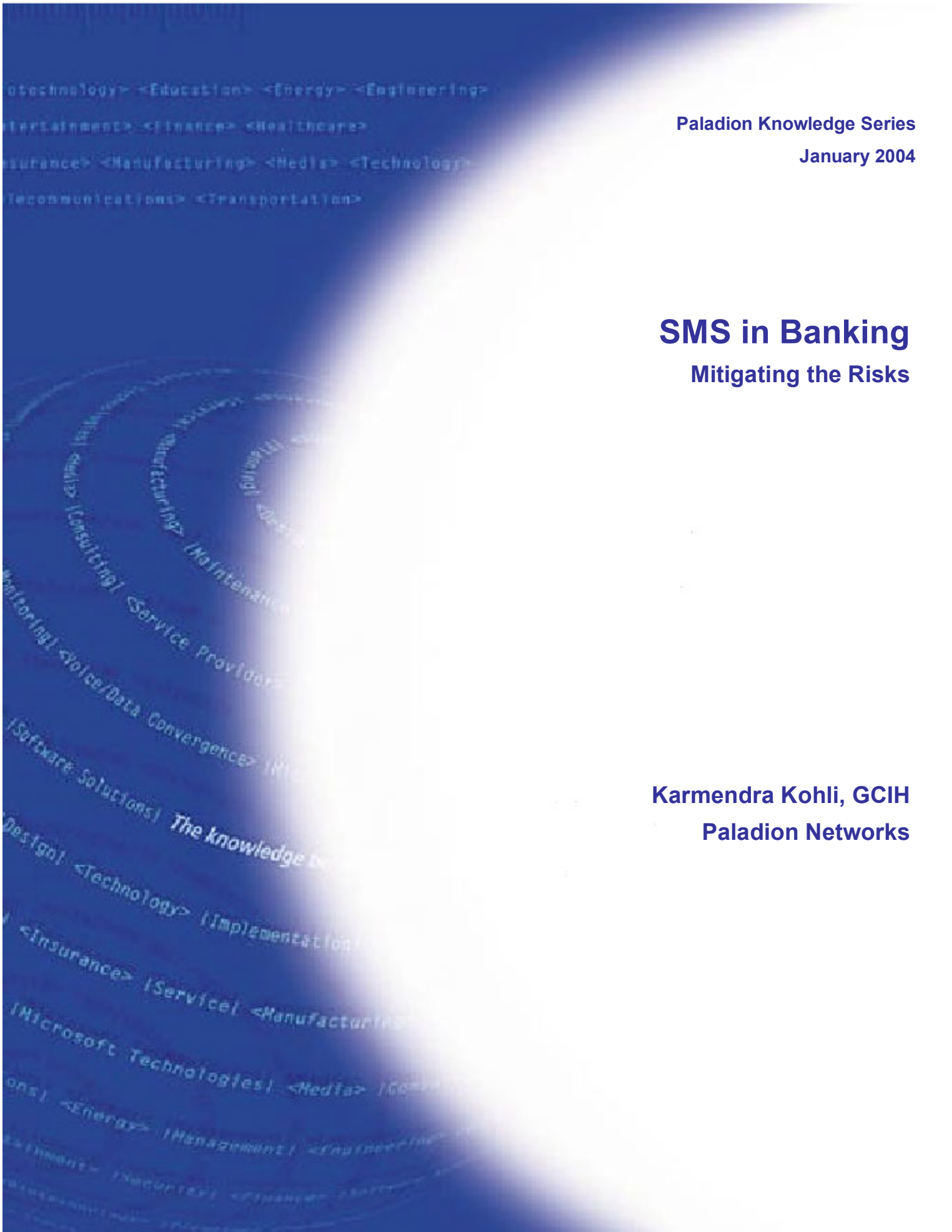


Paladion Knowledge Series
January 2004

SMS in Banking

Mitigating the Risks

Karmendra Kohli, GCIH
Paladion Networks

Introduction

In today's business environment, with so many activities going on simultaneously, the bank's customers are hard pressed for time. They have appointments to keep, meetings to attend, etc. Many customers wish they could also do other activities while traveling from one meeting to another. Here comes the use of mobile phones. The Mobile Banking service gives your customer account information and real-time transaction capabilities from the mobile phone at a true "anywhere, anytime, anyhow" convenience. It also allows you to send messages on the Bank's services and products to your customers. Mobile Banking with the regular mobile phones enables the following transactions:

- Get account balance details
- Obtain last 3 transaction details
- Request an account statement
- Request a cheque book
- Stop a cheque payment
- Enquire the status of a cheque
- Get bill payment details for electricity, and telephone services
- Get bill payment details for mobile phone

Two terms we frequently come across:

Wireless carriers: These are the mobile service providers like Sprint, AT&T, Orange and Airtel.

Bulk SMS service provider: These are the intermediate providers between the bank and the wireless carrier for mobile banking.

An Overview of Mobile Banking

There are two ways that a bank may choose to communicate with customers using SMS over the internet:

1. The bank proactively sends information like promotional messages & transaction alerts its customers.
2. The customers request information from the bank and the bank sends the response as an SMS message.

1. Banks may proactively send the information to customers in the following ways:

   E-mail to Mobile

   In this method, the bank first sends an e-mail to a mobile banking application installed on the bank's network. The application receives the mail containing the message along with the mobile number, and sends these contents in a specified format over to the bulk SMS service provider. The SMS service provider forwards the message to the wireless carrier, which in turn sends the messages to the customers.

   Database to Mobile

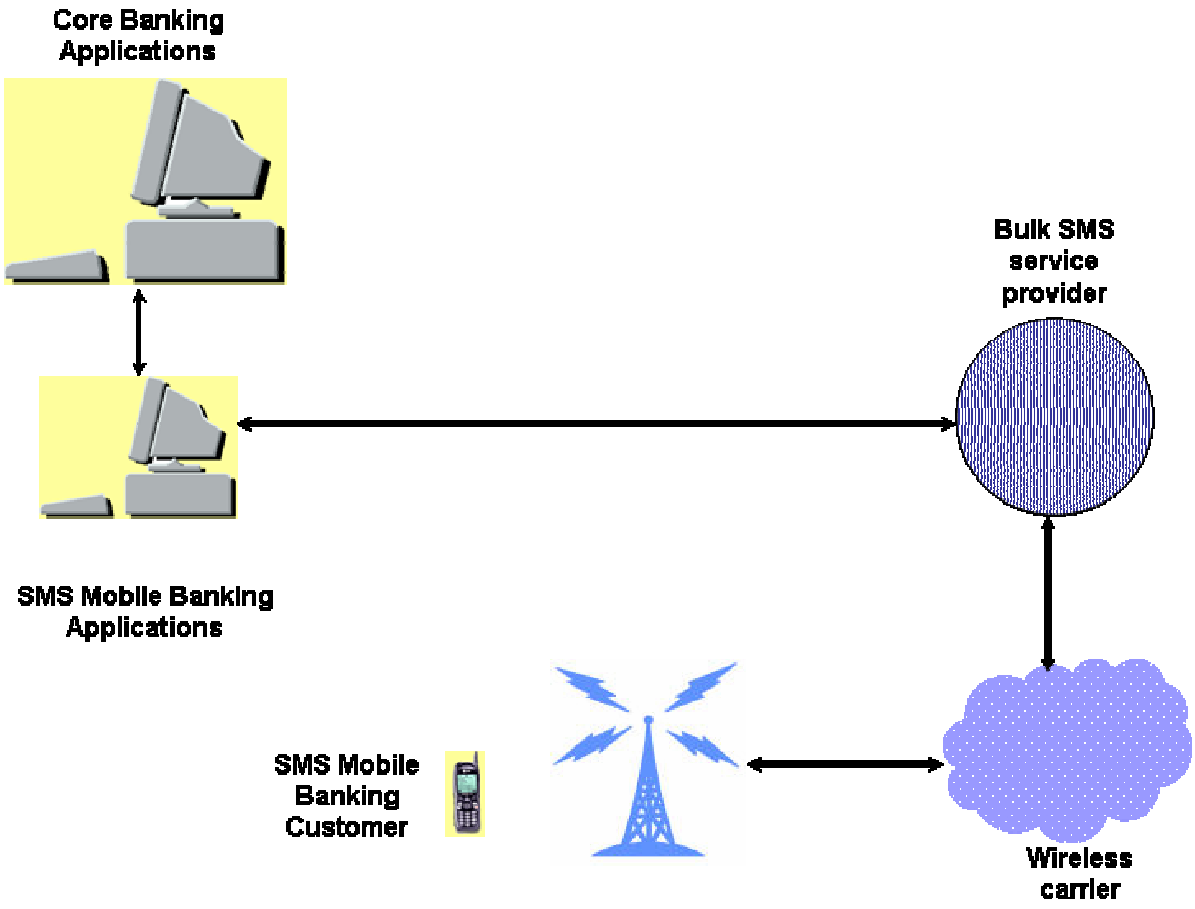
   Here, a mobile banking application is installed on the banks network that continuously polls a bank's database. Whenever a relevant event occurs – like the crediting of a salary account - the application detects a change in the database, and triggers an SMS message to be sent based on the details in the table. This application also sends the contents in a specified format over to the bulk SMS service provider. The message after reaching the SMS service provider is forwarded to the wireless carrier, which in turn sends the messages to the customers.

2. Banks can also send data on requests made by the customers. A customer sends a request message to the bank with a pre-defined transaction code to the wireless carrier providing the GSM service. The wireless carrier in turn sends the message to the SMS service provider. The SMS service provider forwards the request to the mobile banking applications running in the banks network. These mobile banking applications in turn interface with the core banking applications to service the customer request. The response is then sent back to the customer.

The entities participating in mobile banking transactions are:

- Core banking applications that contain account information
- SMS Mobile banking applications that interface with the SMS network
- Bulk SMS service provider application that sends SMS to the wireless carrier
- The wireless carriers who transport the messages to the mobile handset
- The handset that is the end user interface to the bank.

The high level block diagram shows the participants in Mobile Banking.

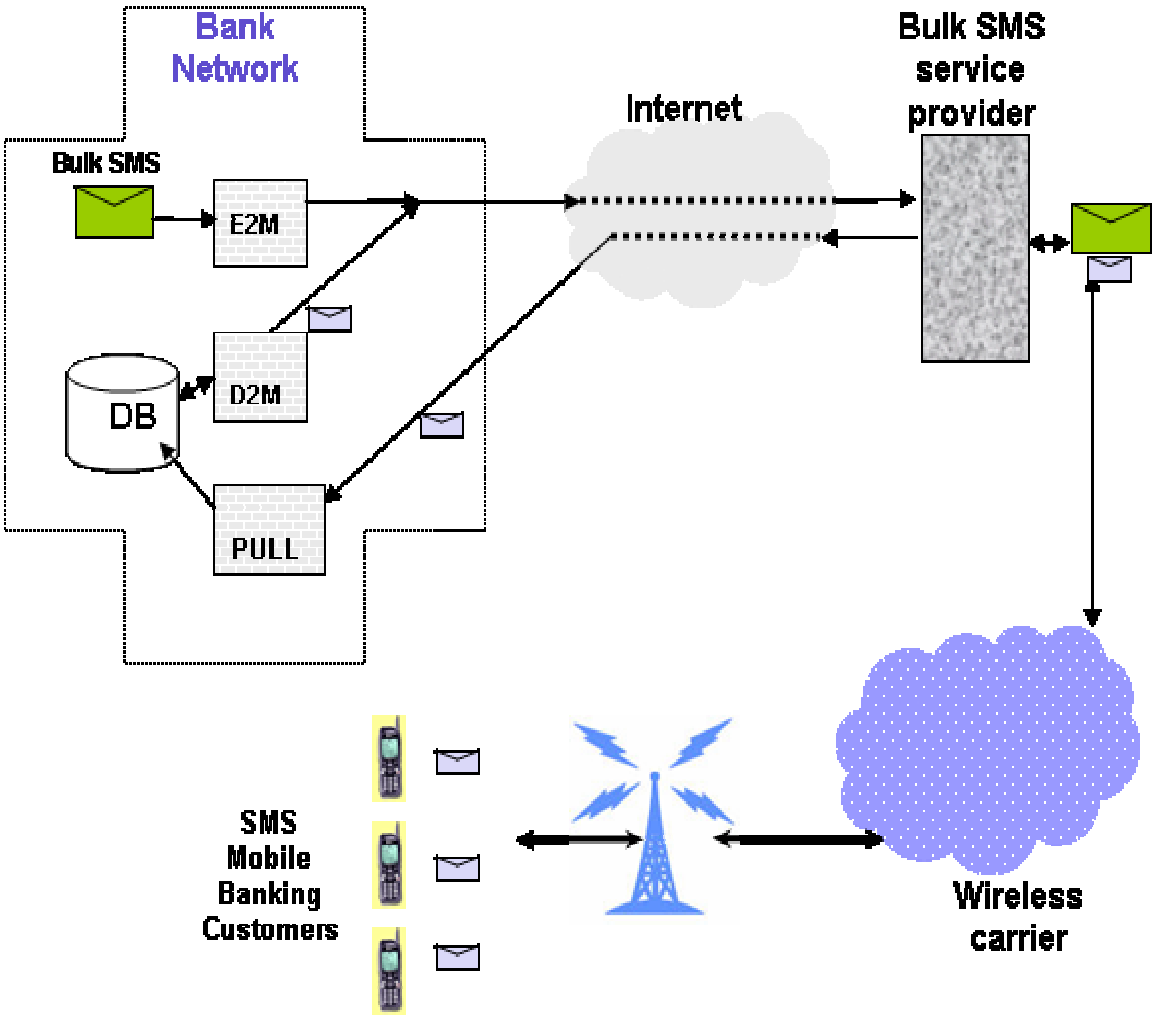


A Closer Look at Mobile Banking

Let's take a closer look at the mobile banking architecture and the components involved in the next page.

The three interesting components we need to understand are:

E2M – E-mail to Mobile application
D2M – Database to Mobile application
PULL – Customer-Request receiving application



The E2M application

The Email to Mobile (E2M) application is used to send promotional/informational messages to the bank's customers. In this, the bank sends an e-mail to the application in the required format. The E2M application then formats the message and sends it to the Bulk SMS service provider who then sends the message to the Wireless carrier. The wireless carrier delivers the message to the bank's customers.

The D2M application

The Database to Mobile (D2M) application is used to send event driven messages to the bank's customers. An event in this case may be crediting of money in the

account, payment of credit card dues, etc. The D2M application continuously checks for relevant changes in the database. When a change is detected, it constructs a message in the correct format and sends it to the Bulk SMS service provider who then sends the message to the Wireless carrier. The wireless carrier delivers the message to the bank's customers.

The PULL application

The PULL application is used to receive customer requests and to forward them to the core banking application. The customer first sends a pre-defined request code via SMS to the Bulk SMS service provider's registered mobile number. Depending on the message code, the bulk SMS provider forwards the SMS to a PULL application. The PULL application receives the request and forwards it to the core banking application for further processing.

The E2M, D2M and PULL applications are provided by the Bulk SMS provider. These talk to the servers located on the Bulk SMS provider's network. The Bulk SMS Provider also has custom components installed at the wireless carrier's end. These are the components that it communicates with when forwarding messages from the bank to the Wireless carrier and vice-versa.

The Security Perspective

As a security conscious bank, what are the security concerns that you need to be wary of? From our experience, the threats to mobile banking come in the following forms:

1. **Sending Spam SMS messages to mobile numbers.**

   It may be possible for outsiders to send spam messages to the customer's mobile using the mobile banking application- this would affect the reputation of the bank.

2. **Disclosure of information through logs**

   Frequently, mobile banking applications log the message that is sent to customers. The message may contain sensitive information like account details, and anyone having access to these logs or the backup of the logs will gain unauthorized access to this information.

3. **Eavesdropping on traffic between mobile banking application and bulk SMS provider.**
   Traffic transmitted from the mobile banking application to the Bulk SMS provider over the internet can be eavesdropped. The message may contain important information about customers and could lead to unauthorized information disclosure.

4. **Sending messages to the SMS provider's server by impersonating as the mobile banking application.**
   If the format of the messages transmitting between the mobile banking application and the bulk SMS provider is known, an attacker might impersonate as the mobile banking application and send messages to customers via the bulk SMS provider.

5. **Sending Spam requests to the PULL component by impersonating as SMS provider's server**
   An attacker may obtain information from the PULL component installed in the bank's network by impersonating as the SMS provider's server. This is possible if the attacker sends the messages in the required format, and the PULL component does not authenticate the sender.

Mitigating the Security Risks

The following steps could be taken to mitigate the risks in Mobile Banking:

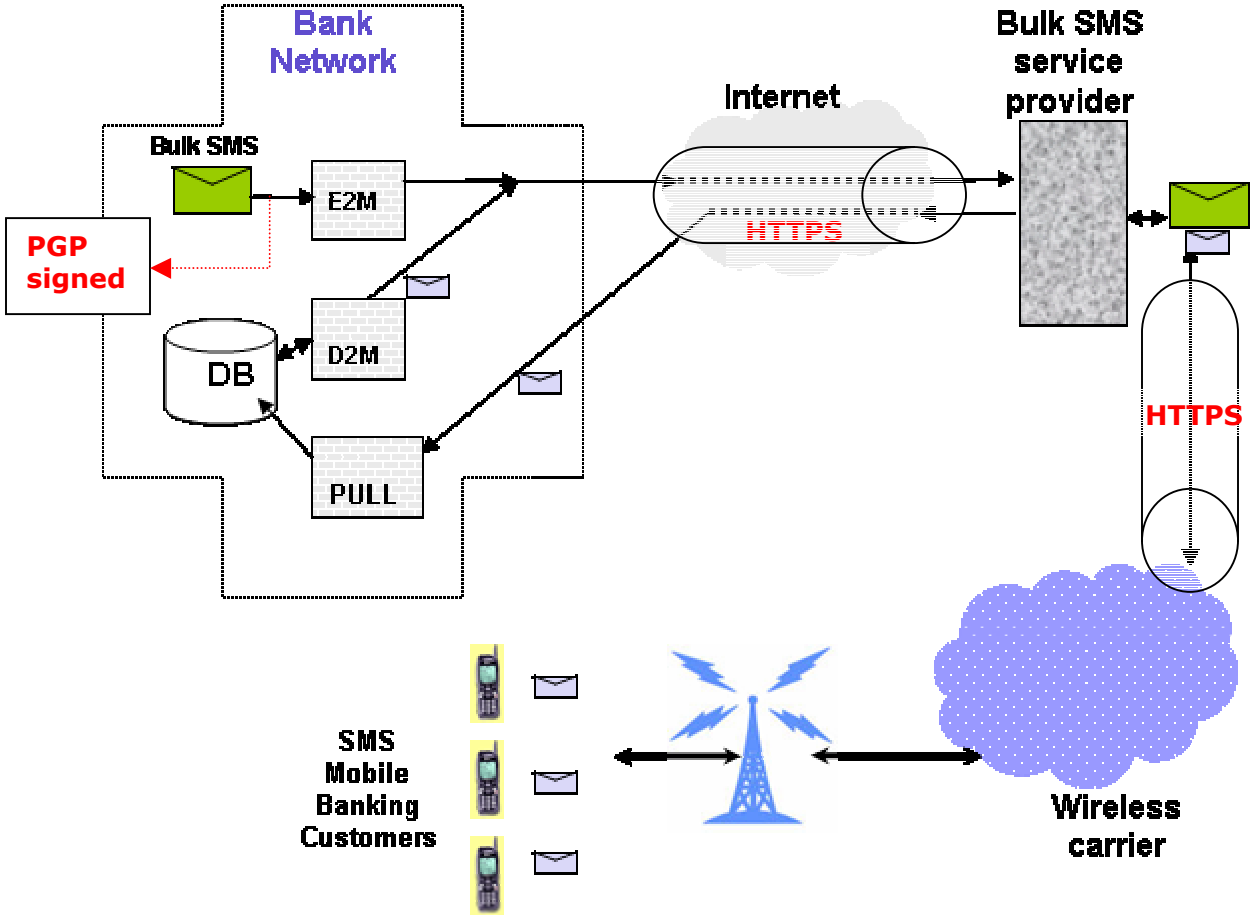
1. Authenticate the sender before sending data from the mobile banking application to the bank's customers. It must be ensured that only the authorized employees of the bank are allowed to send E-mails to the E2M application. Depending on the mail server used by the bank, multiple options are available. Further, an appropriate digital signing mechanism should be considered to send E-mails to the E2M application.

2. Care should be taken to ensure that critical information like account details are not stored in the logs. Additionally, the logs generated by the application should be stored encrypted.

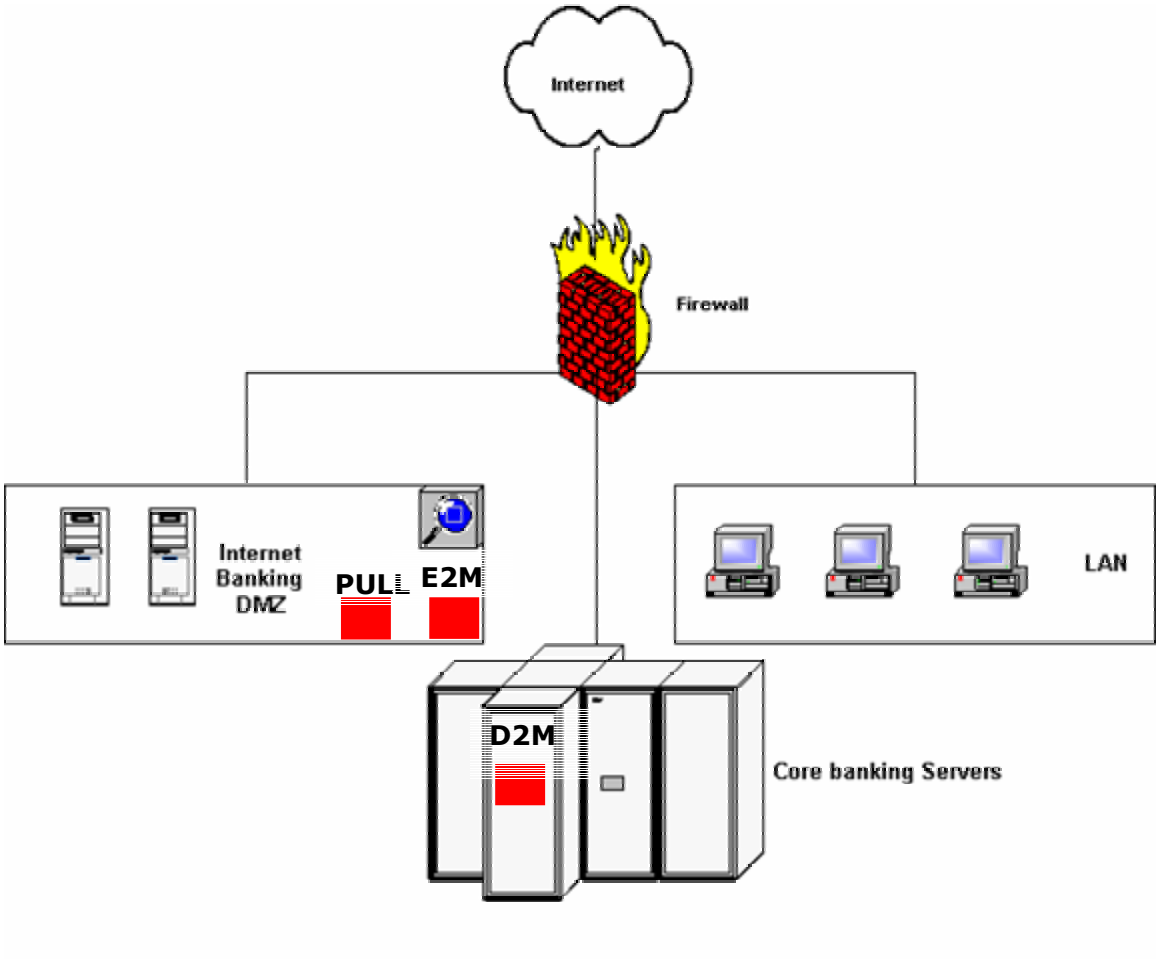
3. The traffic between the bank and the bulk SMS provider and again between the bulk SMS provider and Wireless carrier should be sent over a secure channel. In our experience, 2-way SSL gives adequate protection and is simple enough to implement in this system.

A Secure Architecture for Mobile Banking

Here is an architecture that addresses the risks discussed in this paper. The next diagram shows the recommended placement of the components in the banking infrastructure.



Location of Mobile Banking Components in the Network



We recommend the above architecture for production environments:

- The E2M component should be placed on the mail server in the Internet facing DMZ. The component receives the message from the mail server. The message is then forwarded to the bulk SMS provider's server over HTTPS.
- The D2M component should be placed in the inner segment where the core banking systems are located, as it continuously polls the banking database. When the D2M component receives an event trigger, it crafts an XML message and sends it over HTTPS to the bulk SMS providers' server.
- The PULL component should be placed in the Internet facing DMZ – it receives information from the bulk SMS provider's server over HTTPS. It then forwards the request to the backend application which is responsible for processing the request.

Summary

SMS in banking provides a new opportunity to banks to extend their services to customers, and improve their competitiveness. As with other technology initiatives, this service also has its concomitant risks that need to be addressed. Through a mix of policies and suitable design, the risks can be mitigated and a safe environment assured to the bank's customers.

About Paladion Networks

Paladion Networks is a leader in security consulting serving some of the largest corporations in the world. Our consultants have worked closely with technology strategists of banks, financial institutions and telecom providers to plan the security roadmap for SMS banking and other new services. Please do contact us for any further information you may need regarding our offerings in SMS security or any other security service you may require. Our contact details are given below

USA, Canada
Email: sales@paladion.net
Tel: +1 510 468 9285
Tel: +1 510 490 3755
Contact: Rohini Gupta, PhD

Middle East, India
Email: sales@paladion.net
Tel: +91 22 55910513
Fax: +91 22 55912429
Contact: Rohit Kumar, CISSP

Malaysia
Email: sales@paladion.net
Tel: +603 2168 4275
Fax: +603 2168 4201
Contact: Sreeraj G, CISSP