

# MicroSave Briefing Note # 67

## Choosing a Mobile Phone Banking Format

Ben Davis and John Owens

During the August 2008 *MicroSave*-CGAP workshop in Nepal, various m-banking providers shared the use of a range of communication formats supported on GSM networks, ranging from SMS (Short Messaging Service) through to HTTPS (internet). Each format has a number of advantages and disadvantages over the other potential formats.

The key issues faced when choosing which format to use include:

- *Usability/Reliability* – is the format easily adopted by customers?
- *Security* – how easy is it to intercept customer sensitive information for the purposes of committing fraud?
- *Ubiquity* – how many different types of phones generally used by the public support the communications format?

When evaluating these formats, m-banking/m-commerce providers need to always remember what type of service will be offered. Each transaction type has a range of characteristics that need to be supported by the communication formats. In most instances, ubiquity of the service is more important than the level of security capability of the m-banking/m-commerce provider's platform. This is because, internationally, transaction frequencies and amounts of lower income customers are in the low/medium risk category.

### Usability/Reliability

Voice has been used by financial services companies to service customers, using either a call centre operator or Interactive Voice Response (IVR) system, depending on the type of service being offered (credit applications or transaction queries vs. balance enquiries). One determining factor regarding the success of using this channel is the cost per transaction faced by the service provider (call centre, IVR platform, communications) and/or customer (communications) as well as the transactional functionality (supporting payments services for regular recipients have been successful, but not new recipient payments).

Initial m-commerce and m-banking platforms have provided services through USSD (Unstructured Supplemental Service Data) and SMS. Each type required customers to remember codes to initiate transactions, e.g. USSD requires the use of a format typically reflected in a set of \*, numbers and a # (\*140\*12345678#) that initiate a query. In the case of both USSD and SMS, the requirement that customer remember the codes for each transaction limited the usability of the platform. In the

past, m-payment transactions were limited since customers battled to remember what code to use for each type of transaction. To deal with this, m-banking and m-commerce providers generally have to provide users with quick reference guides to assist them in remembering the codes for various transactions.

USSD's advantage has been that it offers the most reliable communication format available as it is prioritised above all other communications formats offered by Mobile Network Operators (MNOs). Voice and SMS generally suffer from being second and third order priorities respectively on the network, (although SMS can be prioritised above voice). To handle issues related to this problem, some MNOs that offer mobile money services provide this service on a dedicated network that does not compete with regular voice and SMS traffic (for example Globe's GCASH).

Menu driven formats supported by USSD2 and WIG (Wireless Internet Gateway)/STK (SIM Tool Kit) have proven more user friendly for customers. The menus are either hosted on a central server and pushed to the phone or downloaded over-the-air (OTA) onto the phone and stored on the SIM (for example GCASH and SMART Money). Note, however, that in some markets pushing an STK menu onto low end phones is sometimes unreliable and therefore extensive and expensive SIM swaps are necessary. Depending on the completeness of the menu, customers may not need to know anything more than the PIN. However, depending on the configuration of WIG/STK, delays in the sending and receiving of secure SMS can affect service levels. USSD2 (being session based) can also suffer reduced service levels if sessions time out.

HTTPS services through WAP, GPRS, 2G formats and 3G formats (including HSDPA) offer access to internet level usability on the phone. The speed of GPRS can make website downloads slow; therefore, only EDGE, 3G and HSDPA are recommended for website downloads and these will only be used as MNOs upgrade their networks over the next few years.

### Security

Earlier formats tended to be less secure than more recently released formats. Voice, USSD1/2 and SMS are considered the most easily "hack-able"<sup>1</sup>. Encryption at the level of the network is either non-existent or very limited when compared to internet protocols. This has limited these formats usage for higher risk transaction types (non-designated recipient payments and card acquiring).

<sup>1</sup> One bank in South Africa using USSD2 technology has not experienced a single case of fraud on the platform. This was attributed mainly to the complexity of accessing the mobile phone banking application vs. other bank channels such as ATM & POS.

Transaction Types	Risk Profile	Typical Risk Mitigants
<b>Informational:</b> balance enquiries, mini statements	Low – information can be used to transfer value to other accounts	Identification PIN not the same as ATM/debit card PIN
<b>Low value transactions:</b> prepaid services – water, power, airtime	Medium – information can be used to transfer value to other accounts	Identification PIN not the same as ATM/debit card PIN
<b>High value (designated recipients):</b> supplier payments; salary payments; regular recipient payments	Medium – information can be used to transfer value to other accounts	Identification PIN not the same as ATM/debit card PIN
<b>High value (undesigned recipients):</b> non-regular recipient payments; card acquiring	High – information used to initiate these transactions can be used to defraud customers, most mobile phones are not 3DES compliant (do not offer security levels of a POS)	Mobile phone security upped by the use of WIG/STK or internet protocols – ideally encryption keys are hardwired onto SIM; card acquiring limited to 1 card per phone – phone becomes “personal key entry device”; undesigned recipients can become designated through verification of customer ID

### Ubiquity

Certain formats are not supported on phones. HTTPS, for example, is only available on higher end internet enabled phones. Workshop participants estimated that only 20% of mobile phones in India had internet capability, and, of those, between 20-30% had enabled their mobile phones for internet service. Providing banking services in this format would limit immediate take-up to 6% of the potential market, with the majority of users belonging to higher income bracket.

While the global trend towards HTTPS enabled mobile phones is positive and rapid, it is likely that lower income segments of society will not own HTTPS enabled mobile phones during the next 3-5 years. M-commerce and M-banking providers are therefore required to address demand from lower income segments through other formats such as WIG/STK and USSD2.

<sup>2</sup> Bank of the Philippines Islands with Globe (Philippines), Banco de Oro with SMART (Philippines), Kookmin Bank and several smaller banks with SK Telecom (South Korea). It should be noted that these partnerships are often influenced by the regulatory environment and have been more challenging in some markets, especially in Africa.

In the case of WIG/STK, the control of the SIM is required in order to load these applications onto the mobile phone. While in the past, MNOs have generally not provided access to SIMs to third-parties, partnerships between MNOs and banks are beginning to take place, especially in Asia<sup>2</sup>. This effectively allows the MNO to restrict access to the network to those banks with which it has partnered. In these cases, however, the potential penetration of m-commerce and m-banking services will be limited to the market share of the network’s customer base. In countries such as the Philippines where there are only two major MNOs, banks can easily partner with both operators. In more fragmented markets, with smaller, multiple MNOs, this may be more on an issue.

USSD2 requires less direct intervention from MNOs (MNOs need only enable the USSD2 channel – an issue for MNOs who sometimes do not have a billing module for USSD2, or who are looking to block third party providers). This opens the channel to third-party providers such as banks and payments aggregators. Once the channel is open, potential market penetration is limited to the potential market size. In the case of a bank provider, this would be the percentage of customers with mobile phones that the bank is able to target. For payment aggregator businesses, penetration using USSD2 could be 100% of the mobile phone subscriber market if a card based acquiring platform is used by 100% of the banked market. Joint ventures and partnerships (see Briefing Note # 68) between MNOs and banks or networks of small MFIs using WIG/STK channels will probably be more effective in the long run to reach un/underbanked customers.

### Concluding remarks

While the trend towards mobile phones supporting HTTPS is expected to be rapid, the medium-term outlook is that financial service providers will be required to use USSD, SMS and STK formats to provide access to lower income customers.

The type of communication format used is to a certain extent determined by the providers’ status as a MNO, bank, third party service providers or joint venture between MNO-bank-MFI. MNOs have greater flexibility in terms of which format to use to service their customers, while banks and third party service providers typically default to USSD1/2/SMS/WIG STK solutions.

Key determinants of which format to use will depend on what services the provider is looking to offer. Security of transactions should be traded off against who the target customers are, and what types of transactions they will make.