



Two-way Secure Communication between SIM and Backend



Table of Contents

Executive Summary 2

Introduction and Background 3

Description of the problem..... 4

Solution implemented 7

Potential Market analysis 9

Recommendations/Future work..... 10

References 10

Executive Summary

The evolution of mobile communication has significantly increased the amount of sensitive information transmitted between mobile phone and backend systems. It won't be an exaggeration in saying that mobile has become the single most personal powerful device for communication, financial transactions, banking, entertainment, authentication and authorization.

Although, the major mobile operating systems such as android and iOS regularly release updates and patches to keep their OS secure and safe. In spite of that, these mobile OS are susceptible to cyber-attacks like OTP stealing, SMS interception and other malware attacks. Attackers are developing sophisticated malwares to exploit vulnerabilities in the layers of mobile OS, applications, libraries, middleware and packages etc.

This white paper delves into the implementation of end to end secure channel communication between a SIM card and a backend server eliminating the interaction with mobile OS. The solution highlights an operating system independent way to provide two way communication between Subscriber Identity modules (SIM) and backend systems. It enables execution of sensitive operations protected by strong cryptographic semantics offered by tamper resistant hardware of SIM and backend technologies.

This may open up avenues for MNOs to help various application providers such as finance, banking and government to get better security framework for their applications and solutions to strengthen the overall security and privacy. Technical Implementation details and potential market analysis are also discussed in this white paper. A possible roadmap is also placed to exploit the power of the developed backbone for secure messaging targeting applications ranging from banking, finance and strategic sectors.

Introduction and Background

Mobile has become primary choice of device for accessing banking, financial, government and many other sensitive services & applications. This makes mobile phone a hot spot for attackers.

To understand these security threats and attack surface, first we need to understand how a typical mobile app works. In general, mobile apps make use of APIs for communication between App and backend server where most of the business logic is implemented.

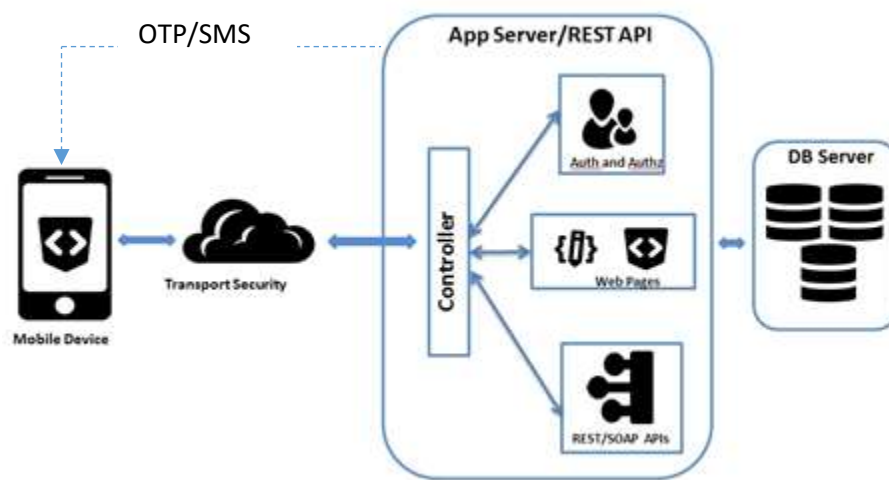


Figure-1 General Mobile App-Backend Interaction

Mobile app uses standard TLS/SSL transport layer security between mobile app and backend server for confidentiality as depicted in the figure above. In situations like banking & financial transactions and password reset, an OTP is also sent from backend (with the help of third party SMS service/MNOs) for user authentication. Although OTP is extensively used for authentication. APIs and OTP communicate over separate channels. However, there are many vulnerabilities in the entire communication chain inviting cyber attackers to exploit.

For instance, the OS on which these mobile apps run can't be trusted fully for sensitive operations and information storage. Data security at rest, in execution and in transit is to be ensured for secure operations.

Although government has mandated the use of other factors of authentication to strengthen the security of banking and finance applications. However, the existing system of multi factor authentication are either conventional SMS based or app based which are not properly secured.

SMS can be classified into two broad groups: sensitive SMS and non-sensitive SMS. Apart from traditional plain text user data (non-sensitive SMS) transfer, it is being used for sensitive information sharing where possession of mobile (SIM card) is necessary to validate. Few of those application usages are:

- Mobile number or User verification by sending a secret code to specific mobile number or user. It is mainly used in various software service-based user account creation or linking Mobile number with service/s.

- Alternate channel verification or Out-of-Band authentication or 2FA is done/achieved by sending secret code. It is primarily used in user Account log-in in various software services where Mobile number is already linked with other user information (such as Username, Password, and email id etc.).
- Transaction authorization by sending secret code. It is primarily used for transaction authorization in software-based banking service system where user need to give consent by providing same secret code (shared over Mobile number) to the system. In the absence of proper security protection, these digital secret codes may be vulnerable and thus prone to be captured by attackers. Thus, it is evident that there is a need to provide secure ways of communicating sensitive information.

Two factors authentication using OTP is also common nowadays. One Time Password (OTP) or SMS has been extensively used as the second factor authentication or sensitive information sharing method in many applications ranging from Banking to Government etc. to provide better secure digital transactions between users and service providers.

This white paper presents an innovative solution for securely transferring OTPs and other sensitive data to end user with due authentication. The solution provides end to end secure communication between user SIM card and backend systems. The followings are integrated to provide the solution

- Tamper resistant SIM card hardware
- Strong encryption mechanism
- Class-2 SMS
- Return path communication using SMS
- Callback Backend API communication

The solution provides the following advantages over existing methods







Trusted delivery of OTP only after user authentication	Authentication 
Application independent	No Mobile application is required 
Minimal or No Host OS involvement	Works on all the mobile OS 
All types of mobile phones supported	Works on any kind of mobile device 
Optional strong end to end encryption.	Confidentiality 
Ease of use with legacy support	1. SMS OTP 2. Automatic OTP signing 

Figure-2 Advantage of secure messaging

While existing methods of sending OTP or authentication code does not authenticate the intended recipient before the delivery of message, the proposed solution ensure that user is properly authenticated before hand over the message. This solution also provide a facility where OTP or sensitive code even not revealed to the user. In one of the variant of the solution, OTP is sent back to backend server silently. Further the returned OTP or code may signed or encrypted with symmetric and asymmetric encryption based on the capability of the SIM.

Description of the problem

Though two factor authentication is widely and extensively used in our country in many applications and services for user authentication by using two separate channels, but this method of two factor authentication is prone to cyber-attacks. A compromised sensitive data or OTP may lead to many security vulnerabilities including changing password of all the accounts like mail, banking, social media, government services, cloud services etc. and eventually denying access to legitimate user thereafter.

Several cases have been reported including OTP stealing and auto debit where user account gets debited without even any activity in user mobile phone. The problem statement we are attacking is that as of now there is no secure way of communicating OTPs, SMS and other sensitive codes to user. As depicted in the figure below, a generic flow of SMS/OTP is shown on the left side and the proposed solution is depicted on the right side.

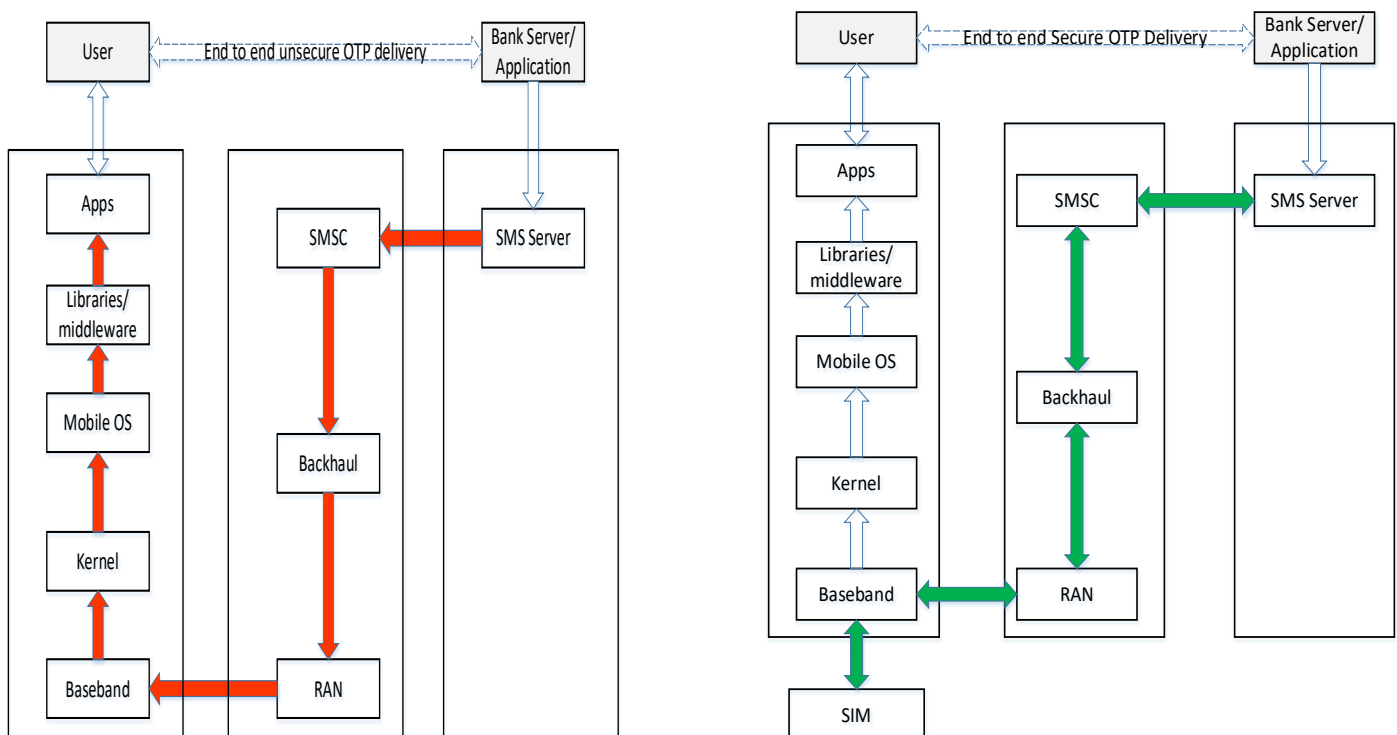


Figure-3 Unsecure SMS/OTP flow (left) and secure flow (right)

There is no end to end encryption of these sensitive information in the path from server to end user. Although there may be encryption used over a one or many segments in the communication path; for example application server may be sending encrypted payload to third party SMS provider using TLS/SSL security. However, there is no end to end secure communication available which ensures the secure delivery as well as verification. In summary the following are the issues with existing OTP/SMS systems

- There is no mechanism for user authentication before delivery of the message to the intended recipient.
- Further, all the existing methods of sharing information between backend system and mobile phone hit mobile OS which allows attackers to exploit.
- For app based authentication, user needs to install and use mobile apps. These apps store data in mobile memory which may not be considered as secure.
- The existing solution are OS dependent

Solution implemented

A solution has been developed to provide end to end security for any message sent between backend system and SIM card. Further, the information exchange is protected by user authentication and backend server authentication if required. The architecture of the developed solution is depicted in the figure below

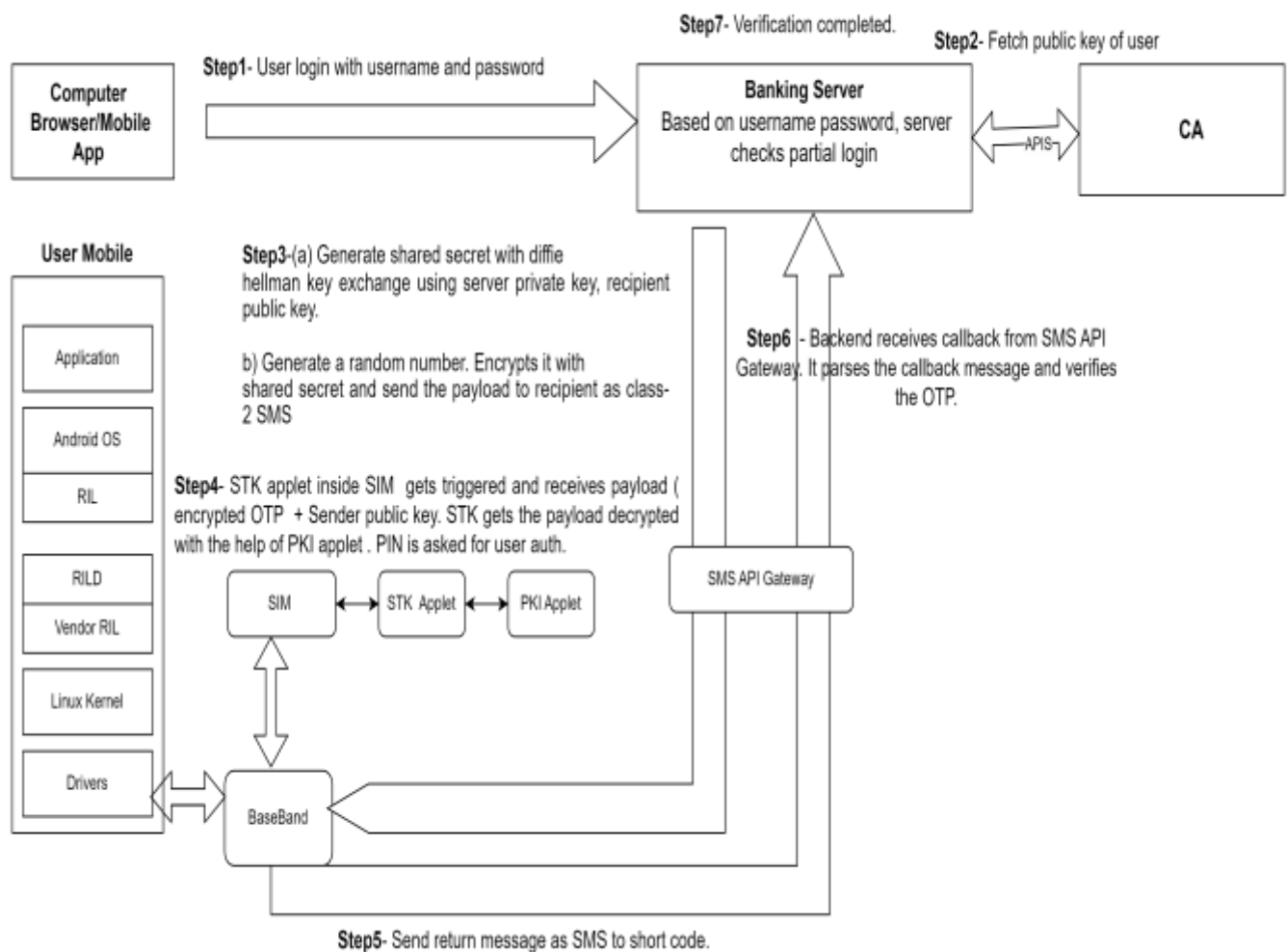


Figure-4: Solution architecture- End to end Bi-directional secure communication

We have developed and implemented a demo banking use case. The following steps explain the solution

Step1- Customer logs in the banking system using his bank provided username and password. This works as partial login where even if user is authenticated with his credentials, he has to perform one more authentication using our solution.

Step2- Based on user information like mobile number, backend system communicates to CA system and fetches the user certificate.

Step3- Two things happen in step 3

3(a) Backend server generates shared secret using its private key, customer's public key fetched from CA.

3(b) Backend server generates a random number for OTP and adds some configurable information to the payload with public key of server. After payload preparation, backend server sends a class-2 SMS to the customer SIM directly bypassing the mobile OS. The details of the variable payload are shown below.

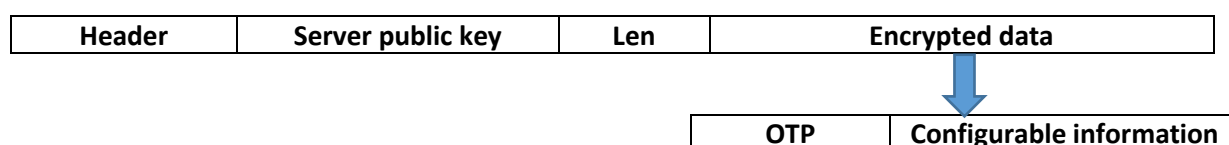


Figure-5 Payload structure

Step4- The secure messaging STK applet inside the SIM card gets triggered and an SMS-PP envelope is sent to STK applet carrying the payload. Secure messaging applet then asks for user PIN for authentication. Once the user is authenticated with valid PIN, it gets the data decrypted by PKI applet on the same SIM. A simpler block diagram is depicted below

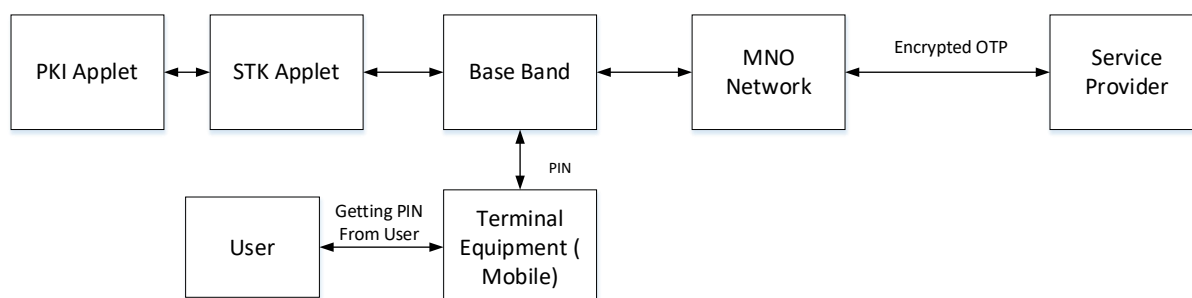


Figure-6 Components of implemented solution

Step5- Once the data is decrypted after user authentication, the same OTP or code is returned via a normal SMS generated from within the SIM card to a short code.

Step6- The SMS or notification server gets notified from SMSC for SMS receive. It then sends a call back to secure messaging backend. It parses the message from SIM and validate it. If verification successful then customer is able to login in the app else won't be allowed to login.

The same flow is implemented for transferring amount to a recipient where a dummy amount is sent after entering transaction password. This solution may be implemented on normal as well as enhanced PKI SIM card. In case of normal SIM card, there is no need of Certifying authority while in PKI SIM, a CA or certifying authority is required to provide certificate details for shared key generation.

Potential Market analysis

Recommendations/Future work

The end to end secure communication is an excellent example of integration of ICT and telecommunication. In this solution, we have leveraged tamper resistant property of SIM card, flexibility of backend infrastructure in terms of REST API to glue backend and SIM. We have also exploited special class of SMS i.e. class-2 SMS for allowing communication between SIM card applet and backend. Further SMS and TCP/IP also leveraged for transporting data between SIM and backend in secure manner.

The solution presented in this white paper provides the backbone for facilitating end to end bi-directional secure communication between SIM and backend. Data exchanged over this backbone may be encrypted using symmetric as well as asymmetric cryptography. Digital signature and Message authentication coder can also be used for authentication. Riding the backbone, numerous applications leveraging the security semantics of this backbone may be developed and potential business use cases may be developed around them. Banking and finance sector may be tapped for suitable applications requiring strong security for logging as well as transactions. The solution may also be used in strategic areas where data security is paramount. Further, the solution also provide secure key storage for storing secret keys for long time. Further, premium banking may be implemented for select customers to provide secure transaction facility.

References

- [1] https://www.etsi.org/deliver/etsi_ts/151000_151099/151011/04.14.00_60/ts_151011v041400p.pdf
- [2] https://www.etsi.org/deliver/etsi_ts/102300_102399/102384/09.00.00_60/ts_102384v090000p.pdf
- [3] https://www.etsi.org/deliver/etsi_ts/131100_131199/131111/09.01.00_60/ts_131111v090100p.pdf