the bank. The unique identity and key credentials are used to present the final user authorization to access services. The user authorization is performed by generating a cryptographic key with different input parameters. Meanwhile, the Security Capsule utilizes and verifies the security tokens and secure messages during the registration and authentication with the bank.

The novel key generation process at the Security Capsule enables a new way of mobile banking framework without consuming number of user inputs for the security validation. The Security Capsule uses the physical and logical identities and key credentials at the mobile device as inputs. Therefore, the key generation process automatically guarantees and verifies the mobile user identity and authentication to access banking services. The cryptographic key will not be generated unless relevant identities are presented else the authentication is unsuccessful. The following are the necessary credentials and identity parameters for the key generation process.

- IMPI (IP Multimedia Private Identity): The mobile operator assigned identity for the mobile user. This identity is stored in the USIM of the mobile device.
- IMEI (International Mobile Equipment Identity): The unique identity of the mobile device and this is issued by the mobile device manufacturer.
- UID: The identity provider issued unique identity for the security capsule. The UID is inserted into the source code of the Security Capsule and it can□t be retrieved by external parties. The UID is an alphanumeric value in the security capsule and it is un-accessible to the device users.

- Token Key: This cryptographic key is issued by the bank as a result of successful mobile user authentication and authorization.

The key generation using the above functions will enable SIM dependent, mobile device dependent, mobile user dependent and bank authentication dependent data access property at the mobile device.

4 Security Protocol Design

The bank has the main role in the security framework such as registering, identifying, authenticating and authorizing mobile users to the banking services. The mobile user's SIM deployed in mobile device with the Security Capsule acts as an authentication authority to the bank. The identification and authentication information about the mobile user are exchanged from the mobile operator to the bank.

Figure 2 presents the main communication links between the bank, mobile operator and mobile user and our mobile banking framework consists of 3 main stages such as:

Registration: a mobile user registers with the bank for mobile banking services. The mobile user downloads the security capsule and then shares some secret credential information with the bank for the authentication. The mobile user registers for the mobile banking services by downloading the Security Capsule from the bank. The Security Capsule is downloaded and installed to the mobile device using over-the-air technique of the mobile network. It contains a unique identification number (UID) and it is used to identify the mobile user at the identity provider. The security capsule sends a registration acknowledgement to the bank after the successful installation. The registration acknowledgement consists of the UID and identification parameters at the mobile handset.

Authentication: the mobile user authenticates with the bank to access services on the bank account. The secret credentials are exchanged and parties are mutually authenticated with each other. The mobile device uses the Bootstrapping Server Function at the mobile operator to create the application layer credentials. The generation of the application layer credentials is presented by the messages (1) and (2) in Figure 2. The B-TID is a mobile operator generated reference to the application layer credentials. These credentials are then shared with the bank according to the GBA of GAA [35]. The messages (3) and (4) in Figure 2 are referred to the GAA function between the mobile operator and the bank. The knowledge of the shared secret mutually authenticates the mobile user and the bank to the mobile banking framework as shown in messages (5) and (6) in Figure 2. The bank uses its public key certificate to authenticate with the mobile user and Security Capsule generated shared key is used for the secure communication after the authentication.

Authorization: this is an extended security feature in mobile banking and bank would use the authorization before any financially valuable transactions. For an example, activities such as money transfer from account, setting up direct debit,

change personal information, etc. These activities have to be authorized with special credentials compared to the authentication.

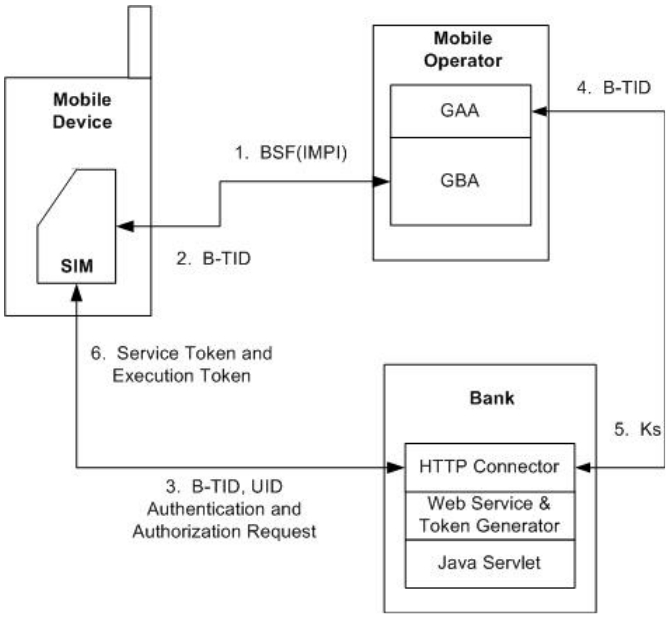

Figure 2: Communication links

The detailed description of the security protocol in the banking framework is presented in the below sub sections.

4.1 Registration

The mobile user downloads the security capsule to the mobile device for mobile banking services. The capsule can be downloaded either by visiting the WAP web site of the bank using a WAP browser in the mobile device or by clicking on the Security Capsule download link sent as a text message. The Security Capsule is downloaded using over-the-air or wired techniques. The following are the main steps in the registration process and the steps are presented in Figure 3.

(1) The mobile device requests to download security capsule. (2) The security capsule is downloaded onto the mobile device.

(3) The mobile user verifies the authentication of the bank and the integrity of the downloaded Security Capsule using the following steps. These steps are carried out prior to the Security Capsule installation process.

- The public key certificate of the bank is used to authenticate the bank.
- The calculated hash value of the Security Capsule binary installation is compared with the hash value at the bank for the security capsule

integrity. The hash value is signed using the bank's private key to present the authentication.

(4) The Security Capsule is installed into the mobile device as a mobile application. The downloaded Security Capsule is uniquely identified using the UID. The UID is used to present the Security Capsule identification to the bank during the future communications.

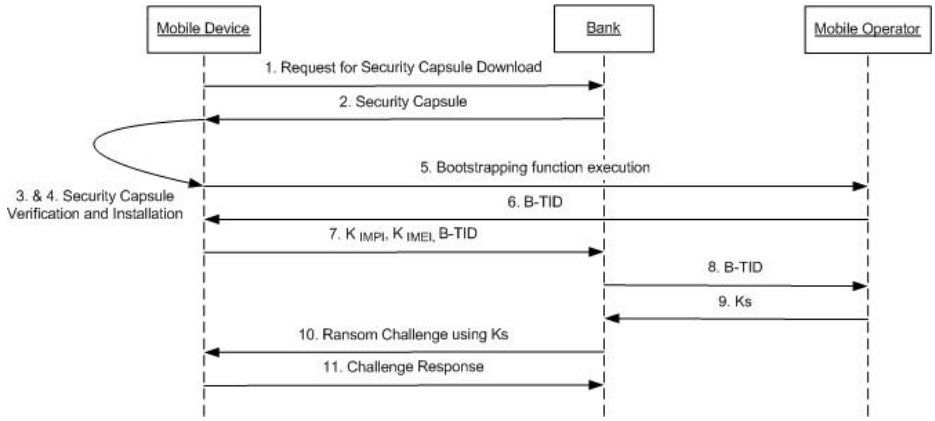

Figure 3: Registration Process

(5) The Security Capsule executes the bootstrapping function at the mobile operator.

(6) The execution of Bootstrapping function will generate a new shared secret key (Ks) between the mobile device and the mobile operator. The Ks is generated in the device and mobile operator sends the B-TID as a reference to the shared secret key (Ks).

(7) The Security Capsule accesses the IMPI and IMEI values from the mobile device and it generates the K_{IMPI} and K_{IMEI} using an inbuilt hash function.

$$HASH (IMPI) = K_{IMPI}$$
$$HASH (IMEI) = K_{IMEI}$$

B-TID, K_{IMPI} and K_{IMEI} are transmitted to the bank by encrypting them using the bank's public key.

(8) The bank sends the B-TID to the mobile operator and requests the shared secret key (Ks).

(9) The mobile operator sends the shared secret key (Ks) to the bank.

(10) The bank generates a random challenge using the Ks and a random number. The random challenge is sent to the security capsule and it is used to validate the mobile users' ownership to the B-TID and Ks.

(11) The Security Capsule generates the Challenge Response using the Ks and returns the Challenge Response to the bank.

4.2 Authentication

The authentication phase starts when the user wants to login to the mobile banking service. The login function in the Security Capsule is initiated by the user. The following are the main steps in the authentication process and the steps are summarized in Figure 4.

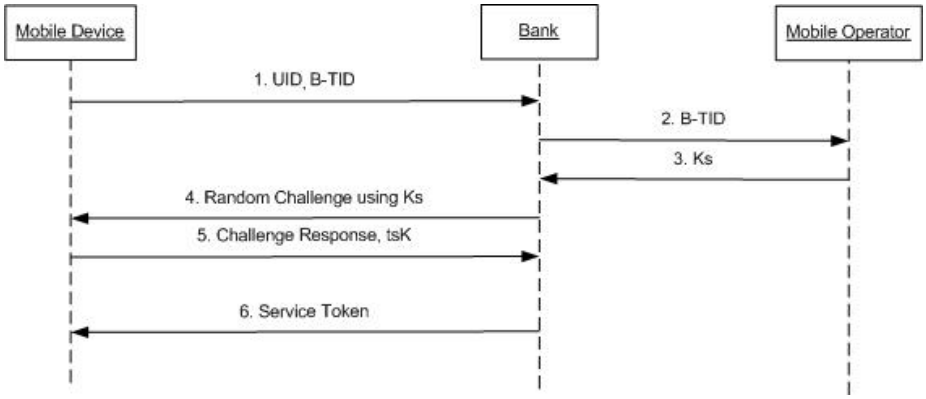

Figure 4: Authentication Process

(1) The Security Capsule accesses the present B-TID in the mobile device and sends the UID and the B-TID to the bank. If the B-TID is not available then Bootstrapping function is executed at the mobile operator. The B-TID and the UID are encrypted using the bank□s public key.

(2) The bank sends the B-TID to the mobile operator to obtain the relevant Ks for the communication.

(3) The mobile operator checks the B-TID and send the associated Ks to the bank

(4) The bank generates a random challenge using the Ks and a random number. The random challenge is sent to the Security Capsule and the challenge is used to validate the mobile users□ ownership to the B-TID and the Ks.

(5) The Security Capsule generated the Challenge Response using the Ks and returns the Challenge Response to the bank. Meanwhile, the Security Capsule generates session key (tsk) and sends it to the bank. This session key is used for all the future communication with the bank. The complete message to the bank is encrypted using the bank□s public key.

(6) At this stage, the Security Capsule and the bank are mutually authenticated to each other. The bank uses the Ks knowledge at the Security Capsule to authenticate the Security Capsule. The B-TID and the UID are encrypted using the public key of the bank by the Security Capsule. The knowledge of the banks private key at the bank is used to authenticate the bank to the Security capsule. The *Service Token* is generated by the bank and the token is sent to the Security Capsule as the authentication confirmation. Service requests from the mobile user to the banks should consist of the *Service*

Token and the service requests and service responses are encrypted by the tsK.

4.3 Authorization

The authorization phase is required when a mobile user wants to access or execute more sensitive activities. The user authorization is presented to the bank by generating the Data Key at the Security Capsule. The Data Key is generated using a number of identity and credential parameters at the mobile device. The following are the main steps in the authorization process and the steps are also presented in Figure 5.

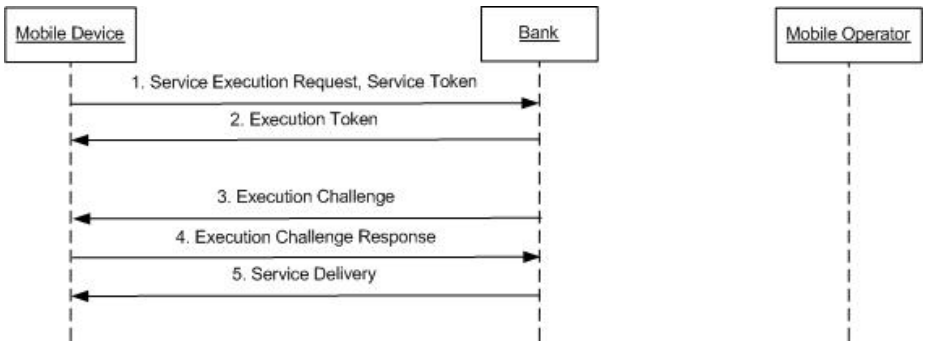

Figure 5: Authorization Process

(1) The user requests to execute a sensitive activity. The request for the execution is transferred to the bank with the *Service Token*.
(2) The bank generates an *Execution Token* and returns to the Security Capsule. The Execution Token is the authorization token for the activity execution. The bank issues the Execution Token based on the user access privileges evaluation at the bank.
(3) The bank generates the *Data Key* and sends the *Execution Challenge* to the Security Capsule. The Data Key generation process at the bank is explained in Section 4. The Execution Challenge is encrypted using the Data Key. The Execution Challenge is generated to verify the successful end-user level authorization.
(4) The Security Capsule generates the *Data Key* and then generates the *Execution Challenge Response* using the Data Key. The Execution Challenge Response is sent to the bank. The Data Key generation at the Security Capsule is explained in Section 4.
(5) If the *Execution Challenge Response* is successfully verified then execution of the activity is authorized to the user.

5.0 Execution Challenge Response generation

The Security Capsule obtains the request for the Execution Challenge Response from the bank and it retrieves relevant Execution Token from the device memory. The Data Key is generated as the initial step and then the Execution Challenge Response will be generated. The following are the Data Key generation steps at the security capsule.

(1) Validates the Execution Token integrity and the freshness. If the token is not valid then it is deleted from the Security Capsule and a new token is requested from the bank.
   - The XML signature of the token is verified with the bank□s public key certificate for the token integrity and authorization.
   - The timestamp of the token and the token lifetime are compared with the present timestamp from the bank.

(2) The Security Capsule obtains the IMPI and IMEI from the mobile device and the UID from the internal data storage.

(3) The Data Key for the Execution Challenge Response generation is generated using the hash function based key generation algorithm as shown in Figure 2. The key generation algorithm is designed using the hash functions.

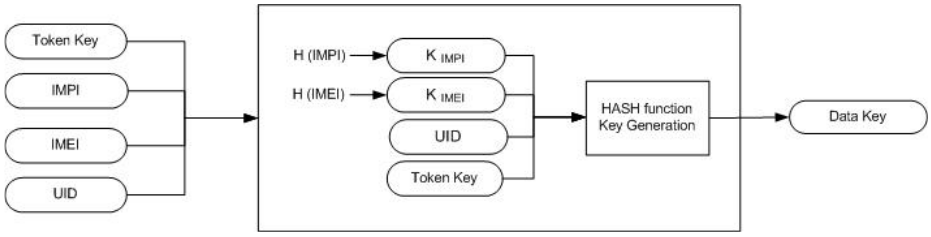

Figure 6: Key generation at the Security Capsule

(4) The Security Capsule generates the Execution Challenge Response using the Data Key and the Execution Challenge as shown in the below function. Then Data key is permanently deleted from the device memory after the process.

Function $_{\text{Execution Challenge Res}}$ (Data Key, Execution Challenge) = Execution Challenge Response

The Data Key generation and Execution Challenge Response generation functions are presented in Figure 7.

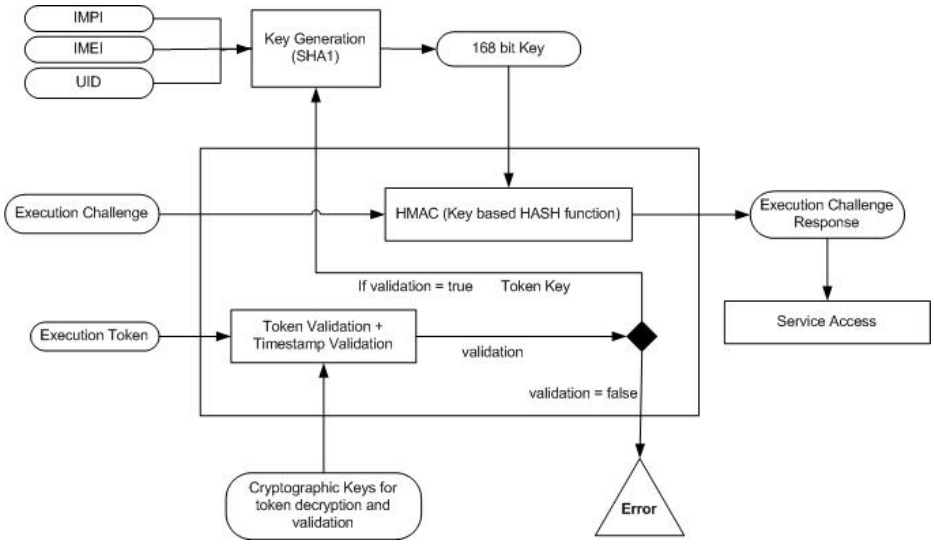

Figure 7: Security Capsule Functionality

6 Conclusion & discussions

The research novelty discussed in this paper leads to a standard secure mobile banking framework for mobile users to access their banking services from anywhere. The present mobile banking solutions require number of user intrusive activities during the authentication but our solution presents effective and user-friendly authentication solution for mobile devices.

We have evaluated our framework using the Scyther model checking security protocol verification tool [16]. Scyther is an automatic push-button tool for the verification and falsification of security protocols. The secure banking protocol is written using the SPDL (Security Protocol Description Language) and then validated using "Automatic claim" and "Verification claim" procedures in the Scyther tool. We have developed a proof of concept prototype for the evaluation. The prototype was successfully evaluated using number of know security attacks such as Hardware based

memory attacks, phishing attacks, source substitution attack, time-memory trade-off attack, codebook attack and known key attack.

A number of user intrusive activities for the authentication and authorization in the current mobile banking frameworks are one of the major drawbacks for users on the present authentication services for mobile banking and hence are not suitable for users to use at anywhere. However, the user authentication and authorization in our model is done using non-intrusive methods and hence user inputs are not required for the process. The proposed model will improve the efficiency and the usability of the mobile banking services. However, an extra 4 digit user PIN is recommended to prevent SIM cloning and mobile user impersonation attacks.

Using the parameter based access control techniques the banks will be able to introduced more identities and attributes to the key generation process. This will lead to different authorization levels based on the sensitive nature of the banking data involved in each transaction.

Finally, the proposed mobile banking security framework will be an effective and secure solution for present mobile banking applications. The solution will present novel secure authentication and authorization mechanisms to improve the customer confidence and satisfaction.

Acknowledgement

We would like to thank Ankur Garg from PEC University of Technology, Chandigarh, India for helping us on the technological research activity on mobile banking applications in UK, USA and Asia.

References

1. Wilcox, H., *Mobile Banking Strategies, Applications & Markets 2008-2013*, Juniper Research Limited, January 2009
2. Mobile Banking Association, *Mobile Banking Overview*, version 1.0, December 2009.
3. Halonen, T., *Authentication and Authorization in Mobile Environment*. Seminar on Network Security, HUT TML 2000.
4. Wu, M., Garfinkel, S., Miller, R., *Secure Web Authentication with Mobile Phones*, DIMACS Workshop on Usable Privacy and Security Software, 2004.
5. Clarke N., and Furnell, S., *Authentication of users on mobile telephones–A survey of attitudes and practices.* Computers & Security, 24(7):519–527, 2005.
6. Horn, G., Martin, K., Mitchell, C., *Authentication protocols for mobile network environment value-added services*, IEEE Transactions on Vehicular Technology, vol. 51, no. 2, pp. 383–392, 2000.
7. Weigold, T., *Java-Based Wireless Identity Module*, Proc. London Comm. Symp. 2002 (LCS 2002), 2002
8. Shin, S. U., and Rhee, K. H., *Hash functions and the MAC using all-or-nothing property*. In Proc. of Public Key Cryptography, LNCS, 1560:263–275, 1999.
9. Rannenberg, K., *Identity Management in Mobile Cellular Networks and Related Applications,* Information Security Technical Report, vol. 9, no. 1, pp. 77 – 85; ISSN 1363-4127; Elsevier Sciences, 2004.
10. Rannenberg, K., *CamWebSIM and Friends: Steps towards Personal Security Assistants*, pp. 173- 176 in Viktor Seige et al.: The Trends and Challenges of Modern Financial Services – Proceedings of the Information Security Summit; May 29-30, 2002.
11. Rossnagel, H., *Mobile Qualified Electronic Signatures and Certification on Demand*, Proceedings of the 1st European PKI Workshop - Research and Applications, 2004.
12. 3GPP 3rd Generation Partnership Project, *Interworking of Liberty Alliance ID-FF, ID-WSF and Generic Authentication Architecture*, Technical Report, 3GPP TR

33.980; Technical Specification Group Services and System Aspect, Release 4, version 1.0.0., July 2007.
13. Kalden, I. M., and Meyer, M., *Wireless internet access based on GPRS*, IEEE Personal Communications, vol. 7, no. 2, pp. 8-18, 2000.
14. Weerasinghe, D., Elmufti, K., Rajarajan, M., and Rakocevic, V. *Securing electronic health records with novel mobile encryption schemes,* International Journal of Electronic Healthcare (IJEH), v. 3, n.4, pp. 395 – 416, 2007.
15. MacDonald, J., Elmuft, K., Weerasinghe, D., Rajarajan, R., Rakocevic, V. and Khan, S., *A Web Services Shopping Mall for Mobile Users*, The 4th IEEE European Conference on Web Services (ECOWS□06), Switzerland, December 2006.
16. Cremers, C., *The Scyther Tool: Verification, falsification, and analysis of security protocols.* In Proc. of the 20th Int. Conf. Computer Aided Verification (CAV□08). Lecture Notes in Computer Science, vol. 5123. Springer Verlag, 414–418, 2008.