Secure USSD Facility for Financial Institutions
Analysis and Recommendation Report

<table>
<thead>
<tr>
<th>Client</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>System</td>
<td>Amber USSD Gateway</td>
</tr>
</tbody>
</table>
### Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Author</th>
<th>Date</th>
<th>Change Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.0d1</td>
<td>PMT/HJ</td>
<td>2010/05/28</td>
<td></td>
</tr>
</tbody>
</table>

### Document Approval

<table>
<thead>
<tr>
<th>Position</th>
<th>Name</th>
<th>Sign-Off</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>PMT Director</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Head</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Development Lead</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright © Pattern Matched Technologies 2010. All rights reserved.

This document contains confidential and proprietary information that is the property of Pattern Matched Technologies and/or its clients. The information may not be copied, modified, circulated, distributed or used in any manner without the prior written permission of Pattern Matched Technologies. For additional copies of the document, please contact Pattern Matched Technologies.
Contents

1. Introduction and Executive Overview .................................................................................4
2. A centralised secure facility for USSD ..................................................................................5
   2.2. The MNO’s contribution ...............................................................................................5
3. Why a public USSD gateway is not suitable ........................................................................6
   3.1. Repudiation of transactions .......................................................................................6
   3.2. Access to the USSD gateway .......................................................................................6
   3.3. Mixing of trusted and non-trusted content .................................................................6
   3.4. Billing of subscribers .................................................................................................6
   3.5. Provisioning process ..................................................................................................6
4. Requirements for a USSD gateway dedicated to financial institution .................................7
   4.1. SIM card validation .....................................................................................................7
   4.2. Financial grade encryption .........................................................................................7
   4.3. Secure hosting ............................................................................................................7
5. Business Models ..................................................................................................................8
6. Operational impact of the secure facility .............................................................................9
   6.1. SS7 integration ...........................................................................................................9
   6.2. Support and Monitoring ............................................................................................9
   6.3. Financial transactions ..............................................................................................9
7. USSD Security .....................................................................................................................10
   7.1. USSD Communications .............................................................................................10
   7.2. Transport data ...........................................................................................................10
   7.3. Session data .............................................................................................................11
   7.4. PIN Encryption .........................................................................................................11
Appendix A. Glossary .............................................................................................................12
1. Introduction and Executive Overview

Background

When a major South African bank awarded a tender for the supply and implementation of an USSD-based mobile banking solution to Pattern Matched Technologies (in partnership with Nokia Siemens Networks), we had a mandate to discuss various options with each Mobile Network Operator (MNO) to establish this service.

We concluded that the best solution requires the establishment of a trusted USSD facility that is run and operated separately from the standard, public USSD services. This document provides arguments on why the current public USSD infrastructure in Southern Africa is not a suitable solution for financial services, and contains a proposal for a better solution.

Goals

Our aim is to work with the MNO to establish a secure, financial-grade USSD environment that is suitable for use in mobile financial services, such as mobile banking, mobile payments or mobile money transfer. We propose a partnership with the MNO to provide this facility for mutual benefit and to enable our customers to service the market. There is a large opportunity currently on the table, that can add significant value in the future.

Pattern Matched Technologies (PMT) proposes to supply and operate this facility on behalf of the MNO and the financial institution, and maintain the security and integrity in a manner that is acceptable to both the MNO and the financial institution.

The solution

The solution consists of several components including SS7 level integration into the MNO network: secure servers, audit services and a complete package focusing on a great customer experience.

Benefits to the MNO

The MNO stands to benefit in the following ways:

1. It gains a close relationship with financial institutions. There is also the possibility of direct debits to customer accounts, because of the trusted service provided to the financial institutions.
2. Reputation – this will send a message that the MNO provides secure and trusted transaction services, as opposed to only telecommunications.
3. The MNO pre-empts the requirements of the financial sector and provides a single solution for use by all financial institutions.
4. Depending on the business model, the MNO can earn transaction-based income.
5. The MNO becomes the market leader in transactional services.
6. A solution in Southern Africa can be extended to other African countries, thereby leveraging a single solution throughout the entire enterprise.

What do we need?

- Buy-in from the MNO and sign-off at an executive level that it is possible to establish the secure facility.
- Access to the core network on the SS7 level with appropriate configuration on the HLR to be able to use USSD.
- A suitable location for the secure facility in the MNO’s data centre.
2. A centralised secure facility for USSD


There is a very strong trend in the financial markets to invent new ways of reaching the large Southern African market. Mobile banking and the ability to transact from your mobile phone is a key aspect to many of the solutions currently under consideration.

USSD is a core technology for mobile financial services such as mobile banking. It is very likely that many banks and other financial institutions will approach MNOs in the near future with requests for access to the USSD carrier, and they will most likely have very similar requirements.

2.2. The MNO’s contribution

It is in the MNO’s interest to be pre-emptive and to establish a central facility, shared by all financial institutions – at the present, before the markets force the MNO to follow the lead of other networks.

There are two options for a financial institution to use the USSD services on the MNO:

1. Connect via the existing public USSD gateway provided by the MNO to USSD service providers for primarily content-based applications.

2. The MNO provides a suitable, highly secure and trusted environment for the use of Southern African financial institutions.
3. Why a public USSD gateway is not suitable

3.1. Repudiation of transactions

It is possible for parties (for example, MNO staff or support personnel from suppliers) to access the environment and relatively easily intercept USSD messages and impersonate subscribers. Messages are recorded in CDR form and in log files, and will contain plain text PIN values. Most MNOs cannot guarantee the confidentiality of information passing through the gateway. This means that the MNO will not be able to be indemnified by the financial institution in the case of non-repudiation.

The best solution is to provide a facility where interception and impersonation is impossible. Only if the MNO implements a dedicated, secure USSD gateway facility will it be possible to prove that a certain subscriber originated a transaction, and will it be possible to manage the risk.

3.2. Access to the USSD gateway

The public USSD gateway is not designed with banking-grade security and auditing requirements in mind. It is not feasible to mix the basic USSD requirements for many tens of what are primarily content providers with the very specialised requirements of financial services providers in a single system. Too many persons have access to the USSD machines, either in the data centres or remotely.

3.3. Mixing of trusted and non-trusted content

A public USSD gateway (such as the South African WASP USSD gateway) has been designed to deliver simple, non-trusted services to WASPs. It delivers ring tones, prepaid balances and top-up services that do not require stringent security.

3.4. Billing of subscribers

A major issue with public USSD gateways of most MNOs, is that it bills the MNO’s subscribers for transactions. However, a banking model, for example, would require that the subscribers are not billed on their mobile phone account, but rather that the charges be carried by the bank (in other words, reverse billing). Currently, most USSD gateways do not have the infrastructure and billing interfaces available to account for the reverse billing transactions.

3.5. Provisioning process

USSD is usually provisioned on the WASP platform based on a process that focuses on the speed of rollout and possible impact on the network. This process is not tiered for security, nor does it have the proper auditing and trust aspects integrated into it that is required for the financial service.

Financial institutions require a better solution that incorporates a high level of trust. This model is fundamentally incompatible with the WASP process. For that reason, the banking and financial services model should not be merged with the WASP model.
4. Requirements for a USSD gateway dedicated to financial institution

4.1. SIM card validation

It is possible to verify the IMSI of a subscriber using the USSD gateway. If this information is passed to the financial institution, it will be able to detect the case of a simple SIM swap and be able to avoid fraud. This is achieved by using information available on the SS7 MAP layer. The proposed USSD gateway will always link an IMSI number to the MSISDN and pass this to the banks to ensure that SIM swaps can be detected.

4.2. Financial grade encryption

It is of the utmost importance to protect the USSD strings against interception by unauthorised parties. The USSD gateway needs to use an HSM with very tightly controlled encryption keys (similar to those protecting the banking ATM network) to ensure that all information will be confidential.

Each financial institution’s encryption keys will be loaded in a process acceptable to its auditors. This will allow all traffic outside the secure gateway to be encrypted in a way that only the destination financial institution will be able to decrypt. In this way, the area in which the traffic is not secure is minimised, as shown in the following diagram:

![Secure USSD Gateway Diagram]

*Figure 1. Secure traffic via the USSD gateway*

To ensure maximum security, the encryption keys will reside in a secure hardware security module (HSM) certified to FIPS 140-2 Level 3 certification.

4.3. Secure hosting

To maintain physical and IT security, the USSD gateway and HSM must be placed in an environment where maximum security is guaranteed. Only personnel accompanied by an auditor may have access to the physical machine. This means that the devices must be placed in a security vault at the very least.
5. Business Models

There are two primary business models for the use of the facility:

1. Financial institution pays per transaction

One business model is to provide the secure USSD service to financial institutions at a monthly fee accompanied with a transaction fee payable by the financial institution to the MNO.

2. Free facility in return for access to customer accounts for payment processing

Another business model that has a lot of merit, is to provide access to the secure USSD facility to an financial institution free of charge. The financial institution will in return provide the MNO with a simple way of debiting customer accounts, based on a model beneficial to both parties.
6. Operational impact of the secure facility

The secure facility uses carrier-grade equipment guaranteed to deliver maximum throughput and reliability.

6.1. SS7 integration

The physical interface to the core network is through a standard E1 link to an STP, as shown in the following diagram:

![Figure 2. SS7 integration](image)

The solution uses standard GSM interfaces for USSD. No development work is required in the MNO.

6.2. Support and Monitoring

All support and monitoring with regards to the availability of the system to financial institutions will be handled by PMT. There will be no impact to MNO operations. The only requirement is that an SLA must be signed between the MNO and PMT to ensure that any SS7-level issues can be handled if the need arises.

6.3. Financial transactions

PMT will handle the accumulation of financial transaction records and provide these to the MNO for billing purposes.
7. USSD Security

Security in a USSD application for financial services is paramount. The solution proposed in this document achieves end-to-end security by utilising different aspects and elements for each of the communication channels that are used. This is shown in the following diagram:

Figure 3. End-to-end encryption

7.1. USSD Communications

The communication between the handset and the USSD server is secure as it is encrypted on the GSM layer by means of the standard A2 algorithm.

Figure 4. Radio interface encryption

The A2 encryption ensures that each subscriber is authenticated and that his or her identity is ensured throughout the communication session. The A2 encryption secures the USSD communication between the handset and the MNO’s network while preventing interception or impersonation by third parties.

7.2. Transport data

Security on the transport layer is implemented by means of an encrypted link via Virtual Private Network (VPN) as shown in the next diagram:

Figure 5. Transport level encryption
7.3. Session data

Security on the session layer is implemented by means of encrypted Secure Socket Layer (SSL) as shown in the next diagram:

![Figure 6. Session level encryption](image)

The security of this layer is highly dependent on the protocol and available infrastructure of the specific MNO. Session layer encryption is easily implemented if the native protocol supports the Secure Session Layer.

7.4. PIN Encryption

The proposed solution can utilise existing PIN verification services, such as those used by Standard Bank. Alternatively, the proposal includes a dedicated PIN store that uses hardware security to maintain the PINs. The user PIN values are stored in an irreversible format in a secure database. A Prism Incognito Hardware Security Module handles the verification of PIN offsets.

![Figure 7. PIN management](image)
## Appendix A. Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FI</td>
<td>Financial Institution</td>
</tr>
<tr>
<td>FSP</td>
<td>Financial Services Provider</td>
</tr>
<tr>
<td>HLR</td>
<td>Home Location Register, a central database that contains details of each mobile phone subscriber that is authorised to use the GSM core network.</td>
</tr>
<tr>
<td>IMSI</td>
<td>International Mobile Subscriber Identity, a unique number associated with all GSM network mobile phone users. It is stored in the SIM inside the phone and is sent by the phone to the network.</td>
</tr>
<tr>
<td>MAP</td>
<td>Mobile Application Part, an SS7 protocol which provides an application layer for the various nodes in GSM mobile core networks to communicate with each other in order to provide services to mobile phone users.</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>MSISDN</td>
<td>Mobile Station International Subscriber Directory Number, a number uniquely identifying a subscription in a GSM mobile network. Simply put, it is the telephone number to the SIM card in a mobile/cellular phone.</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>SS7</td>
<td>Signalling System Number 7, a set of telephony signalling protocols which are used to set up most of the world’s public switched telephone network telephone calls.</td>
</tr>
<tr>
<td>USSD</td>
<td>Unstructured Supplementary Service Data</td>
</tr>
<tr>
<td>WASP</td>
<td>Wireless Application Service Provider</td>
</tr>
</tbody>
</table>