Bogotá, D.C., Noviembre 6 de 2013

Doctor
CARLOS PABLO MÁRQUEZ ESCOBAR
Director Ejecutivo
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Calle 59ª Bis No. 5 – 53 Edificio Link Siete Sesenta Pisos 8, 9 y 10.
sfm@crcom.gov.co
Ciudad

Ref.: Comentarios al proyecto regulatorio "Promoción de servicios financieros sobre redes móviles y medidas complementarias para provisión de contenidos y aplicaciones"

Respetado doctor Márquez:

A continuación encontrará los comentarios generales y particulares de COMCEL S.A. al documento soporte y a la propuesta regulatoria mediante la cual se pone en conocimiento del sector el proyecto de modificación de las condiciones establecidas en las Resoluciones CRC 3066, 3496, 3500 y 3501 de 2011 en relación con la promoción de los servicios financieros sobre redes móviles.

I. COMENTARIOS GENERALES DOCUMENTO SOPORTE

En primer lugar, debemos llamar la atención de la CRC sobre el limitado y análisis que se hace en el documento comentado, el cual adolece de un estudio de mercado sólido, que evalúe elementos como la penetración de la banca móvil, las condiciones de competencia existentes o la presencia de supuestas fallas de mercado, que soporten las conclusiones en que erróneamente se basa el proyecto para justificar las modificaciones regulatorias propuestas.

En este sentido, es importante resaltar que conforme al estudio de Deloitte citado en el propio documento soporte, Colombia es el tercer país en América Latina, con mayor penetración de servicios de Banca Móvil, por lo que las

medidas regulatorias propuestas no parecen responder a la realidad del mercado.

I.I. Estudios de Tecnología

En relación con la valoración tecnológica realizada por la CRC y específicamente en lo referido a los canales para la implementación de banca móvil, como el IVR, SMS, USSD, WAP, STK entre otros, la propuesta regulatoria erróneamente plantea desventajas de seguridad y asume deficiencias y limitaciones que se alejan de la realidad tecnológica:

USSD

La propuesta se inclina a favorecer una tecnología específica (USS D), estando claramente en contravía con lo dispuesto en los principios orientadores de la Ley 1341 de 2009, y en especial el de neutralidad tecnológica.

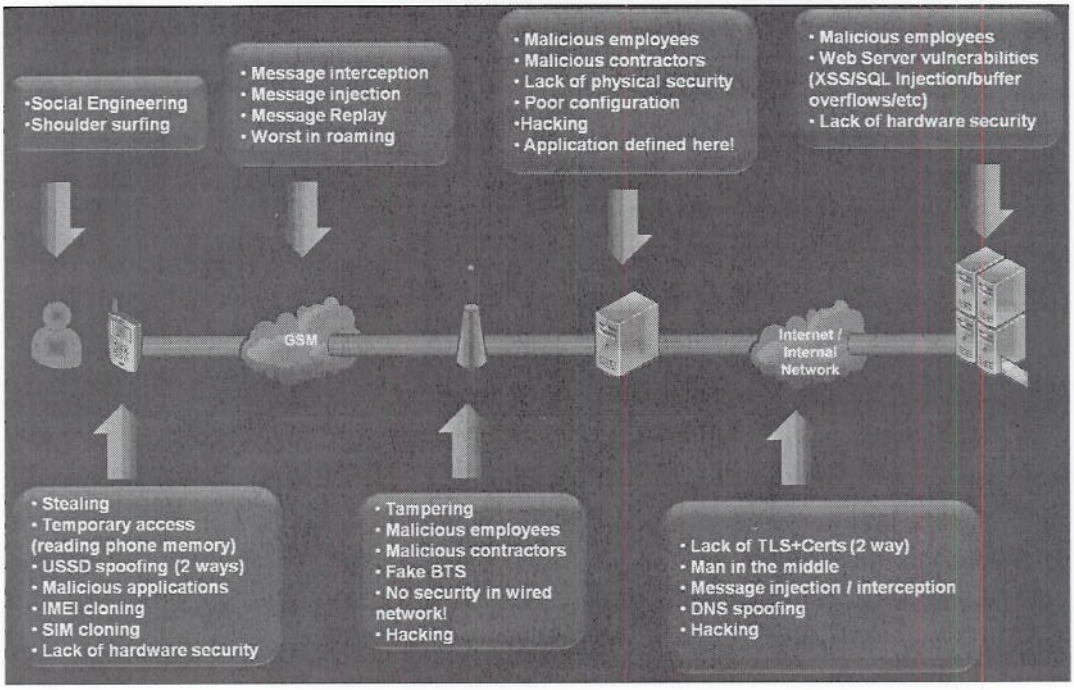
La CRC dispone en el documento soporte lo siguiente:

"(…). De acuerdo con los reportes de información a los que se acaba de hacer referencia, ***los PRST móviles no han permitido el uso masivo de la tecnología USSD, que, como se vio, ha sido exitosa en otras jurisdicciones y que desde la perspectiva de algunos integradores y redes de bajo valor*** *puede hacer mucho por la masificación de los servicios de Banca Móvil. (…)"* (Negrilla fuera de texto)

La anterior transcripción evidencia un contrasentido respecto de lo establecido en la Ley 1341 la cual dispone sobre Neutralidad Tecnológica: *"El Estado* ***garantizará la libre adopción de tecnologías, teniendo en cuenta recomendaciones****, conceptos y normativas de los* ***organismos internacionales competentes e idóneos*** *en la materia, que permitan fomentar la* ***eficiente prestación de servicios, contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones*** *y garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible."* (Negrilla fuera de texto).

Así las cosas, ni el documento soporte ni la propuesta regulatoria contienen un estudio técnico idóneo que valore la conveniencia ni el impacto de la tecnología USSD en las condiciones de seguridad, ni las consecuencias asociadas al diseño de la infraestructura que implicaría la implementación de esta tecnología o su impacto en la calidad de los servicios de telecomunicaciones prestados sobre la misma infraestructura.

Es importante que la CRC realice un análisis más profundo de las condiciones de seguridad requeridas en la implementación de servicios móviles financieros, para evitar adoptar medidas que puedan generar riesgos innecesarios para todo el ecosistema, incluidos los bancos, los usuarios y los PRSTM. Al respecto y a modo de ejemplo se adjunta la siguiente gráfica tomada de un estudio técnico del uso de USSD en la Banca Móvil realizado por la firma GEMALTO[1] que presenta vulnerabilidades de dicha tecnología para soportar servicios financieros:



Se desataca que conforme al estudio mencionado, USSD se basa en el mecanismo de seguridad del plano de señalización GSM/UMTS.

[1] GEMALTO. USSD vulnerability assessment. Julio de 2010. Versión 1.0.

La firma Gemalto, concluye que USSD dentro de la red interna es susceptible de sufrir muchos de los ataques que se presentan en otros servicios de Internet, tales como la comunicación desde la puerta de enlace de USSD al servidor financiero (*Bank backend or Mobile Wallet*) el cual se hace sobre protocolos de Internet y, a menudo con HTTP.

Algunas de las amenazas identificadas en este entorno son:

- La falta de uso de TLS en la comunicación entre los servidores, que permite a un atacante inyectar mensajes fácilmente.

- La falta de certificados de TLS.

- Envenenamiento de DNS cuando el servidor remoto financiero reside en otra red o incluso dentro de la red cuando se utiliza DNS (o WINS de Windows o NBNS).

- La red de piratería informática habitual.

En razón de lo anterior, es importante que la CRC analice a profundidad su inclinación hacia una tecnología en particular y valide la existencia de condiciones de seguridad requeridas en aplicaciones financieras.

Por otro lado, la propuesta no parece considerar lo dispuesto en la Resolución 3067 de 2011(y sus respectivas modificaciones), la cual señala las condiciones de seguridad en la red que deben adoptar tanto los PRSTM como los PCA, conforme a los marcos de seguridad definidos por la UIT en las recomendaciones a las series X800 de autenticación, acceso, no repudio, confidencialidad e integridad entre otros.

SMS

También es preciso aclarar que, sin soporte evidente, la propuesta plantea riesgos e inconvenientes asociados a la implementación de los servicios mencionadas a través de mensajes de texto (SMS), como supuestos problemas de acceso al menú de las tarjetas SIM. Este planteamiento carece de fundamento, ya que, al menos en el caso puntual de COMCEL, el paso a producción de los bancos con aplicación de Banca Móvil, se visualiza en todas

las tarjetas SIM de perfil 4 y superiores, que son prácticamente el 100% de las tarjetas activas.

Así las cosas, es desacertado afirmar que dicha funcionalidad es controlada por los fabricantes de tarjetas SIM y que por tanto existen inconvenientes en los acceso a través de la tarjeta SIM.

En respaldo de las anteriores afirmaciones, se adjuntan al presente documento los estudios realizados por "*Alliance for Financial Inclusion de 2013*", y "*Analysis of Mobile Infrastructure for Secure Mobile Payments de 2008*", que corroboran los argumentos anteriormente esgrimidos.

La Circular Básica Jurídica 80 de la Superintendencia Financiera, modificada por la Circular Externa 42 de 2012, indica que se debe contar con "mecanismos de autenticación de dos (2), factores para la realización de operaciones monetarias y no monetarias".

En este sentido y si bien la superintendencia indica que no es requerido realizar cifrado de la información para operaciones inferiores a dos (2) SMMLV, también indica que *"la entidad deberá adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe considerar los mecanismos de seguridad en donde la información no se encuentre cifrada. La Superintendencia Financiera de Colombia (SFC) podrá suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información*".

En virtud de lo anterior, la CRC debe considerar la regulación existente en materia de seguridad, previo a establecer la tecnología mediante la cual se deben soportar las transacciones financieras. Cualquier falla de seguridad que se genere soportada en esta regulación, afectará no solo a la entidad bancaria que preste el servicio sino también al operador a quien el usuario identificará como el prestador de un canal con deficiencias en seguridad.

I.II. Modelos de los negocios actuales

La CRC afirma en el documento soporte *"(...)* ***En la actualidad el negocio de banca móvil en Colombia se basa en dos tecnologías remotas: STK y SMS,*** *y se fundamentan en un modelo aditivo donde el control de los clientes y de las diversas operaciones la tiene el sector financiero, siendo el canal móvil una adición a la oferta de distribución de los otros canales de servicios de la entidad (oficinas, cajeros, Internet, etc.) En este esquema, la comunicación entre las entidades financieras, los operadores móviles y los clientes se hace a través de las plataformas de las redes de pago de bajo valor que facilitan y agrupan las entidades financieras para negociar paquetes de SMS por volumen.*

3.5. Tarifas

En Colombia se puede observar que en la actualidad los operadores tienen diferentes sistemas y tarifas que dependen del uso de la tecnología que se utilice

- *En la utilización de STK se permite que los clientes de los bancos realicen transacciones financieras y no financieras para administrar y controlar los productos y servicios ofrecidos por la entidad. En este esquema, el banco paga por las transacciones cobrables y técnicamente exitosas una tarifa de* ***$50 por transacción a la red de bajo valor +*** *el costo de transacción del operador (rango de transacciones) + IVA.*

- *Para los SMS de notificaciones y alertas en una y dos vías que buscan informar, alertar y generar una acción particular sobre el cliente receptor, se utilizan SMS. Estas alertas y notificaciones pueden ser enviadas en línea o por lotes a través de un mismo motor de envío y el uso de interfaces y desarrollos de impacto tecnológico mínimo para las entidades financieras. El banco paga* ***una tarifa de $23,96 por mensaje a la red de bajo valor +*** *el costo del operador (rango de transacciones) + IVA (el contenido del mensaje puede ser informativo o comercial)."* (Negrilla fuera de texto)

Conforme a lo anteriormente trascrito, existe un participante en la cadena de valor de la banca móvil, de alta importancia, como es la **RED DE BAJO**

VALOR, con influencia determinante en los costos finales a la banca y al usuario final y que no está siendo considerado dentro del análisis realizado por la CRC.

Este punto resulta altamente relevante, teniendo en cuenta que la misma Comisión reconoce que la red de bajo valor de mayor tamaño (Redeban), reportó información exclusivamente para diciembre con COMCEL y con inconsistencias,[2] lo cual hace que la propuesta regulatoria requiera información adicional para realizar una valoración precisa, previa la expedición de una regulación con las implicaciones del presente proyecto.

Ni el documento soporte ni la propuesta consideran que existen transacciones que el PRSTM no cobra, pero que la Red de pago de bajo valor si cobra a los bancos, como por ejemplo la recarga y pago de facturas en el caso de COMCEL.

Así las cosas, el sumario análisis realizado por la CRC no contempla la realidad del negocio ni considera la totalidad de los costos y fuentes de ingreso asociados a cada uno de los agentes de la cadena de valor.

I.III. Regulación de Tarifas en función de Cargos de Acceso

El proyecto regulatorio propone la extensión del precio regulado de los cargos de acceso de SMS, para ciertas relaciones comerciales entre los proveedores de redes y servicios de telecomunicaciones (PRST) móviles y terceros, lo cual genera los siguientes inconvenientes:

I.III.I. Regulación de Precios de los Servicios de Telecomunicaciones

El proyecto, al proponer la regulación del precio de los SMS, excede los límites legales y las disposiciones regulatorias que garantizan la libertad tarifaria y la fijación **excepcional** de precios por parte del regulador:

---

[2] Comisión de Regulación de Comunicaciones. Documento Soporte. "Promoción de servicios financieros sobre redes móviles y medidas complementarias para provisión de contenidos y aplicaciones" Página 101.

1. El artículo 23 de la Ley 1341 de 2009 establece: *"**Los proveedores de redes y servicios de telecomunicaciones podrán fijar libremente los precios al usuario. La Comisión de Regulación de Comunicaciones sólo podrá regular estos precios cuando no haya suficiente competencia, se presente una falla de mercado** o cuando la calidad de los servicios ofrecidos no se ajuste a los niveles exigidos, lo anterior mediante el cumplimiento de los procedimientos establecidos por la presente Ley."* (Negrilla fuera de texto)

2. Por su parte, la Resolución 2058 de 2009, estableció los criterios que debe tener en cuenta la CRC para determinar mercados relevantes sujetos a regulación ex ante.

La metodología establecida en la regulación sobre la definición de mercados relevantes, es fundamental para la expedición de regulación ex ante o cualquier intervención regulatoria que amerite con ocasión de una falla de mercado:

"(...) Que la regulación ex ante, entendida como aquélla que se expide en orden a promover la competencia en el mercado, así como corregir las fallas que se presenten en el mismo es una herramienta primordial de intervención estatal en la economía para garantizar condiciones homogéneas y económicamente viables para el normal desarrollo de la competencia efectiva en aquellos mercados que dados sus problemas de competencia, ameriten dicha intervención. (...)"[3]

En virtud de lo anterior, la Comisión estableció los criterios para intervención de precios que debe observar en el presente caso, toda vez que en el evento que se establezca el mercado relevante que a la fecha no se ha establecido, el mismo debe estar fundamentado en los siguientes principios:

1. Promoción de la Competencia

La regulación debe propender por un entorno competitivo, basado en un mercado equitativo; sin embargo, lo que se evidencia en la propuesta regulatoria, es una regulación de precios que en principio favorece exclusivamente al sector financiero, sin considerar costos o los agentes involucrados en la cadena de valor.

[3] Resolución CRC 2058 de 2009. Parte Considerativa.

2. **Protección de los derechos de los usuarios.**

La Comisión debe propender por la protección de los derechos de los usuarios, pero ninguno de los fundamentos del documento que soporta la presente propuesta regulatoria, parece estar alineado con este principio, toda vez que la regulación de precios propuesta no garantiza que la tarifa de usuarios financieros disminuya, pero si garantiza que mayores costos sean asumidos por el sector de telecomunicaciones, estando en contravía de los principios primordiales que la Comisión de promover.

3. **Promoción de la inversión**

Teniendo en cuenta que los costos asociados a la prestación del servicio para los PRSTM no se recuperan con la tarifa regulada por la Comisión, es evidente que la inversión que se ha venido realizando para promocionar el servicio de banca móvil se verá altamente afectada en la medida que dicha infraestructura se torna insostenible y sin ningún incentivo para su promoción.

De otra parte, existen criterios para determinar mercados de servicios de telecomunicaciones sujetos a regulación *Ex ante*, que no se encuentran desarrollados por la comisión a saber:

1. **Análisis actual de las condiciones de competencia en el mercado**

La regulación establece que se debe realizar un análisis de organización industrial, barreras de entradas técnicas, económicas y normativas dentro de un ámbito geográfico para evidenciar la existencia de fallas de mercado, estudio que no se ha realizado por parte de la Comisión, máxime cuando no ha considerado todos los agentes de la cadena de valor del mercado que es objeto del proyecto regulatorio.

2. **Potencial de competencia en el corto y mediano plazo**

La Comisión debe revisar si en un horizonte de corto o mediano plazo se intensifica la competencia en el mercado; sin embargo, en la presente propuesta no generaría un efecto de promoción de la competencia como se resaltó previamente, pudiendo incluso resultar en un beneficio injustificado

(aumento del margen) para el sector financiero y en un detrimento injustificado para el sector de telecomunicaciones, que se enfrentaría a tarifas reguladas que no le permitirían siquiera recuperar sus costos a corto o mediano plazo.

3. Aplicación del derecho de competencia

No ha sido puesto a disposición del sector un estudio que evidencia una falla de mercado que justifique una medida intervencionista como la propuesta. Por el contrario, como se demostrará más adelante, la propuesta como se ha presentado, podría generar una falla de mercado al fijar tarifas máximas que no permitan recuperar costos asociados a la prestación del servicio.

De otra parte, la Resolución 2058 de 2009, establece la lista de mercados relevantes susceptibles de regulación ex ante, en los que no se encuentra el mercado objeto de análisis. El Anexo 02 establece el siguiente listado:

- Voz saliente móvil
- Terminación de llamadas fijo – móvil en todo el territorio nacional
- Mercado Mayorista de terminación de llamadas fijo – fijo en cada municipio del país.
- Mercado Mayorista de terminación de llamadas móvil – móvil en todo el territorio nacional.
- Mercado Mayorista de terminación de llamadas de larga distancia internacional en todo el territorio nacional.

La propuesta bajo estudio no ha dado cumplimiento a los procedimientos establecidos en la Ley, pues de no se ha puesto en conocimiento ningún estudio de mercados relevantes ni se cuenta con un estudio sólido del mercado que sugiera falta de competencia o la existencia de alguna falla que merezca la intervención del regulador.

En virtud de lo antes mencionado, la intervención tarifaria propuesta desconoce las garantías legales y omite los procedimientos establecidos, vulnerando el principio de libertad tarifaria previsto en la ley.

Sin perjuicio de lo antes expuesto, es preciso advertir que la regulación de precios a los PRSTM no resulta en una reducción de la tarifa que el banco le cobra al usuario final, como erróneamente se ha manifestado en diferentes medios de comunicación, incluso antes de la retroalimentación y comentarios del sector del presente proyecto, toda vez que en la fijación de la tarifa

intervienen diferentes agentes en la cadena de valor, que no quedarían alcanzados por las medidas propuestas en el proyecto.

Para concluir, se reitera que no se ha puesto a consideración del sector un estudio de mercados relevantes ni un estudio sólido que sugiera la falta de competencia o una supuesta falla en el mercado relevante (el cual no ha sido definido), omitiendo la CRC de los presupuestos legales necesarios para avanzar en una intervención de precios, que se reitera, debe ser una medida excepcional. Por el contrario, la propuesta de intervención parece fundarse en la promoción de la banca móvil, desconociendo que la medida propuesta afectaría la relación comercial de los PRSTM con integradores, agregadores, y otros proveedores, los cuales envían notificaciones hacia usuarios móviles de la red de COMCEL y que incluso tienen la posibilidad de hacer que COMCEL los entregue a una tercera red de otro PRSTM.

Este evento cobra especial relevancia, en la medida que según el modelo propuesto, la tarifa máxima que podría cobrarse es el cargo de interconexión, desconociendo la condiciones particulares de las relaciones comerciales con los PCA, como sería el caso de la solicitud de entrega del tráfico a la red de otro PRSTM, caso en el cual se causaría un cargo de acceso que no estaría considerado en la medida regulatoria propuesta, imponiendo al PRSTM un precio máximo que no cubriría los costos asociados a la transacción.

Finalmente, debe advertirse que los precios tomados como referencia en la propuesta regulatoria (precio del cargo de acceso o interconexión), fueron fijados para el marco de la relación de interconexión de tráfico de SMS entre los PRSTM, considerando incluso una senda de reducción con una tendencia del precio hacia cero (0). Las condiciones económicas y de competencia evaluadas para definir el cargo de interconexión para el intercambio de SMS y la evolución del mismo en el tiempo, difieren de aquellas presentes en el envío de SMS por parte de terceros agentes como agregadores, integradores o prestadores de servicios financieros, que involucran condiciones comerciales, costos y componentes de red claramente disímiles en comparación con los existentes en la interconexión, lo cual conduciría a una falla de mercado, pero derivada de la regulación.

I.III.II. Costos no contemplados en el análisis

Es preciso tener en cuenta que la CRC ha venido utilizando la metodología de Costos Incrementales de Largo Plazo por elementos o LRIC+ en sus modelos de definición de cargos de acceso para redes móviles, tanto a nivel de Voz como de SMS, donde el cargo de acceso se obtiene en términos metodológicos de la división entre los costos totales y la demanda total.

De esta forma el Costo Total de Largo Plazo se obtiene de la suma de tres factores: el costo de la inversión, la depreciación por la tasa de tributación y los gastos ponderados por el complemento de la tasa de tributación, lo cual se lleva a valor presente y se le resta el valor residual de los elementos, en el año final. Para obtener el valor del Cargo de Acceso se divide por la demanda total (es decir incluyendo reposición) a través de los 5 años de evaluación, respectivamente para estimar la tarifa correspondiente al CTLP por unidad.

Para el 2011, la CRC realizó una variación sobre el modelo y utilizó la metodología LRIC Puro o Costo Incremental por Servicio (CI). Esta variación se obtiene a través de la comparación entre una empresa que provee el servicio de voz de acceso y una empresa que no lo provee determinando así los costos incrementales necesarios para brindar el servicio, metodología que la CRC en la Resolución 3500 del 2011 aplicó a la determinación de los Cargos de Acceso de SMS.

Ahora bien, una vez aclarado lo anterior, se evidencia que la CRC en su análisis primario, no tuvo en cuenta que para los SMS derivados de este tipo de servicios, **se utilizan elementos de red diferentes de los normalmente utilizados en la interconexión, tales como codificadores y encriptadores** entre otros.

En virtud de lo anterior y con el fin de colaborar con el sistema financiero, COMCEL ha implementado infraestructura que cumple con altas medidas de seguridad las cuales permiten mitigar los riesgos de amenazas tecnológicas en las transacciones financieras para propender por la confidencialidad, integridad, disponibilidad, autenticación e irrefutabilidad entre otros.

Los SMS pueden ser utilizados para realizar pagos móviles, pero deben estar asociados a aplicaciones Java o clientes desarrollados en STK (Sim Toolkit),

con el fin de que se puedan generar transacciones sobre SMS con encripción *end to end*.

De igual manera existen otros costos asociados que no se encuentran en las relaciones de interconexión con otros proveedores, que no han sido considerados en la propuesta regulatoria y que son acordados entre las partes al definir el valor final del precio del mensaje, tales como los costos asociados a publicidad, mercadeo, distribución etc.

Aunado a lo anterior, el proyecto prevé la obligación del PRSTM de dar traslado al PCA de las solicitudes relativas a la provisión de contenidos y aplicaciones cuando las mismas no se refieran a los servicios de telecomunicaciones, en virtud de lo anterior, el traslado de dichas solicitudes son un costo que no se podrá recuperar y que no se encuentra establecido dentro del análisis de costos de interconexión. De igual manera es pertinente aclarar que el responsable de la atención de solicitudes es el PCA y reconocer que una cosa son solicitudes y otra PQR.

En este orden de ideas, es preciso que el regulador, luego de cumplir con los presupuestos legales necesarios para proceder a la fijación de una tarifa, considere que las tarifas negociadas con estos proveedores pueden ser diferenciales e incluso superiores al valor del cargo de acceso establecido, toda vez que involucran elementos especiales y servicios adicionales a los involucrados en la relación de interconexión, como los derivados de la **seguridad de la información que se está transmitiendo**, y que dichos elementos no han sido considerados ni puestos a consideración del sector en un estudio de mercado que soporta la medida regulatoria bajo análisis.

Por ejemplo, el servicio de Banca Móvil hace uso de una plataforma que hace que la información viaje encriptada y tenga seguridad de extremo a extremo. En consecuencia, las Sim Card poseen en su menú de servicio de VIVE TU SIM, la opción de "MIS BANCOS" la cual es una solución confiable y segura, que incluye una aplicación (software: cliente SIM) almacenada en la tarjeta SIM (Módulo de Identidad del Suscriptor), un servidor (Secure Server Platform - SSP) y un software que interpreta los mensajes que se intercambian entre los bancos o redes de pago de bajo valor y la SIM.

La solución implementa un esquema de seguridad en todo el proceso de la transacción, desde la codificación de los mensajes que se envían desde la tarjeta SIM hasta la decodificación en el servidor de los bancos o Redes de bajo Valor que los traduce al formato específico de cada uno. El proceso de codificación/decodificación se realiza por medio del manejo de llaves transaccionales que en línea con el estándar EMV, hace uso de una llave diferente por cada transacción realizada por el usuario. La información es cifrada de extremo a extremo y tiene doble factor de autenticación (donde el usuario comprueba su identidad al proveer con dos métodos de autenticación para toda transacción realizada: el PIN – algo que el usuario conoce, y la SIM – algo que el usuario tiene).

Este servicio tiene una plataforma en el operador llamada Transaction Router (TR) que se comunica de manera segura (mediante VPN y HTTPs) con la otra parte de la plataforma "Secure Server Platform" (SSP). Estas redes y plataformas a su vez se encargan de interactuar con el banco y permitir o no la autorización de las operaciones financieras, resultando en elementos y servicios adicionales a los involucrados en el intercambio de SMS en una relación de interconexión y que se **reitera** no aparecen considerados dentro de la cadena de valor expuesta por la CRC.

Esta realidad parece ser admitida en la propuesta regulatoria que deja abierta a libre negociación entre los involucrados, para la definición de las condiciones y valores a través de mensajes multimedia (MMS) y/o mensajes a través del servicio suplementario de datos no estructurados (USSD), principio que no debería variar cuando el mecanismo utilizado sea el envío de SMS que se reitera, no puede asimilarse a un simple "uso de red".

Por otro lado, es preciso advertir que desde la perspectiva de una entidad financiera, el servicio de Banca Móvil tiene dos costos; el costo de los mensajes cobrados por el operador y el costo por servicio de administración de la Red de pago de Bajo Valor. **Del valor total que paga en la actualidad un banco por el servicio de Banca Móvil, aproximadamente el 68% lo representa el valor que cobra la red de pago de bajo valor (cifras tomadas del valor cobrado por Redeban), y el 32% el valor cobrado por el operador.** Si bien es un objetivo de todos reducir los costos para que el esquema de bancarización llegue de forma efectiva a la población, se debe revisar los costos de toda la cadena de valor involucrada en el servicio.

Por ejemplo, en la actualidad Redeban cobra $50 por cada transacción, valor fijo independiente del volumen de las transacciones y sin importar si las transacciones son o no cobradas por el PRSTM (como sería el caso de las transacciones de recarga prepago y pago de factura que no son cobradas por COMCEL).

I.III.III. Aspectos relacionados con los precios

El documento soporte parte de una premisa errónea *"(...) En primer lugar, existe una diferenciación entre los SMS en función del tipo de transacción. De acuerdo con lo anterior, el valor del tráfico SMS se supedita al* ***tipo de transacción*** *o al propósito de uso de dicho tráfico, pese a referirse recursos de red similares. Así mismo, se encuentran ostensibles diferencias en los valores a cobrar por parte de los proveedores. (...)"* (Negrilla fuera de texto)

En el caso particular de COMCEL las tarifas de mensajes se ofrecen en función del volumen, no del tipo de uso como erróneamente lo sugiere la propuesta regulatoria. De otra parte, la propuesta regulatoria hace referencia a la información que se suministró por parte de los proveedores, sin embargo en las dimensiones de precio, existen valores que no concuerdan con las ofertas (OBI de SMS), situación que refleja inconsistencias en el análisis realizado dentro del proyecto regulatorio.

I.III.IV. Modificación unilateral de las condiciones de tasación y tarificación

El documento soporte dispone *"(...) Al respecto, ASOBANCARIA afirma que la modificación de estas condiciones representaría un incremento en las tarifas de los servicios de mensajería de texto, entre el 700% y el 1.300%.".*

En este sentido, es preciso aclarar que dicha información es incorrecta en la medida que como se informó anteriormente, el proyecto no está soportado en un estudio que contemple los costos asociados a la red de pago de bajo valor, que como se indicó, hacen parte de la cadena de valor y constituye un factor de costos que incide de manera determinante en la tarifa final. Por otro lado, la

afirmación realizada por ASOBANCARIA es anterior a la negociación comercial realizada en los meses de octubre de 2012, que produjo una reducción de las tarifas de SMS de aproximadamente el 51%, y considerada con dos reducciones más de tarifas, acumula una baja de aproximadamente el 73%.

De otra parte la CRC realiza la siguiente afirmación en el documento soporte:

"(...) En relación con este asunto, la Asobancaria y otros agentes involucrados se han referido a la propuesta en el cambio de las condiciones para proveer el acceso, principalmente en el caso de la provisión de servicios de banca móvil sobre SMS, propiciada por la empresa que opera bajo la marca Claro.

Esta modificación comprende la variación del esquema de cobro, en virtud de la cual se migra de un pago por transacción con independencia del número de SMS involucrados en las mismas (valor global), hacia un cobro por unidades de SMS utilizadas en la transacción.

Al respecto, en carta enviada a la Superintendencia Financiera, la presidente de este gremio, María Mercedes Cuellar, advierte que la masificación de la banca móvil en el país enfrenta un importante riesgo como resultado de las nuevas condiciones que propone el proveedor de telecomunicaciones móviles Claro, para la prestación del servicio de transacciones a través de la SIM Card, pues "pone en grave riesgo no solo la prestación de servicios ya existentes, sino la innovación, generación y desarrollo de nuevos productos", pues señala que "lo que antes era un valor global ahora se transformará en un valor que se debe multiplicar por 4 (en el caso de consultas de saldo) o por catorce (en el caso de pagos), dependiendo de la transacción".

Esta posición puede ser concordante con la posición de este proveedor según la cual existe el interés de este proveedor de efectuar una revisión del esquema de tarifas (de cobro por transacción a cobro por SMS) con miras a "racionalizar" el uso de recursos de red, dada la preocupación de este proveedor frente a la existencia de transacciones que involucran hasta 13 mensajes por transacción.

En relación con los demás proveedores de telecomunicaciones no se han presentado comentarios en este sentido. (...)"

En este punto es preciso realizar las siguientes aclaraciones para efectos de entender el contexto en que se presenta la preocupación de COMCEL con relación al uso de su red:

En primer término, se debe tener presente que las distintas transacciones de banca móvil involucran el envío de entre 2 y 18 SMS, y por tanto el modelo de banca móvil con las redes de pago de bajo valor genera una presión insostenible en el uso de recursos de red, en tanto la proporción en transacciones VS tráfico es de 1: 3,18.

Para propósitos de ilustración, bancos como Davivienda y Bancolombia, hicieron desarrollos de aplicaciones que posteriormente se alojaron en el menú de las tarjetas SIM para ofrecer productos tales como "Daviplata" y "Ahorro a la Mano", respectivamente. Al ser diferentes a las aplicaciones estándar, es decir, "aplicaciones de transacciones dinámicas", se multiplicó el número de SMS por transacción, pasando de un proceso de registro en la aplicación estática de 7 SMS, al mismo registro de hasta con 18 SMS en la aplicación dinámica: Por ejemplo, la consulta del saldo, en el proceso estático demanda 2 SMS mientras que en el dinámico utiliza 14 SMS.

En virtud de lo anterior, se imponía la necesidad de racionalizar la cantidad de SMS por transacción para hacer un mejor uso de los recursos de red, resultando necesario sensibilizar a los bancos y a las redes de pago de bajo valor, sobre la importancia de las transacciones y la cantidad de SMSs involucrados, pues su única preocupación radicaba en el menú y en las funcionalidades de la aplicación.

Como consecuencia de esta situación, hace más de 12 meses se generó un plan de trabajo, que ha derivado en la identificación e implementación de mejores prácticas que han permitido a las entidades financieras procesar más transacciones con menos mensajes de texto, haciendo al ecosistema más eficiente y productivo, manteniendo las funcionalidades y reduciendo la cantidad de SMS necesarios por transacción. Por ejemplo, para la transacción de Pago Proveedores - Daviplata, antes de la implementación de las mejores prácticas se requerían 9 SMS, mientras que en la actualidad se usan 2 SMS.

Esta explicación resulta relevante en el marco de la propuesta regulatoria, pues resalta la importancia de mantener el esquema de la libertad en la negociación

y fijación del precio por transacción entre las partes, que ha permitido, como se demostró, la identificación e implementación de mejores prácticas comerciales. La fijación de una valor máximo por SMS elimina los incentivos a las redes de pago de bajo valor y a los bancos, de desplegar aplicaciones que hagan un uso eficiente de la las redes de comunicaciones móviles, pudiendo generar saturación de uso de la red y afectación en la calidad de otros servicios y aplicaciones que utilizan los mismos recursos. No resulta irrelevante en este punto, recordar las innumerables regulaciones recientemente expedidas por la CRC que imponen obligaciones de envió de SMS, generando una carga adicional a las redes y recursos involucrados en el envío y recepción de SMS.

En virtud de lo anterior, es preciso que antes de proponer medidas regulatorias la CRC elabore y socialice con el sector, un estudio comprensivo que considere aspectos fundamentales como los anteriormente expuestos.

I.V. Regulación multisectorial y OCDE

La misma propuesta regulatoria reconoce que debe existir una regulación multisectorial:

"(...) Ahora bien, en este punto no puede perderse de vista que la efectividad de las medidas propuestas en la promoción de la provisión de servicios financieros que hagan uso de las redes móviles y demás contenidos y aplicaciones, ***debe estar acompañada de una regulación multisectorial que le permita efectivamente al usuario o consumidor de dichos servicios acceder tales servicios a unos costos razonables,*** *no sólo desde el punto de vista de la infraestructura de telecomunicaciones, sino también desde las respuestas que sectores, como el bancario y actividades conexa, beneficiarios de la reducción del costo mayorista de insumo cada vez más importante en sus actividades conexas, beneficiarios de la reducción del costo mayorista de un insumo cada vez más importante en sus actividades, ofrezcan en sus propios sectores, en términos de cobertura e inclusión respecto de sus servicios. (...)"*

Es evidente que la OCDE reconoce la importancia de una regulación que considere todos los elementos asociados en la prestación de estos servicios procurando un balance en la cadena de valor, de manera que los beneficios sean efectivamente trasladados al usuario.

Como se pudo explicar en los capítulos anteriores, el proyecto de regulación no contempla todos los elementos ni costos asociados al uso de redes móviles en la prestación de servicios de banca móvil, pudiendo generar una consecuencia no deseada de afectación de los usuarios de los servicios de telecomunicaciones que deberían absorber en su tarifa los costos no considerados en la tarifa propuesta para los servicios de banca móvil, sin que los usuarios de estos últimos servicios, perciban una reducción tarifaria en la medida que no existe una regulación que considere todos los agentes de la cadena de valor, especialmente el financiero y la red de bajo valor.

De otra parte, uno de los argumentos que propician la expedición de este proyecto regulatorio, es la posibilidad de ingresar a la Organización para la Cooperación y el Desarrollo Económico – OCDE[4]; sin embargo, es necesario que dicho propósito no conduzca a la adopción de medidas sin el debido soporte y sin la observancia de los presupuestos legales existentes.

Adicionalmente, sin desconocer la importancia impulsar el desarrollo de la banca móvil, es preciso evaluar que la penetración de dichos servicios también depende de factores exógenos ajenos a las telecomunicaciones, tales como el acceso a terminales que permitan dicha funcionalidad, nivel de educación de los usuarios para acceder a dichos servicios, las brechas sociales y las condiciones financieras de los bancos que limitan a los usuarios, entre las que se evidencian claramente los altos costos asociados a servicios financieros.

Así las cosas, es evidente que no todos los usuarios que tengan un dispositivo móvil son susceptibles de acceder a servicios financieros, toda vez que los factores anteriormente enunciados no se eliminan con la propuesta regulatoria y se mantendrán dentro del mercado.

En virtud de lo antes expuesto, resulta necesario que la Comisión, revise claramente la finalidad del proyecto y la modificación de actos administrativos

---

[4] Ibídem. Página sexta. *"(...) Así las cosas, ante el joven mercado de los SFM y específicamente de la banca móvil en el país, el* ***desafío de los responsables de la formulación de políticas públicas consiste en elaborar proyectos y una reglamentación que contribuyan a impulsar el desarrollo de este tipo de servicios, más aún ante la posibilidad de ingresar a la Organización para la Cooperación y el Desarrollo Económico (OCDE)9 camino que ha iniciado el Gobierno Nacional.*** *De esta manera, los nuevos miembros del mencionado organismo estarán obligados a cumplir con ciertos lineamientos y políticas públicas, por lo cual, se deben incentivar y solucionar problemas para el desarrollo de sectores rezagados, entre los cuales se encuentra la inclusión y profundización del sector financiero. (...)"* (Negrilla fuera de texto)

que podrían generar la asunción injustificada de costos y la transferencia de beneficios de un sector (telecomunicaciones) a otro sector (financiero), en contravía del beneficio de los usuarios.

II. COMENTARIOS PARTICULARES DEL ACTO ADMINISTRATIVO

De antemano se reitera que el proyecto de acto administrativo, que resulta en una fijación de precios, no cumple con los presupuestos legales para este tipo de medidas, en tanto no se ha realizado una definición del mercado relevante ni se ha puesto a consideración del sector un estudio de mercado sólido que evidencie la falta de competencia o la existencia de una eventual falla de mercado. La ausencia de estos presupuestos, pone en riesgo la legalidad de la propuesta bajo estudio.

Por las razones expuestas las disposiciones sobre "Condiciones de Remuneración de las redes de servicios móviles asociadas a la provisión de contenidos y aplicaciones a través de SMS/MMS/USSD" contenidas en el Título VII, debe ser eliminadas, así como las obligaciones mandatarías de uso de una tecnología específica como USSD.

II.I. Modificación de la estructura y clasificación de códigos cortos para la prestación de contenidos y aplicaciones – Artículo 9

El proyecto regulatorio, adiciona al artículo 22 de la Resolución 3501 de 2011 lo siguiente:

*"PARÁGRAFO 1. Para la utilización del códigos cortos a través de USSD, la marcación se deberá realizar de la siguiente manera: *100*CÓDIGO CORTO#. Las demás combinaciones de números que se encuentren dentro del esquema establecido en la especificación técnica 3GPP TS 22.090, podrán ser utilizados por los Proveedores de Redes y Servicios de Telecomunicaciones única y exclusivamente para propósitos internos relativos a la operación de su red"*

Consideramos importante comunicar a la CRC que no se requiere anexar *100* a la marcación, toda vez que la esencia del código corto es la fácil recordación para el usuario, asociada a la longitud de las marcaciones que a la vez evita confusiones al usuario.

En virtud de lo anterior, se sugiere el eliminar el mencionado parágrafo.

II.II. Modificación del reporte de información a cargo de los PRST – Artículo 11.

El proyecto propone modificar el formato 33 actual, incluyendo el formato de ingresos recientemente solicitado por la CRC a través de requerimiento. Sobre el particular, se reitera lo manifestado en la respuesta de dicho requerimiento, en el que se aclara que no es posible establecer el recaudo de usuarios por código corto, resultando posible identificar lo facturado por código corto.

De igual manera, es pertinente aclarar que todas las modificaciones que se generan a los formatos requieren de desarrollos de sistemas para su implementación. En este contexto, es preciso recordar a la CRC que en la actualidad los PRSTM se encuentran adelantando desarrollos para adecuar sus sistemas a las regulaciones recientemente expedidas relacionadas con: Resolución 3128 de 2011 de Terminales Hurtados, Resolución 4040 de 2012 sobre transferencia de saldos, Resolución 4050 de 2012 condiciones particulares, Resolución 4112 de 2013 Roaming Automático Nacional, Resolución 4295 de 2013 sobre promoción de mensaje de Queja e información en el servicio de Roaming internacional, Resolución 4296 de 2013 compensación automática, etc.

Por esta razón, y sin perjuicio de los comentarios antes expuestos, la CRC debe revisar el tiempo mínimo de implementación debe ser de al menos doce (12) meses a partir de la fecha de publicación de cualquier norma que implique nuevos cambios en los sistemas, máxime cuando solicitan modificación de contratos.

II.III. Deber de Información y Control de Consumo – Artículo 14

El proyecto regulatorio propone un control de consumo de la siguiente manera:

"(...) Los proveedores de redes móviles facilitarán un control de consumo asociado a la provisión de servicios de contenidos y aplicaciones que hagan uso de SMS/MMS/USSD, para lo cual deberán, al menos una vez al mes, enviar al usuario un mensaje corto de texto –SMS- a través del cual se informe al usuario el consumo acumulado en dinero por concepto de estos servicios, así como la discriminación de los consumos acumulados en dinero por cada código corto. Para los usuarios prepago, el mensaje deberá enviarse entre los días 20 y 25 de cada mes, y para los usuarios pospago entre 5 y 10 días antes del corte de facturación"

Sobre el particular es preciso aclarar que en prepago, el usuario cuenta con una bolsa de dinero que puede consumir en los servicios que desee y la plataforma no permite limitar su consumo a determinados productos o servicios o imponer un límite para tal efecto.

De otra parte, el descuento por la adquisición de los servicios se hace en tiempo real y el usuario puede consultar en cualquier momento su saldo disponible, lo cual suple claramente la disposición de control de consumo propuesta.

En el caso de pospago, tener un control de consumo asociado a un código implicaría tener un sistema de facturación en línea para cada código y además limitaría la capacidad comercial de ofrecer paquetes y servicios de mensajería incluidos dentro del plan, los cuales son tarificados una vez el usuario haya cumplido el periodo de su ciclo de facturación.

Actualmente, se dispone de un control de límite de crédito para los servicios de voz, datos y contenido, que informa previamente cuando su consumo llega determinados umbrales y lo restringe cuando es superado, pero no es posible realizar la discriminación de los consumos acumulados por cada código corto.

II.III. Manifestación de la voluntad del usuario de contratar el servicio – Artículo 16

La propuesta regulatoria adiciona el siguiente parágrafo:

"PARÁGRAFO. Para el caso de los servicios de suscripción, con el fin de asegurar de que existe el consentimiento por parte del usuario, con posterioridad al envío de la información especificada en el artículo 30 y previamente a la provisión de contenidos y aplicaciones a través del envío de SMS/MMS de un servicio de suscripción, los PCA deberán enviar a los usuarios una invitación a confirmar la aceptación del servicio a través de un mensaje corto de texto o a través de cualquier otro medio dispuesto por el PCA para tal fin. Dicha invitación deberá incluir el siguiente texto:

"Esta es una invitación para la provisión del servicio XX. Si desea suscribirse al mismo, responda con la palabra ACEPTO. Esto implica la aceptación de las condiciones previamente informadas incluyendo el precio".

La confirmación de la aceptación del servicio deberá realizarse a través de un mensaje corto de texto o a través de cualquier otro medio dispuesto por el PCA para tal fin en forma gratuita para el usuario. En cualquier caso, el PCA deberá guardar registro de la confirmación expresa del usuario. La falta de confirmación del usuario se entenderá como una renuncia a recibir el servicio solicitado, y podrá ser considerado como equivalente a la emisión de un mensaje de rechazo."

Se considera excesiva la solicitud de un doble mensaje, considerando que la CRC ha expedido recientemente regulación que ha aumentado el envío de SMS a los usuarios por diferentes razones, lo cual ha saturado la plataforma y a los usuarios.

De otra parte el mensaje sugerido es de 210 dígitos lo que generaría el envío de dos mensajes que comercialmente hacen que el acceso al servicio pierda su motivación al momento de recibir el segundo mensaje.

En virtud de lo anteriormente expuesto, se exponen los comentarios y observaciones realizadas al proyecto publicado, esperando que sean de recibo

para el regulador y por tanto analizados previo a la expedición del acto administrativo anunciado para el próximo diciembre, teniendo en cuenta el alto impacto que el mismo representa para el sector de telecomunicaciones, la libre competencia y el beneficio a los usuarios.

Finalmente, se reitera la solicitud de realizar los estudios financieros que soportan la regulación de precios, y cumplir con el procedimiento establecido por la Ley y la regulación para que se defina el mercado relevante que fundamente la presente regulación, de tal manera se evidenciará que no es procedente el modelo de costos propuesto.

Cordial saludo,

ORGINAL FIRMADO
SANTIAGO PARDO FAJARDO
Vicepresidente de Asuntos Regulatorios y Relaciones Institucionales

MANAGING THE RISK OF MOBILE BANKING TECHNOLOGIES

This report was commissioned by FinMark Trust

Bankable Frontier Associates LLC
www.bankablefrontier.com
24 March 2008

BFA-080324

EXECUTIVE SUMMARY

1. M-payments and m-banking are now spreading fast across the world, in developed and developing countries. The use of mobile phones for mobile Financial Services (m-FS) is relatively new and, as a consequence, the knowledge of the risks and the risk experience of providers is still limited. However, the rapid take-up and potential scale of new offerings has led to increased interest from mobile Financial Services Providers (mFSP), both banks and non-banks, and from government regulators in understanding and managing any unique, additional risks.

2. Two elements of the mobile channel are distinctive relative to other e-banking channels like Internet banking or point of sale devices:

   a. The mobile handset, which comes with a wide range of functionality from basic on standard handsets to advanced on feature phones and smart phones;

   b. The mobile network, which includes all the links carrying a data message from a handset to the mFSP or vice versa and the methods used to communicate between the handset and the mFSP.

   Both these elements contribute to a different risk environment for m-banking. Boards and management of mFSPs as well as regulators need to have a clear basic understanding of how these elements work, including a comparison to other established e-banking channels. Increasingly, as handset functionality increases, mobile financial services are converging with Internet banking.

3. Regulators and others commonly list additional risk considerations arising from the use of the mobile channel. These include: the higher possibility of loss of device, the restricted screen and keypad of the device, the information security of the end-to-end network, the availability and reliability of the communications network, and the use of outsourced service providers. However, a priori, these factors do not in themselves make most use cases of m-FS more or less risky than other forms of e-banking.

4. The main technical characteristics affecting the risks of m-FS:

   a. The security functionality available on the handset: the lower the security requirement from the handset, the broader the potential market, especially in developing countries;

   b. The degree of dependence or independence from a particular Mobile Network Operator (which controls access to the SIM card and the mobile network): channel options may or may not require downloading of an application to the SIM or phone, which in turn may require participation of the manufacturer or MNO.

These characteristics imply four main use cases as summarized in the diagram below:

		Mobile Handset Capability	
		Standard (all)	Advanced
Independent of Mobile Network Operator?	Yes	**Use Case 1:** **Use what is there**, existing generic mobile bearer services provided on all phones accessible directly by user	**Use Case 2:** **Use mobile browsing services** that are provided on phones **Use Case 3:** **Use advanced application services** provided on phones
	No	**Use Case 4:** **Use a secure environment on the mobile** provided by the MNO or MNOs	**Use Case 4 prime:** **Dedicated secure application environment on a handset**

In general, in developing countries, the mass market for the foreseeable future will have only standard handsets, hence m-FS models which seek wide reach are likely to fall into Use Cases 1 or 4. These situations are more likely to be **"Transformational"** because of the potential to extend financial services to people who are without them.

For applications in the upper end of developing markets or in developed markets, Use Cases 2 or 3 are likely to apply. Use case 4 prime is not yet widely available.

5. m-FS are subject to many of the same vulnerabilities as e-banking. However, the risk associated with each identified vulnerability must be evaluated in a three step process.

   a. First, the likelihood and severity of the vulnerability occurring are assessed in order to calculate the risk rating. That is done within each one of the Use Cases.

   b. Second, control measures are proposed based on the assessed risk. The final risk is the risk adjusted for the control measure.

   c. Third, environmental factors may scale the adjusted risk rating upwards or downwards. These factors include whether the mFSP is a new entrant or not; and the extent to which the mobile channel is the main or dominant channel offered by the mFSP itself and/or on a country basis.

6. In general, Use Case 1, which is common in developing countries and can provide ubiquitous access, presents higher inherent technology-related risks largely because of the lack of end-to-end secure encryption of messages. This increased risk may be mitigated by effective business process and or product design controls. While Use Case 4 addresses the encryption risk by providing encryption within the SIM, and provides the most security; its use and market may be limited by the need for MNO cooperation and a SIM with SIM Toolkit capability. In Use Cases 2 and 3, the risks (and services) increasingly converge with standard Internet banking risks.

7. Emerging technology: several developments are likely to change the picture of risk:

   a. An increasing proportion of smart phones will lead to more reliance on Use Case 2 and 3 even in developing countries; this will heighten the need for knowledge of e-banking risks in countries in which Internet banking may not yet be common;

b. The development of near field communication (NFC) enabled handsets which can effectively act as a token for local purchases (already common in Japan and under trial in several developed countries such as UK and US) is likely to further increase take-up of m-FS. The risks of the integration of NFC into mobile banking require further investigation and are outside the scope of this report.

8. Findings:

The mobile technology options available today allow for a variety of choices when implementing Mobile Financial Services. Options range from technologically secure end-to-end implementations to less secure options that do not have full mobile to banking system security.

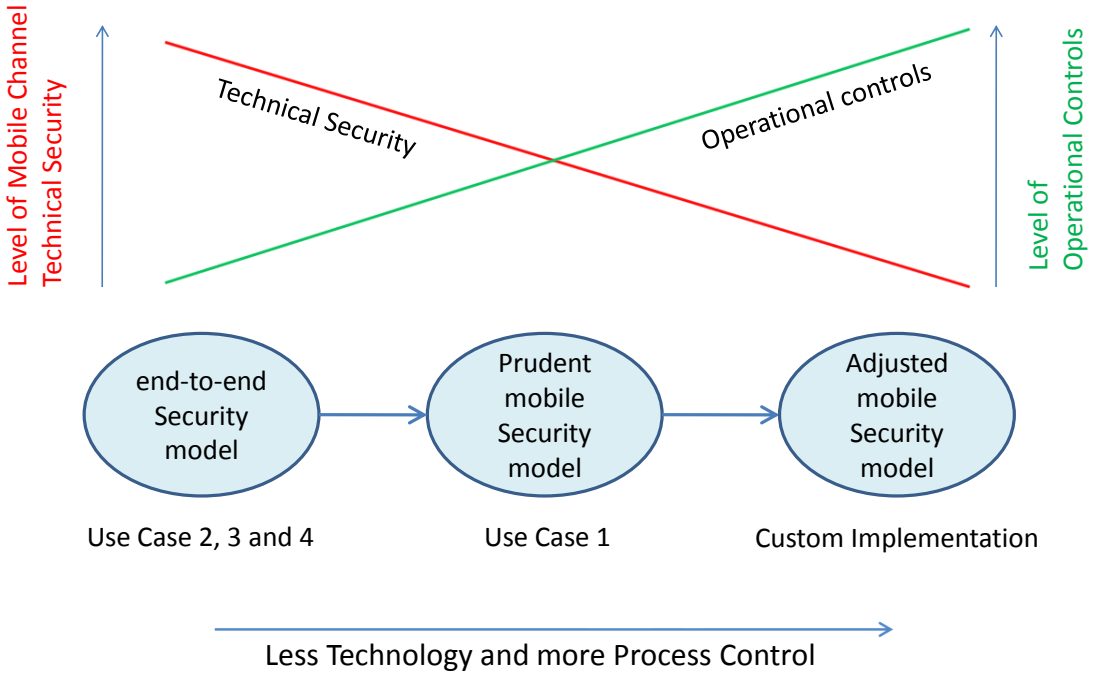
It is possible to offset the increase in risk caused by using less secure mobile technologies by introducing operational controls.

The ubiquity of less secure mobile technologies, namely Voice/DTMF/IVR, SMS and USSD on all mobile handsets and the feasibility to offset the risks introduced by their use in mobile financial service provision makes it possible to extend financial services to all mobile subscribers.

Given the lower levels of mobile handset technology prevalent in many developing countries, transformational mobile banking can be accomplished by a careful appraisal, introduction and management of operational controls (including user education) necessary to offset the higher technical risks inherent in choosing ubiquitous but less secure technologies.

The following diagram depicts the security models that can be used and the relative tradeoffs between technical security and operational controls that are discussed in this report.

Moving to prudent and adjusted security models requires a proportionate regulatory framework within which to ensure on-going and active supervision of risk management.



Recommendations:

9.1 For mFSPs:

a. To provide transformational m-FS, the mFSP should consider choosing technologies, such as those in Use Case 1, that provide quick and widespread access to its services. Where less secure technology is chosen, technical and operational countermeasures can be introduced to reduce the risk both to the business and to individual clients.

b. The boards and management of mFSPs should develop a comprehensive risk framework. This is true for banks and non-banks alike. For starting a business, a probable Use Case should be the basis for this framework.

c. mFSPs should either implement the BIS operational risk management principles or highlight where they intentionally intend to deviate from them.

d. After the initial business launch, the risk framework (in the form of a risk matrix) should be updated in light of risk experience as well as other vulnerabilities identified once operational.

e. Just as large international financial institutions are increasingly sharing their experiences of operational risk on an ongoing, confidential bases through information exchanges such as ORX, mFSPs operating in particular Use Cases may benefit from an arrangement in which a current industry level assessment of vulnerabilities and risk is available as a benchmark for operational risk assessment.

9.2 For financial regulators:

f. Regulators should be careful not to entrench technology specific standards in regulations which may unnecessarily stifle m-banking development. They should create a flexible, proportionate framework within which an on-going, active supervision of mFSPs can take place. This assures attention to the mobile channel risks while providing adequate room for risk appropriate innovations.

g. Regulators engaging with domestic mFSPs should share their learning with colleagues in other jurisdictions in a structured manner so as to contribute to and benefit from an emerging global perspective

9.3 For mFSPs, financial regulators and organizations promoting the development of the sector:

h. Given the lower levels of mobile technology prevalent in many developing countries, transformational mobile banking is best accomplished by a careful appraisal of the operational controls (including user education) necessary to offset the higher technical risks inherent in choosing ubiquitous but less secure technologies.

i. The basic level of knowledge required by board, senior management and financial regulators to meet Basel Guidelines for awareness of operational risk management in this new area should be defined. Training curricula should be developed to meet this need.

j. As the rapid pace of technological change continues, a trusted central organization should maintain a list of all known vulnerabilities of the mobile channel, updated by experience, to which regulators and mFSPs should have access as a baseline for their risk frameworks.

ACKNOWLEDGEMENTS

Specific thanks to those who gave their time to participate in our interviews, whose names are listed in Annex N; and to the following who gave comments on drafts of the document: Jenny Hoffmann, John Ratichek, and the participants at the Transformational Branchless Banking Seminar in Windsor, England in March 2008.

Johann Bezuidenhoudt
Johannesburg, South Africa

David Porteous
Somerville, MA USA

FOREWORD—the FinMark Trust Mandate

FinMark Trust has established a strong reputation for producing credible research which supports the development of innovative approaches to extend access to financial services. FinMark Trust then seeks to make this research widely available to market participants, unlike proprietary research which is not easy or affordable for many to access.

In pursuit of its mission, FinMark has commissioned a series of reports on m-banking, most recently "Mobile Banking Technology Options" by Troytyla (Gavin Kruegel) which overviews the different mobile banking technology options available in the market.

In pursuit of its mission, and specifically building on the last report, FinMark Trust commissioned this report on the risks of the different technology options and how best to manage them. As the terms of reference stated, "The lack of information about the level of risk inherent in the different technologies and the opportunities to mitigate the risk through business processes and strategies may be leading to choices which do not necessarily match the needs of the market most in need of innovative access to financial services." This report should therefore not only provide relevant information but support choices which match the needs of the market which FinMark Trust seeks ultimately to serve.

Disclaimers

This report is intended to provide a general overview of risk patterns and trends attaching to the use of the mobile channel for providing financial services. The report is for information and guidance of readers and it is not intended to support a specific plan of action since this would require additional information and insight into each particular situation.

The vulnerabilities, analyses and risks shown and analysed in this report are intended to be **indicative** of what risks which a mFSP may or will face. The analysis is not intended as an exhaustive or a fully objective list. Each mFSP should assess and validate their own risks in terms of their own situation, the intended functionality to be offered and the process controls that will be put and or are already in place.

Additional advice should be sought where necessary from expert advisors before taking action.

Neither BFA nor FinMark Trust may be held liable for the consequences of implementing any or all of the recommendations of this report.

TABLE OF CONTENTS

SECTION 1. INTRODUCTION

1.1 Context of report

Mobile banking brings new opportunities and risks to financial providers, carriers and the financial system.

On the one hand, it holds out the prospect of adding new convenience for accessing banking and payment services to existing banked customers ('**additive** m-banking'). Especially in developing countries, it may go even further to offer banking and payment services to those who have never participated in the formal electronic banking system before. This is called **transformational** m-banking to distinguish it from additive m-banking (BFA 2006). In the process, banks, mobile network operators (**MNO**) and third party suppliers stand to gain. These opportunities have caused new players to enter this market.

On the other hand, the addition of a new channel brings new **operational risks** to providers, just as the introduction of Internet banking more than a decade ago opened new categories for risk. For this reason, mobile Financial Service Providers (**mFSP**) seeking to enter the market, or those already in the market, have to assess their risks and develop strategies to mitigate them on an ongoing basis. As adoption of mobile financial services (**m-FS**) increases, financial regulators in various countries are also paying increasing attention to the specific risks brought by the use of the mobile channel.

Although some providers in m-banking are not banks and are not subject directly to banking regulation, we use as a benchmark the principles of operational risk management developed for national regulators by the Bank for International Settlement (BIS).

Operational risk is defined as the risk of loss arising from the failure of operational procedures. A number of categories of operational risk have been defined by the BIS. The operational risks related to the choice of technology include: internal fraud (including theft and unauthorized activity), external fraud (including theft and systems security), business disruption and system failures, failures in the execution and maintenance of transactions, and failures on the part of vendors and suppliers. For a full listing with descriptions of the Categories of Operational Risks, see **Annex A**.

The portion of technology risk related to the mobile channel specifically is a further subset. This report focuses on identifying the specific vulnerabilities of different payment models in different contexts related to m-banking and m-payments.

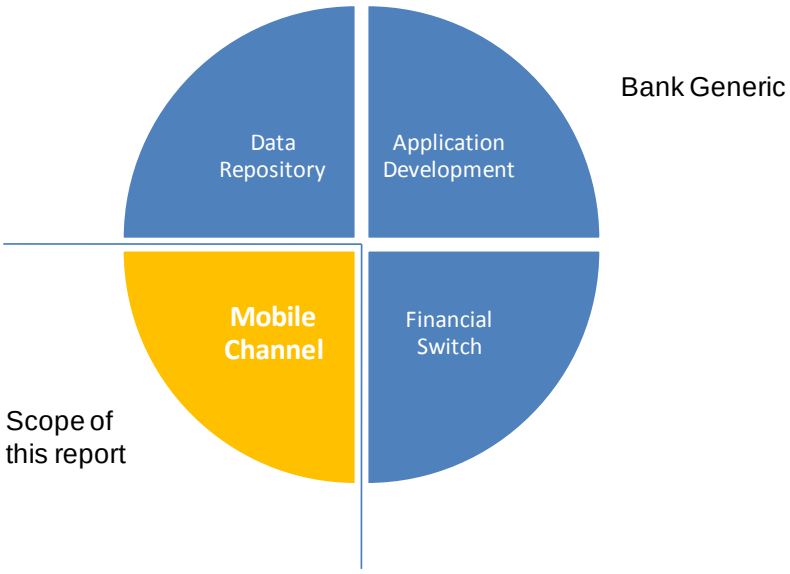
Previous reports such as that of the Mobile Payment Forum (2003) have considered the technological vulnerabilities and have assessed the risks related to certain specific use case scenarios for mobile payments. In addition, the recent report for FinMark Trust by Troytyla (2007) considers the channel choice and risks around the bearer channel and MNO integration.

However, vulnerability and risk assessment are never independent of the choice of business model or the context in which the model is to be operated. This report differs from previous reports in that the risk framework developed here is a dynamic one, which varies by model and context. This enables it to be more widely applied than a static framework. Because the permutations around model are many, the focus of this report is on models which target unbanked customers and developing market contexts, although the framework is valid for all markets.

1.2 Scope of report

This report focuses on the specific technology risks of the mobile channel and does not consider the integration of mFS platforms with other typical IT system components, such as financial switches, data depositories or applications as shown in Figure 1 below. The risks arising from the integration between these components are not specific to the use of mobile, and have received attention in other reports.

Figure 1: Technology components of m-banking models



Source: Troytyla (2007)

The report should be of interest to:

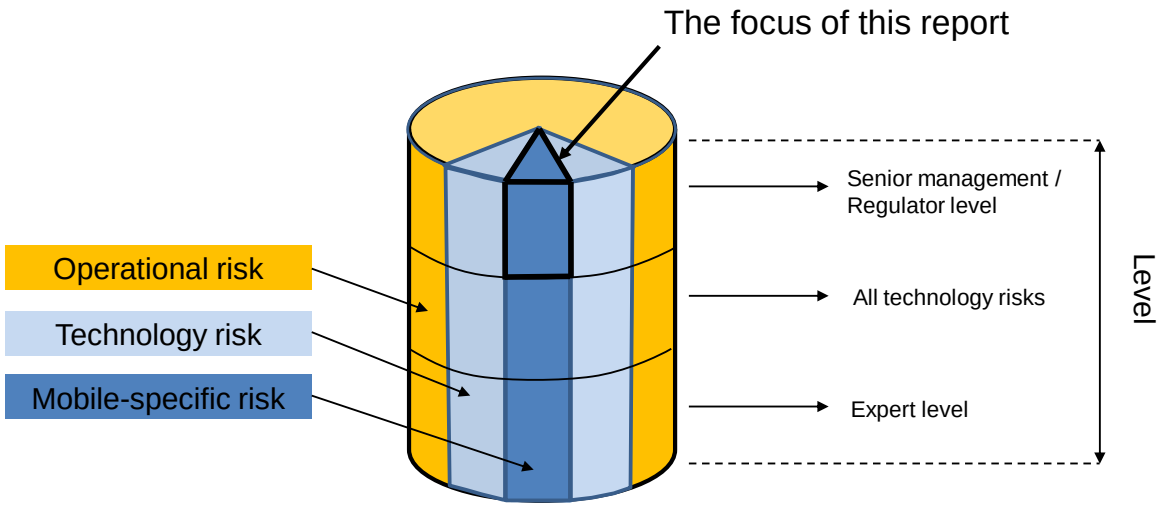
- mobile Financial Service Providers, whether banks, MNOs or non-banks, who are considering introducing m-FS, and
- financial regulators who are increasingly interested in the risks of m-banking and the extent to which providers are understanding and managing these risks.

This report is written containing the information which a senior executive or financial regulator should know about the vulnerabilities and risks of the mobile channel for financial transactions. Indeed, part of the purpose of this report is to benchmark the levels of knowledge which a non-specialist manager or board member should have about this new and dynamic area, in line with BIS Operational Risk principle No.1: *"the board of directors should be aware of the major aspects of operational risks, and should approve and periodically review the bank's operational risk framework*." Prior detailed knowledge of m-banking is therefore not assumed, although comparisons are made to banking via other electronic channels such as the Internet with which readers may be familiar.

More detailed information on the technology can be found in the **Annex C** - Use Cases – Definitions and Technology of the report.

The two parameters of the scope of the report, the content and the level, are depicted in Figure 2 below.

Figure 2: Focus of this report



1.3 Methodology

This report was compiled on the basis of:

- Personal knowledge and experience of the authors;
- Published reports from various sources listed in the references;
- Interviews with leading providers, listed in **Annex N**.

1.4 Structure of report

This report provides a process for identifying and assessing risks in the mobile channel, and then suggests controls for their mitigation. It provides a prospective mFSP with a logical process of reasoning through which to consider mobile banking risk. It provides regulators not only with that same process but additional strategic considerations. (Note: **Annex O** provides a glossary of terms used in this report.)

Section 2 reviews the particular technologies relevant to the mobile environment and benchmarks these according to known, older electronic channels, such as e-banking or ATMs. Four main Use Cases are outlined and are differentiated by the key factors related to the technological choices which have a fundamental impact on risk.

Section 3 identifies the main threats and vulnerabilities attached to the mobile channel. By assessing the likelihood and severity of each vulnerability, a risk weighting is assigned within its particular Use Case. In particular, the distinction is made between risk at an individual incident level, where a customer or the mFSP may be exposed to loss, and at a business or mass attack level, where the loss to the mFSP may be severe. Controls are identified as part of defining current practice scenarios for each Use Case.

Section 4 then addresses the choice of business model and the question of environmental risk factors which need to be taken into account in reaching a final adjusted and scaled risk rating.

Good governance practice by boards and management as well as the process of interaction with financial regulators are discussed.

Section 5 concludes with an update on emerging technologies and how they may affect the risk picture. Specific recommendations are made for mFSPs, financial regulators and supporters of this sector as a means of increasing access to financial services.

Box A: Definitions: mobile financial services: m-banking and m-payments

The following are the definitions used in this report for:

mFSP - Since a variety of type of provider—banks, telcos or others—may provide mobile financial services, we use the expression **mobile financial service provider or mFSP** to refer to the entity which is directly interfacing with the end customer to provide mobile financial services (m-FS). M-FS includes both:

m-banking – the activity whereby a customer uses their mobile phone to interact with their bank either directly or indirectly via mFSPs. The customer issues instructions, authenticates themselves and or receives information through their mobile phone.

m-payment – customers issue instructions from their mobile phone that initiate a payment to a third party. The instructions can be to their bank, to a merchant or to a Payment Service Provider for the payment of a specified amount to a specified beneficiary on the customer's behalf. Where an m-banking relationship is in place this will include m-payment. Where a m-payment relationship is in place this does not imply that a banking relationship is part thereof, only that electronic access is available to a value store (eg bank account) owned by the customer and that that customer can issue payment instructions relating to the value store for execution.

SECTION 2: ELEMENTS OF THE MOBILE CHANNEL

This section serves as the primer to introduce and outline the key technology components of the mobile channel and then the main current Use Cases as the basis for the analysis which follows.

The use of mobile brings two new elements to the financial services equation:

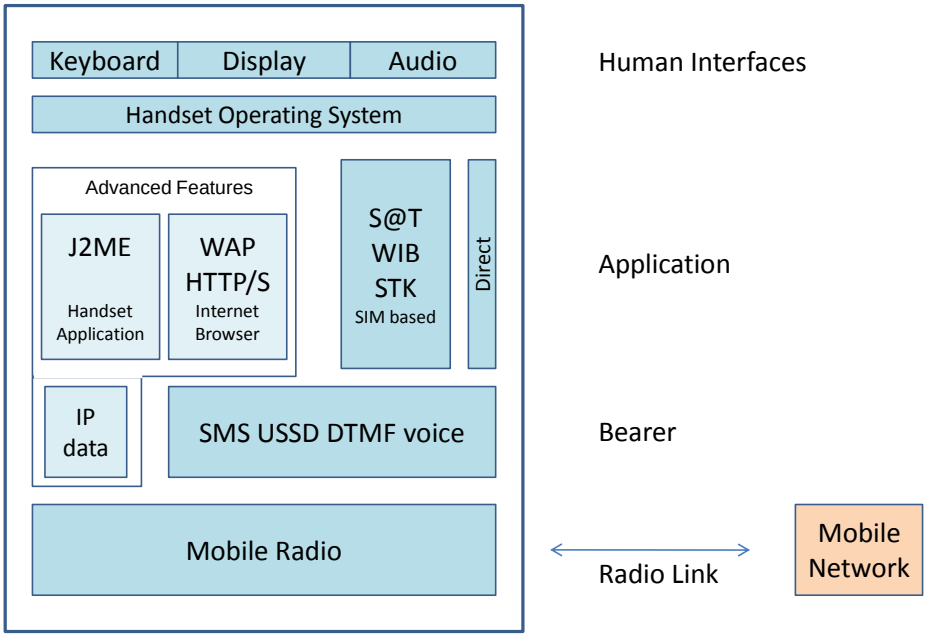
- The mobile device itself
- The communications channels offered by mobile network operators.

Both vary considerably in their functionality, as described in turn below.

2.1 Mobile device

The handset consists of several layers of components as shown in Figure 3 below.

Figure 3: Elements of the mobile handset



Standard handsets are "plain vanilla" devices that contain:

- A mobile radio to communicate to the mobile network
- The capability to send Voice, SMS, USSD, and DTMF over the radio interface
- An operating system that ties all the elements on the handset together
- Human interfaces for audio (speaker and microphone), a keyboard and a display

- At the Application level the standard handset passes the SMS, USSD, DTMF and voice "directly" between the display, the keyboard and the audio human interfaces and the bearer services.
- A capability to interface via SIM toolkit to SIM based applications also exists. The SIM Toolkit programmable application facility on the SIM is the way that standard handsets can be made secure and be given additional menu based 'application' functionality – such as mobile banking

Standard handsets do not provide:

- Facilities to secure or encrypt data before sending it to server based applications at mFSPs.
- Ability to run programs on the handset

The capability of the most common standard handset will increase over time.

For the purposes of this report a standard handset has been taken as a basic GSM handset that has been shipping worldwide since around 2004, that has USSD phase 2 and SIM Toolkit functionality, does not have a browser and can not run programs. Typically these handsets cost under USD100. A small minority of standard handsets on GSM networks may not have the capability to support USSD or SIM Toolkit applications.

Where needed, data security can be added to the standard handset by providing this on a new SIM through applications loaded into the SIM and accessed through SIM Toolkit.

The report analyses the mFSP technology assuming handsets based on the GSM standard[1]. So that mFSP's who have subscriber bases with CDMA handsets can apply this report, a comparison between the GSM and CDMA technologies has been included as **Annex M**.

Advanced Handsets have all the functionality of standard handsets; and in addition

- can communicate using IP data (GPRS, EDGE, 3G HSDPA)
- have the ability to run applications under the handset operating system (usually in a J2ME/Java environment)
- browse WAP and Internet sites – these are the 'advanced' features.

Advanced handsets fall into two sub-types:

- *feature phones* – handsets that have browsers and J2ME environments.

  They are usually locked down, in that they do not have easily accessible programming environments and often are MNO controlled in what software they may run. Typically feature phones can be described as the high end mobile phones.

- *smart phones* – handsets with programmable environments.

  Operating systems such as Symbian, Windows Mobile and Mobile Unix (iPhone) and, in the future, Android, are used. The environment on the handset resembles a small personal computer and on most the user is free to choose and run whatever software they choose. The handsets typically have large displays and can perform full function Internet browsing. Examples of these phones are HTC, iMate, Apple iPhone and Nokia N95.

[1] The Global System for Mobile Communications (GSM) is the most commonly used mobile standard in the world today, especially in developing countries.

Advanced handsets provide facilities to secure data before sending it to server-based applications at mFSPs. This security is provided by the browsers and J2ME environments on the phones.

Application based data security can also be provided on the advanced handset using the SIM. Secure applications can be loaded into the SIM and accessed through SIM Toolkit.

2.2 Network

The mobile network comprises the components which carry a data message to and from the handset to the mFSP. The features of the mobile channels used to carry those data messages are summarized in Table 1 below.

A more detailed survey of the various mobile channel technologies is presented in **Annex B** - Functional Survey of m-FS Technologies. The two tables in this Annex identify what can and cannot be done with these technologies from both a customer and a security perspective.

The considerations in **Annex B** lead to the deployment of the technologies in what have been defined in this paper as "**Use Cases (UC)**".

The nature and security of the mobile channel varies by these Use Cases.

Table 1 below depicts the relevant features of the mobile channel technologies, providing a description and indicating important security attributes for each channel technology.

- Type of handset that supports the technology
- Whether the handset can secure the technology
- If the technology provides end-to-end security
- When using the technology if the mFSP can operate their service through multiple MNOs
- Which Use Case the technology is assigned to

Table 1: Mobile Channel Features

Channel Technology	Description	Supported on Handsets	Security of transaction on handset	End-to-end Security	Supports Multiple MNOs	Use Case	Descriptive Reference (3) TroyTyla 2007
IVR	A call is made to (or from) an automatic system and the user receives pre-recorded prompts and responds by selecting keys	Standard Handset	None	No	Yes	UC1	Section 4.2
Structured SMS	A SMS text message is sent to the mFSP. The message is interpreted and acted upon and a response SMS sent		None	No	Yes	UC1	Section 4.1
USSD	A number is called from the handset and a menu then displayed on the handset that the user navigates through and selects options and enters data		None	No	Yes (1)	UC1	Section 4.3
SIM toolkit (WIB / SAT / Java / custom)	Implemented within the SIM that is inserted in the handset. The functionality appears as a set of additional menu/s on the handset		Provided in SIM	Yes	Possible (2)	UC4	Section 4.6
J2ME	Applications that can run on the handset	Advanced Handset	Provided within the application	Yes	Yes	UC3	Section 4.5
WAP	Internet Browsing using a WAP protocol browser. Same as browsing off a PC. WAP provides optimised (data usage and size of screen presentation) interaction for the mobile.		As provided by the WAP Browser	Yes – SSL	Yes	UC2	Section 4.4
HTTPS – Internet browser	Standard Internet browsing off the mobile to the bank's web site. Mobile performs the function of a PC		As provided by the Internet Browser	Yes - SSL	Yes	UC2	n/a

Note:

(1) Requires a common USSD short-code on every MNO

(2) Because of the need for access to the MNO SIM. Typically MNOs do not run common 3rd party applications (exceptions such as South Africa do exist).

(3) For a descriptive use of each technology option in mobile banking refer to the Troytyla (2007) report from Finmark Trust .

2.3 Technology-related Use Cases

Technology choices regarding handset and network define four main Use Cases which have different risk characteristics. These Use Cases can be distinguished according to:

- the level of handset functionality required: Standard or Advanced; and
- the degree of independence from a MNO or many MNOs.

Table 2 shows how the four Use Cases are derived from these two factors.

Table 2: Use Cases[2]

		Mobile Handset Capability	
		Standard (all)	Advanced
Independent of MNO	Yes	**Use Case 1:** **Use what is there**, existing generic mobile bearer services provided on all phones accessible directly by user	**Use Case 2:** **Use mobile browsing services** that are provided on phones **Use Case 3:** **Use advanced application services** provided on phones
	No	**Use Case 4:** **Use a secure environment on the mobile** provided by the MNO or MNOs	**Use Case 4 prime:** **Dedicated secure application environment on a handset**

The technologies associated with each of these Use Cases, along with some of the more general associated risks, are seen in the following table (Table 3).

Table 3: Main Use Cases Identified By Technology

Use Case Approach	Technologies available	Associated Risk
1 "**Use what is there**" Use existing generic mobile bearer services provided on all phones accessible directly by a user	SMS Voice/IVR USSD	There is no encryption of information so the channel from the mobile to the mFSP is open to monitoring, replay, modification and impersonation
2 "**Use mobile browsing services**" that are provided on phones - not MNO dependent	HTTPS = normal web browsing WAP phase 1 WAP phase 2	Same risks as for a PC on the Internet. Channel is less exposed than regular Internet as much of it is within MNOs

[2] Note: Use Case 4 prime (4') in the lower right hand quadrant of Table 2 (dedicated secure application environment on a handset) has to date not been adopted in the GSM mobile environment because of the control over the environment as well as the security available/provided. However, this Use Case may develop in future. To date, an example of a secure, managed and controlled environment on a handset is the BREW environment developed by Qualcomm for CDMA handsets. This Use Case is seen as a future extension of Use Case 4 and has been called Use Case 4 prime for this reason.

3 "**Use advanced application services**" provided on phones - not MNO dependent	J2ME	Same as client side applications on PCs. Mobiles less exposed to the Internet and the threats. However issues around the trust (integrity and authenticity) of the applications exist and need to be managed
4 "**Use a secure environment on the mobile** " provided by the MNO or MNOs	SIM Toolkit WIB, S@T and Java cards	The highest technical end-to-end security as the application runs securely within the SIM and the encryption keys are kept within the SIM.

Under Use Case 1, the usual practice is to combine the available technologies.

An example is the use of structured SMS messages which are sent to the mFSP. The mFSP then prompts the user using a USSD prompt to enter their PIN.

For this report, five sub-use cases incorporating such combinations have been defined for Use Case 1.

They are outlined in Table 4 below.

Use Case 1A is the only Use Case where the transaction and PIN are sent at the same time. All the other Use Case 1s interactively ask for the PIN which reduces a number of risks and thus makes the Use Cases (1B to 1E)more secure and less risky.

Table 4: Sub-Use Cases of Use Case 1

1A. Structured SMS	Send plaintext SMS with instruction mnemonic, value and PIN to the mFSP number, the SMS content is processed and a response sent back to the handset
1B. Structured SMS with confirmation and PIN authorisation via IVR	Send plaintext SMS with instruction mnemonic and value to the mFSP number, the SMS content is processed. IVR calls back asking for confirmation of transaction and PIN. PIN entered as DTMF. A SMS response sent back to the handset
1C. Structured SMS with confirmation and PIN authorisation via USSD	Send plaintext SMS with instruction mnemonic and value to the mFSP number, the SMS content is processed. USSD message sent back to handset requesting confirmation of transaction and PIN. PIN entered in USSD menu. A SMS response sent back to the handset
1D. IVR call to setup transaction and IVR call-back for PIN authorisation	Call in to IVR to setup transaction via IVR voice prompts and DTMF responses. Transaction is processed and checked. IVR calls back asking for confirmation of transaction and PIN. PIN entered as DTMF
1E. USSD menu with PIN login	USSD shortcode entered by user to initiate a USSD session, prompt for PIN sent from USSD server, PIN entered and session opened and menu displayed. Follow menu to set up transaction and then submit it for processing. USSD transaction confirmation and thereafter a confirmatory SMS

Table 5 below maps various current mFSP business models into these Use Cases, indicating transformational models in red. Those interviewed for the purpose of this report are marked with an asterisk (*).

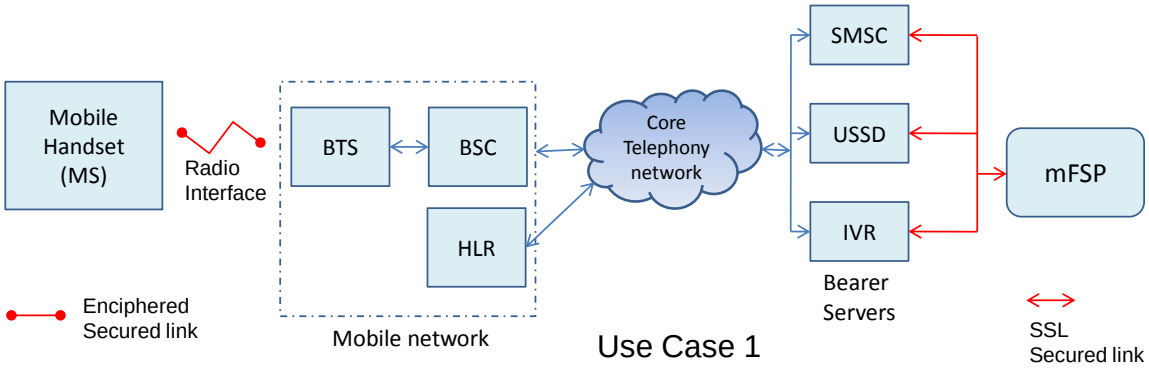
Table 5: Current examples of each Use Case scenario

		Mobile Handset Capability	
		Standard (all)	Advanced
MNO independent	Yes	**Use Case 1:** **G-Cash*** (Ph) **Wizzit*** (SA) FNB* (SA) ABSA* (SA)	**Use Case 2:** Nedbank* (SA) FNB* (SA) ABSA* (SA) Obopay* (US) **Use Case 3: J2ME** Obopay* (US) Monitise* (UK)
	No	**Use Case 4:** **G-Cash*** (Ph) **Smart** (Ph) **MTN Banking*** (SA) **M-Pesa*** (Ke)	**Use Case 4 prime:** Obopay* (US) Firethorn* (US)

Note: No one Use Case may totally fit the situation of an existing or prospective mFSP. Additionally a mFSP may use multiple technologies and offer m-banking services under one or more of the Use Cases. However, the Use Cases do represent the main technology related choices which affect the risk environment of an mFSP.

Security by Use Case: The differences in the path and security associated with data messages can be distinguished by the Use Cases. These are summarized in successive figures below. Full description of the system linkages can be found in **Annex C**: Use Cases – Definitions and Technology.

Figure 4.1: The mobile channel for SMS, USSD and IVR DTMF – Use Case 1

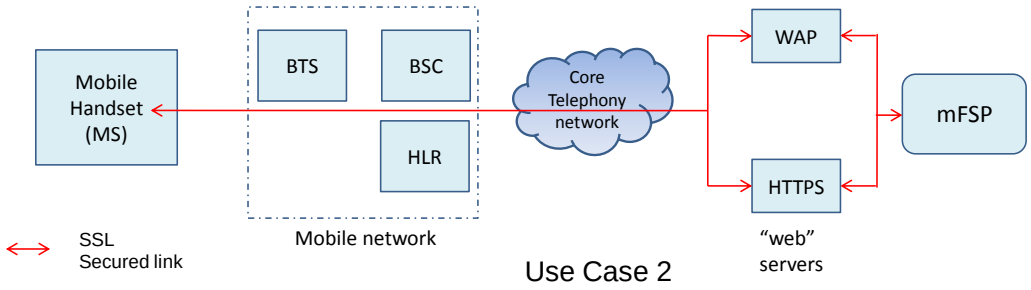


In this Use Case, the intrinsic security available in the network is used. This security is not end-to-end but is instead built up of the security available at each of the individual elements that make up the path that the transaction takes from the Mobile handset through to the mFSP.

Thus, at insecure elements, the transaction can be copied, altered, resent (replayed) and or destroyed.

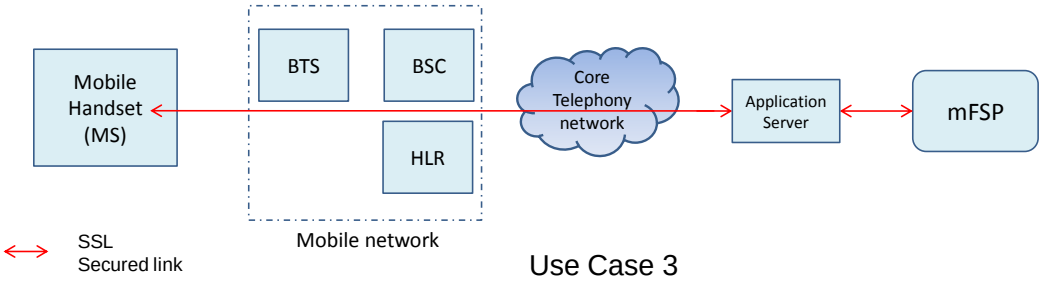
The vulnerabilities of this Use Case are analysed in Section 3.

Figure 4.2: The mobile channel for IP Data Browsing – Use Case 2



In this Use Case, because it is possible to run an explicit security program on the handset in the form of a browser with SSL it is possible to secure the data link end-to-end from the handset to the WAP or HTTPS Web Servers.

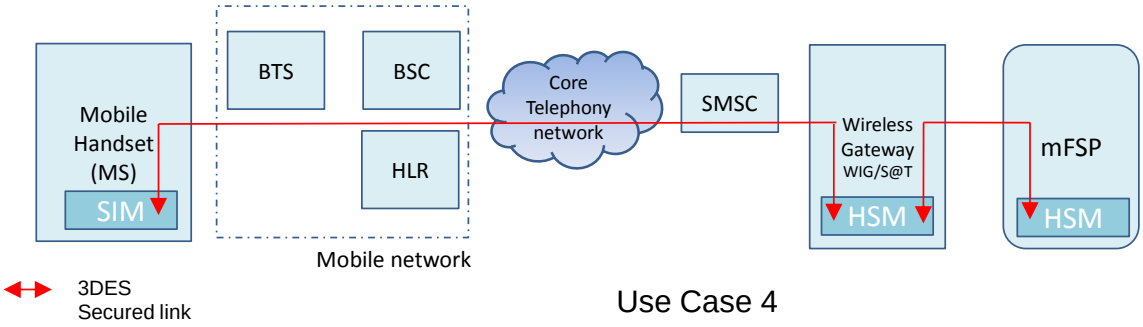
Figure 4.3: The mobile channel for IP Data Applications – Use Case 3



In this Use Case, because it is possible to run a program with explicit security on the handset, in this case a J2ME application with a cryptographic capability, it is possible to secure the data link end-to-end from the handset to the Application Server.

This handset based application secures all the data sent and received typically through a SSL link (secure tunnel or 'pipe') that passes through the mobile network all the way to the Application Server.

Figure 4.4: The mobile channel for SIM toolkit – Use Case 4



In this Use Case an application is securely placed into the SIM. The handset communicates with the SIM and thus the application using a set of commands called SIM Toolkit. The communication allows the application on the SIM to appear as part of the cell-phone's menu. The display and selection of menu items and the entry of data is then possible.

The SIM has a set of security keys stored within it that are linked to keys in the secure High Security Module (HSM) attached to the Wireless Gateway. In this way the SIM can communicate to the Wireless Gateway securely as the traffic between the two is enciphered using these shared keys.

2.4 M-banking compared to other e-channels

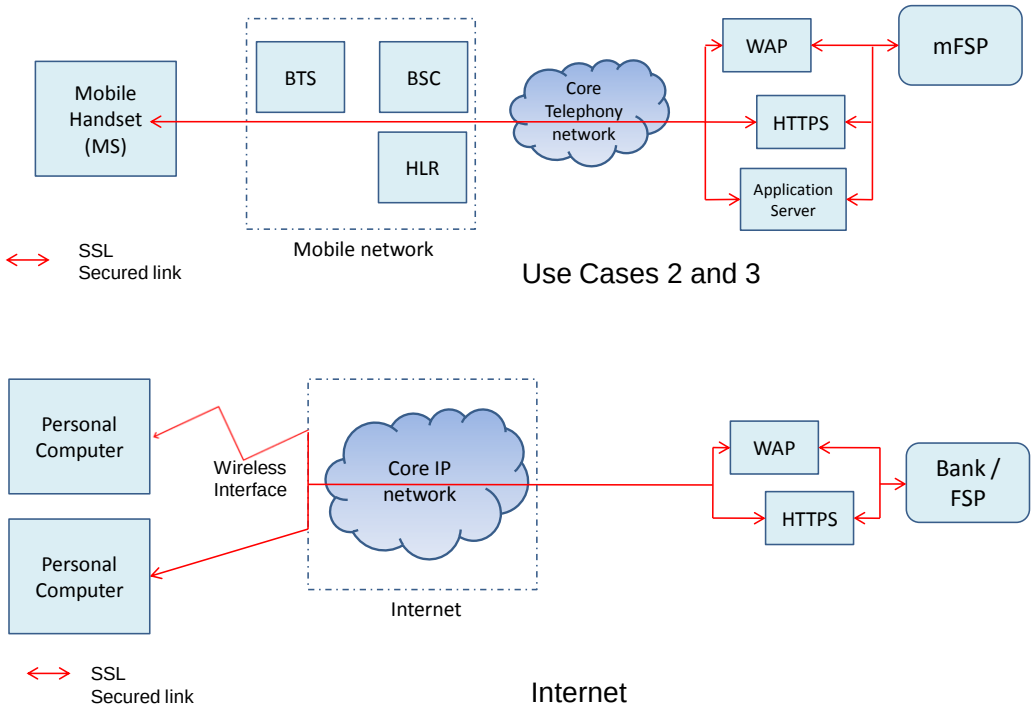
To put m-banking as described by these Use Cases into the proper context, it is helpful to understand that it is one type of electronic banking. The following table provides a comparison among the various e-channels used in banking.

Table 6: Comparing the different forms of e-banking

	ATM	**EFT POS**	**Internet banking**	**m-Banking**
Devices	ATM	POS device Shop tills	PC Advanced mobile handsets	Mobile handset
Owned by	Bank or third party network	Acquiring bank or merchant or ISO	Client	Client
Common functionality	Balance enquiries Transfers Payments Cash in or out	Payments Cash in or out	Balance enquiries Transfers Payments	Balance enquiries Transfers Payments Cash in or out
Form of authentication	2 factor (card + PIN)	2 factor (card + PIN/ signature)	1 or 2 factor (with additional token or OTP)	2 factor (MSISDN + PIN)
Encryption usage for securing communications	3DES common	3 DES common	SSL in browsers	3DES when available on handset or in SIM
Communications	Dedicated line Mobile IP data (GPRS/3G/HSDPA)	Dedicated line Wifi Mobile IP data (GPRS/3G/HSDPA)	TCP/IP over: Dedicated line Wifi Mobile IP data (GPRS/3G/HSDPA)	IVR / DTMF SMS USSD Mobile IP data (GPRS/3G/HSDPA)
			Client access to Mobile Financial Service Provision	

Internet banking and m-banking share many features. Figure 5 below illustrates the similarity between Internet banking and certain m-banking technologies. It shows how the SSL link through the mobile network (Use Cases 2 and 3) and the link through the Internet both provide end-to-end security. Whether browsing on a mobile handset or off a PC, the security is end-to-end. The vulnerabilities are at the ends of the secure SSL links.

Figure 5 – Mobile Banking versus Internet Banking



Mobile/wireless data connections are now widely used across the different banking channels. For example, they are used to connect ATMs and portable POS devices to banks and to connect PCs to the Internet for Internet banking.

In many developing communities, mobile data, or more accurately access to the Internet over the mobile/wireless network, is becoming the predominant way of accessing the Internet due to the lack of fixed line alternatives. In this role the data service provided over the mobile network is not different from the Internet provided over fixed lines, wireless or satellite connections.

A rapidly growing Internet banking sector uses Advanced mobile handsets, such as Apple iPhones, to access banking web sites and perform Internet directly banking off the mobile. This is both Internet banking and mobile banking. For the purposes of this paper, Internet banking off a mobile device is considered as mobile banking and assigned to Use Case 3.

Browser based Internet banking whether from a PC or a mobile phone is technically identical and the associated vulnerabilities are the same. However, there are differences in some of the risks arising from these vulnerabilities. For example the malware threat is different. While malware (viruses, Trojans key loggers and the like) is highly developed in the PC environment, it is not yet so fully developed in the mobile handset environment. But with the rapid growth of advanced handsets, it is expected that mobile malware will be on the rise in the medium term.

As convergence continues to take place where the number of smart phones that have direct access to Internet banking grows, the distinction between Internet banking and mobile banking will continue to reduce. To the extent that mobile banking converges with Internet banking, the existing, well-developed e-banking security procedures apply.

As a result, the focus of this paper is particularly on those Use Cases (1 and 4) not covered by the existing e-banking security measures. These require particular attention as they are the leading edge of mobile banking expansion, especially in developing countries.

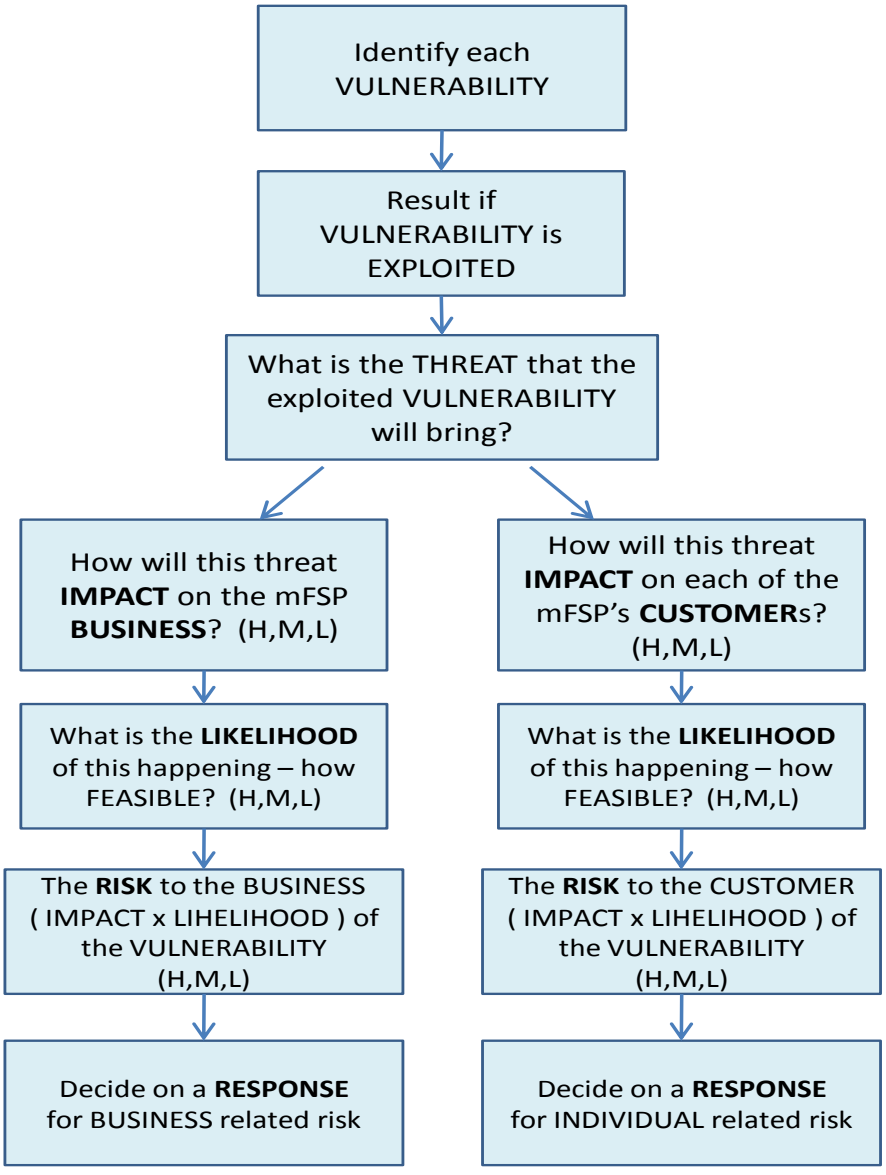
SECTION 3. VULNERABILITIES, RISKS & CONTROLS

3.1 Structured process of risk evaluation

In order to evaluate risks and choose the controls to manage them, the structured approach laid out in Table 7 was followed for each Use Case. It is important to note that what may well be a high risk for an individual customer may not be a risk to the business (and visa versa) so the business and individual risks have to evaluated separately.

The process can be represented graphically as follows:

Figure 6: Structured Risk Evaluation Process



The metrics used in this paper to allocate the risk ratings of High (H), Medium (M) and Low (L) to the impact, likelihood and resulting risk of specific vulnerabilities are defined in Table 7. The explanation for each term and a worked example are also given.

Table 7: Process and Risk Metrics

Analysis Item	**Explanation**	**Metric used**	**Example** using plaintext SMS messages (UC1A)
Vulnerability	The weakness identified	Description of the weakness	SMSC not protected
Result	What happens if the vulnerability can be exploited	Identification of the result if the vulnerability materialises	The traffic through the SMSC can be logged and MSISDN and PIN harvested
Threat to the business	What is the resultant threat to the business if the vulnerability is exploited	Indication of how a threat to the business would materialise – as a: • Fraudulent transaction • Error transaction • Loss of data privacy (exposure of information) • Denial of service	Fraudulent transactions can be initiated and access to personal data obtained
Impact	The magnitude of the event if it occurs There are two ways to look at the impact: • On the business as a whole and • On the individual customer	Business: • High Impact – the result of an event that will disrupt the business to the extent that it's existence may be threatened • Medium Impact – the result of a non-routine event that will seriously disrupt the business • Low Impact – a routine event that is handled by the day-today management processes and whose impact is absorbed in the operational expenditure Individual: • High Impact – loss of all funds and/or reputation • Medium Impact – loss that can be remedied but that seriously affects the individual's financial position	Business: Mass attack is possible through the bulk harvesting of credentials (MSISDN and PIN) and it would have a major impact on the business due to bulk account compromise therefore Mass Impact is High Individual: the impact is High as the individual's account could be emptied of funds

		• Low Impact – loss that can be recovered using operational process of the mFSP	
Likelihood / feasibility.	Probability of the event happening – namely the probability that an attacker will be able to actually exploit the vulnerability	Business and Individual • High – likely in the course of business in the short term <1 year • Medium – likely in the course of business in the next 3 years • Low – unlikely in the next 3 years	To get access to the SMSC is possible. There are people at an operator that could either gain access to a SMSC or to the transaction logs and traces. Thus the probability of an attack succeeding is High (both against the whole base and against an individual).
Risk to the individual client and to the business	Measured as the **magnitude of the Impact** of the attack **times the probability of it occurring –** likelihood	Business: • High – will disrupt the business to the extent that it's existence may be threatened • Medium - will seriously disrupt the business • Low – absorbable in day-to-day the operational expenditure Individual: • High – loss of all funds and/or reputation • Medium – seriously affects the individual's financial position • Low –recoverable using operational processes of the mFSP	Thus a High magnitude times a High likelihood gives a High Risk which implies something that the management must manage both in terms of the business and in terms of their individual customers
Response assigned	The stance taken with respect to the risk	This will vary according to the evaluation of the risk; and will result in adjusted risk	Ensure protection of the SMSC by further isolation from access, regular checks for malware. Screening of authorisation of staff to work on the SMSC and introduction of specific audited procedures for working on the SMSC

In order to reach risk assessments, we make the following security assumptions, which are generic to secure banking systems and are equally important for the mobile channel:

i. That the necessary process controls and security schemes and techniques have been implemented in the systems and network elements and that the mobile networks are not compromised (hacked, poorly implemented and/or poorly operated);

ii. That the implementation of the mFSP systems have had no security vulnerabilities added through the implementation thereof.

iii. That the system concepts and designs for the systems used to describe the Use Cases analysed have real world parallels that operate in a substantially similar manner to the functional descriptions given in this report;

3.2 Vulnerabilities of the mobile channel

Using the process described in Table 7, the first step is to identify the vulnerabilities to which an mFSP must be alert.

There are a set of generic vulnerabilities (irrespective of Use Case/technology choice) which are common to all m-FS applications, and indeed to most Internet banking as well:

1. Use of weak user PINs
2. Reset of PIN and or password by fraudster
3. Linkage of imposter MSISDN against the bank account
4. Issuing PIN to Imposter
5. Steal and use mobile device
6. Incorrect transaction due to user error
7. Lack of user knowledge or experience

Regulators [such as the US FFIEC (2003) and State Bank of Pakistan (2007)] regularly list the following factors (Table 8) as the additional, special vulnerabilities that they associate with the use of a wireless channel for financial transactions, rather than with e-banking in general.

A fuller introduction to these particular risks, including a comment on each, can be found in **Annex D** - Particular vulnerabilities of the Mobile Channel.

Table 8: Particular vulnerabilities of the mobile channel

General view
1. Relating to the handset:
(i) Because the handset is more portable than say a laptop or PC, it is also more easily lost
(ii) The limited keypad functionality of standard handsets may effectively limit the choice of PINs, and/or resulting in PINs which can be compromised.
(iii) The small screen of the handset limits the type and form of disclosure which can be made with financial transactions
2. Relating to the mobile channel:
(i) Encryption is not necessarily end-to-end, creating vulnerabilities at various points where data can be intercepted and read by third parties which may act on it
3. Relating to the m-payments application
(i) Since this is often out-sourced, the interface with the provider may create additional vulnerabilities
4. Relating to developing economy environments in particular
(i) Channel dependence: in the absence of widespread alternative e-banking channels, the risk of unavailable or unreliable service from the m-channel may be greater for users, for the provider, and even for the economy as a whole
(ii) High volumes: the widespread penetration of phones and the rapid take up of some existing m-banking platforms suggests that the pressures on the system may be heightened by comparison with Internet banking
(iii) Use of cash agents: given the shortage of other means of accessing cash (such as ATMs), some new services place heightened reliance on new networks of agents for handling cash. The management of these networks create operational risks.

The most significant single heightened risk factor relates to 2(i) above: that encryption is not always end-to-end, as in Use Case 1.

This section will consider further the risks arising from this vulnerability, as well as other generic vulnerabilities.

3.3 Prudent Practice in Addressing Technological Vulnerabilities

The Use Case Scenarios

Before calculating the risks associated with the vulnerabilities in each Use Case, it is appropriate to adjust them for the standard functional frameworks and control measures which are encountered among the active mFSPs. The mFSPs that were interviewed for the report were considered a reasonable cross section of the worldwide mFSP base and their practices examined to determine what the norm for functional frameworks and control measures was in the different Use Cases.

The Use Cases embodying the functional frameworks and control assumptions are labelled **Use Case Scenarios** since they embody current practice in each case. The functional frameworks and controls are embedded into the scenarios since (we believe) prudent risk management would usually mean implementing such controls. These Use Case Scenarios

translate each Use Case into instructive benchmarks for mFSP practice. **Annex E and Annex F** contain descriptions of these practices.

Annex E describes the functional operations through the mobile banking transaction sequence, taking into account the vulnerabilities inherent in the respective mobile technology deployments. It shows a mixture of procedural controls, functional differences in services offered, and specific implementation constraints. These are considered prudent practices.

Note that Annex E covers only Use Case 1 and its sub-Use Cases. This is because attention to prudent practice is particularly important when choosing a technology that does not have the end-to-end security found in Use Cases 2, 3 and 4.

Annex F then shows the types of transaction services appropriately offered in each Use Case.

3.4 Risk Identification and Assessment by Use Case

Given the prudent practices suggested by Annex E and Annex F, the table in **Annex G** Vulnerabilities in specific Use Cases, identifies the most likely vulnerabilities (points of attack) in each Use Case.

The table compares the vulnerabilities in the different Use Cases depending on whether end-to-end security is available or not. Many vulnerabilities are common to all Use Cases; but in the cases without end-to-end security, additional vulnerabilities exist in the channel.

These vulnerabilities are then considered in light of the likelihood of their occurrence and the severity of their impact. Following the process in Figure 6 and Table 7, the probability of the event is multiplied by the impact to calculate the risk.

Table 9 below shows an example of how for Use Case 1E – the USSD menu with PIN log-in – the risk calculation can be performed for some selected vulnerabilities.

The results of the risk evaluations of the four Use Cases are summarized in the Risk Rating tables in **Annex H** - Summary risk evaluation by Use Case. These tables identify the high and medium risks by Use Case. They show that the threats can impact on two levels: the mFSP's business itself and the mFSP's individual customers. The tables thus offer two vantage points from which to evaluate the risks present in the services offered by mFSPs.

The mSFP's task of evaluating a business strategy is simplified by the catalogue of the high and medium risks by Use Case. Corresponding counter-measures are also noted.

The tables reveal that, for almost every vulnerability, the risk for individual clients is greater than for the business as a whole. They also imply that a vigorous, disciplined administration of the countermeasures by both mFSPs and individual clients is necessary to thwart security threats. Whether the countermeasure is technical or operational, weak application of the controls leaves the mobile banking network more available to exploitation.

Business Risks

Most of the business risks that rate as High are found where the transactions pass through a common component, like the SMSC or USSD server, or where there is a vulnerability common for all end users.

Individual Risks

Individual risks are the union of the business risks and the individual risks. A business risk generally effecting the business and therefore all individuals as well as the risks that the individuals are exposed to due to their specific use of the channel.

The risks introduced by the individual are how the individual uses the service. As such the countermeasures usually involve user education.

Table 9: Example of Risk Matrix for Use Case 1E

		Leads to Threats of			Impact		Notes	Likelihood/Feasibility		Risk	
Vulnerability	**Result if Vulnerability exploited**				**Bus**	**Ind**		**Bus**	**Ind**	**Business**	**Individual**
Reset of PIN by fraudster	Know PIN and MSISDN and can initiate transactions off a stolen phone	Fraudulent transaction	Privacy loss	Service Denial	H	H	Limited by number of PIN changes that can be done via the call centre	L	H	M	H
Lack of user knowledge or experience	User sends mis-formatted messages - denial of service, PIN lock due to repeated invalid attempts. User asks others for help and exposes their PIN, shows confidential information	Fraudulent transaction	Privacy loss	Service Denial	No	H	Individual compromise - Difficult to perpetrate on a large scale	No	M	n/a	H
SIM swap	The valid MSISDN is moved to another handset. The user has no access to their account and receives no notifications. The user with the other handset, on knowing the PIN, can transact on the account	Fraudulent transaction	Privacy loss	Service Denial	L	H	Individual compromise - Difficult to perpetrate on a large scale	L	H	L	H
Movement of funds beyond defined beneficiaries	Funds gone and not retrievable	Fraudulent transaction	Privacy loss	-	H	H	System allows only pre-defined beneficiary payments	L	L	L	L
Infection of handset by a virus - Advanced (programmable) Feature and Smart phones	3rd party can see and send transactions through device - act as relay for transactions, PIN sent to 3rd party, information sent to 3rd party, replay of transactions, stop valid transactions, stop notification messages	Fraudulent transaction	Privacy loss	Service Denial	H	H	For phones that can support J2ME and run downloaded applications this is possible	L	M	M	H

3.5 Summary of Risk Controls

As noted above, we have chosen to embed prudent risk countermeasures or controls into each use case scenario in arriving at the risk evaluation. However, given the importance of these measures, this section focuses on them separately. Conventional risk control measures include:

- Reject—by changing the model to avoid the risk
- Accept—pricing for the risk
- Transfer—by moving the risk to another party (eg buying insurance)
- Mitigating the risk through control strategies which operate within 3 domains to stop vulnerabilities being exploited. The following table shows those domains.

Table 10: Domains of mitigation strategies

Domain	Mitigation Strategy	Example	Action
Technology	Change and / or modify the technology to reduce the risk	Plaintext PIN exposure	Move from no security on the mobile to security on the mobile (from structured SMS with PIN to SIM Toolkit with PIN)
Process	Implement process controls to block process paths that can be exploited	Movement of funds to a random beneficiary allows a thief to send money to whoever they want	Require pre-registration of a beneficiary via the call centre where the user's identity is authenticated by asking questions Limit or set the value that can be sent to a beneficiary Fraud monitoring processes to look for out of normal transactions
Environment	Train and inform users to influence behaviour	Theft / borrowing of mobile handset and knowledge of the PIN by thief. (This cannot be stopped by technical or process means)	Train users to not hand out their PINs so as to let others use their mobile Vigorous follow-up and prosecution

A further list of common procedural and process safeguards that can be adopted to reduce risk can be found in the following table.

Table 11: Common Mitigation Strategies and Controls

Vulnerability	Procedural intervention	Result	Applicable
Fraudulent movement of funds away from their owner	Limit Value movements to pre-defined beneficiaries	Difficult to move value away from Owner	All
Users choose weak PINs	Educate users, prevent most vulnerable PINs being used (eg 12345)	PINs less likely to be guessed	All
PIN obtained through social engineering (eg phishing) and ID theft/imposter	Control PIN change processes	Ensure that account access is not fraudulently obtained	All
Single account vs multiple account access - the issue is that if the customer's mobile channel is breached then access is gained to all accounts	Multiple accounts with only one account 'active' for mobile channel can be used as a process countermeasure. Movement of funds into mobile account from other accounts not possible using the mobile channel	Only the funds available in the mobile account are at risk of mobile channel failure	All
Immediate value movements - as the transactions from the mobile to the handset are immediate the velocity of funds movements through the system are high making it difficult to stop suspect transactions.	Delaying value movements within the bank and to third parties outside the bank is a procedural risk control strategy ie transaction is executed but value movement is delayed due to normal processes such as overnight clearing. This allows for back office checks, customer queries and status notifications to happen and be reacted upon	Fraudulent transactions that are delayed provide the bank a chance to analyse the transactions and intervene on suspicion of being fraudulent	All
On-us transfers have a greater chance of being managed if used for fraud as the funds are still within the same institution	Less rigorous process controls can be used for on-us than not-on-us	Funds destinations managed	All
Movement of funds to outside the mFSP's direct control. Not-on-us Transfers and payments are assumed to be the same thing - namely a movement of value away from the accountholder to another account outside the accountholders bank.	Countermeasures available include - limiting amount per payment, limiting amount per day/week/month, limiting number of transactions, filtering new destinations and independently verifying the payments, managing destination (beneficiary) registrations, monitoring velocity to certain accounts	Limited velocity and value of transfers away from mFSP and it's user leading to less risk of funds not being recoverable	All
Replay of transactions	Teach users to enter a sequence number. Can be a randomised list on a card that the user ticks off	Transactions can not be resent / replayed	UC1A
Repeated transfers from a single account	Velocity limits - only one transaction per period and/or triggered manual response / queries	Reduced likelihood of Accounts being emptied on breach of access control	All

SECTION 4. ENVIRONMENTAL FACTORS, BUSINESS MODEL CHOICE, AND GOVERNANCE PROCESSES

4.1 Risk in context: scaling for the environment and the business model

The report so far has considered the risks associated with the choice of mobile specific technology. However, these technology choices do not exist in a vacuum: they are dynamic not only in that they change over time, as technology changes (which will be discussed in Section 5.1) and as knowledge of vulnerabilities and how to exploit them spreads but also because final risk evaluation is shaped by context: both at the level of the environment within which the mFSP firm operates and by the inherent risk of the firm's business model.

This section therefore sets out the scaling factors which should be applied to the results of the preceding process to determine the scaled final level of risk faced by the mFSP.

4.1.1 Environmental risks

The environmental risks linked to the use of the mobile channel may be heightened when:

- A significant proportion of the users are first time users of electronic banking of any form, and hence have had less exposure and practice with issues like PIN protection or with the need to check statements for unauthorized transactions. Transformational models are likely to have more first time users, since targeted customers of m-FS may be previously unbanked at the time when they sign up for the services, than additive models in which the holder of a bank account registers to use the mobile channel in addition to other factors.
- There is substantial dependence by a significant number of customers on the mobile channel only, without alternative options in the event of system failures or disruptions. Again, this is more likely to be the case in developing countries, where the rate of early adoption is high enough to suggest that even temporary denial of service as the result of network downtime would affect substantial numbers of people.
- Customers leave a substantial portion of their disposable financial assets in the new instrument. This increases vulnerability since individual losses could have disproportional consequences for these customers, unlike those who are able diversify across providers.

4.1.2 Business model risks

The choice of business model will, in no small part, be decided by what is available in the target market in the target country. Transformational models which target initially unbanked customers in developing countries are more likely to target users with basic handsets (Use Cases 1& 4) whereas mFSPs in developed countries (additive models) are increasingly able to assume that an addressable portion of the population has a phone with relatively high capability (Use Case 2&3). Advanced handsets can also be used for Use Case 1 & 4 as they support the standard functions.

The question of channel independence from MNOs, which also affects risk, will be decided by the business strategy of the mFSP and the market structure for mobile phones in a country. It is likely that providers which are not telcos, such as banks, are more likely to seek MNO-independent scenarios, since this maximizes the addressable size of their possible client base across many MNOs; while MNOs are more likely to seek offerings which tie-in

their voice customers providing a means of reducing churn on pre-paid services in particular. However, in countries where one MNO is dominant, this may be less of a consideration.

In all cases, the business model for mobile banking carries a number of elements which affect the risk, including:

- The allocation of roles required for m-FS to be offered (see Table 12 below)—the more the roles are split among multiple parties, the greater may be the potential risk of coordination failure among them;

Table 12: Roles required by the mFSP

Role	Possible role players	Risk implication
Legal holder of store of value	Usually a bank, but could be a non-bank e-money issuer where this is permitted	The nature and severity of financial regulation will vary considerably based on whether this store of value is considered a bank deposit or not; and regardless, whether a bank is legally liable for it
Brand	Could be a bank, telco or other non-bank brand	The association of a particular brand brings reputational risk in a way which may result in liability
Carrier	Mobile banking will always involve at least one MNO; however, the issue is whether there may be multiple MNOs in the model or not	Models specific to one MNO bring different risks from technologies which can operate across networks as the number of points of exposure increase
Technology provider	Could be purchased as a package, developed as proprietary software, on an ASP or partnership basis with technology supplier	Different systems will have different vulnerabilities

- The customer base targeted: this will affect the available technologies, since, as discussed in Sections 2 and 3, a lower proportion of potential customers in developing countries are likely to have advanced phones, and hence Use Cases 2 & 3 are ruled out; also, if users are previously unbanked, the generic e-banking risks are enhanced.
- The distribution mechanism chosen, especially for cash handling: in developed countries, m-FS are more likely to complement existing card based options for obtaining cash from ATMs or POS. In developing countries, these options may not be widely available; hence mFSPs will have to design new mechanisms for customers to access cash, such as dedicated agent channels. The introduction of agency for cash handling introduces generic operational risks; but the introduction of mobile technology may in fact enhance the ability to manage these risks, since transactions are completed in real time (see Box B below for discussion of agent risk).

Box B: Business and Individual Risk associated with use of mFSP agents for cash transactions

The main risks are around the introduction of value and removal of value from the electronic value pool ('cash in' and 'cash out'). Operations that affect this are:

- EFT-in and EFT-out
- cash out at ATMs and tellers
- cash in as deposits.

The risk to the individual is that the value given/sent and the value recorded may differ. i.e. short changing by the agent. There is no technical way to prevent this, other than ensuring that both parties involved do in fact get real time information as to the value of the transaction so that mistakes can be corrected or disputes flagged at the time. Another way to address this is to require the sender of the cash to initiate the transaction so that the value in question is set by the sender equal to the cash amount they are handing over.

For the mFSP, this is an on-us electronic transfer and thus as a gross value neutral event, so long as the integrity of the transaction within the banking system is maintained there should be no mass/systemic risk.

The case of a payment where goods and not cash are exchanged and a on-us transfer made is same as cash-in and cash-out

Hence the instant value and non-reversibility of these on-us P2P transactions is obviously key to the integrity of the exchange. Without both of these transaction attributes the cash exchange will be risky.

The identified threat is the loss of trust in the system due to

- transaction errors (the vulnerabilities being loss of value, destination, and confirmation of transaction integrity as well as the loss of transactions)
- man-machine interface errors such as spoofed confirmation messages and intentional value manipulation – eg cash in 100:00 and receiver sends only 10:00 in electronic funds

- Whether the mFSP is a startup operation or a new service line/division within an existing financial services provider. Regardless of the age of the entity, its financial capacity and brand will be significant factors affecting how much potential operational risk it can or is willing to sustain.
- Whether the mFSP is totally dependent on the use of the mobile channel for most or all transactions. If so, the vulnerability of the business to service denial due to mobile network disruption (whether due to overload on a network, power failure, natural disaster or otherwise) will be substantially heightened as well.

Annex I Business Model Choices - Elements of the service offering - provides a table outlining the customer service options defining a business model strategy.

An assessment of the effect of these additional environmental and business model risk considerations should enable senior managers and regulators to scale the adjusted risk measure derived from the technical analysis. For example, if the environmental risk is considered medium/ high (such as in a low income country environment) and the business

specific risk is also high (in the case of a startup mFSP with limited brand or track record of offering), then the risks should be scaled upwards: risks otherwise considered medium may be considered medium/high or high. This scaling would then trigger a different level of response.

Risk management process

The process of managing operational risk is an ongoing one, from the choice of the initial business model, to the development of a robust initial pilot, to scaling up, and then to continuing operations. A variety of parties internal and external to the mFSP have important roles to play in the process. The following table shows that process, adding steps 4 and 5 to the analysis reached prior to this point in the report.

Table 13: Decision steps for mobile Financial Service Provider

No	Step	Content	Responsibility
1.	**Choose initial business model— Use Case and service offering**	Macro environmental factors and business drivers combine to shape fundamentals of the available technology options	mFSP Project team, with sign off of senior management of mFSP
2.	**Define threats & vulnerabilities**	The main threats are identified, together with the detailed vulnerability arising	Project team
3.	**Assign good practice controls and assess initial risk**	Each vulnerability is assessed for the likelihood and severity of loss in order to make an initial risk assessment; and on the basis of this, a control strategy is developed, leading to an initial risk position	Project team
4.	**Evaluate scaled risk, adjust offering and controls to finalize business model agree initial risk position**	The individual risks are now scaled holistically, and adjustments made to service offering and/ or controls to bring the risk level of the business model within risk tolerances	Project team with risk management division of mFSP; also checked with financial regulators
5.	**Monitor risk experience and update risk framework**	As on ongoing process, the risk framework should be updated and board, senior managers and regulators kept informed	Responsible line division with compliance checking by internal audit; and updates discussed with risk management and regulators

The risk framework should include a risk matrix of a format like that of Table 9, Section 3.5.

High risks would be more closely monitored and reported to the responsible board committee as part of the overall operational risk framework.

4.2 Regulatory oversight: Good practice principles

In the face of accelerated technological change in financial services, financial regulators have in general adopted an approach of guiding providers through principles, rather than attempting to regulate the technological details of a fast moving environment. Following this approach, the BIS Committee on Bank Supervision has suggested a series of risk management principles to be applied to e-banking. These principles are captured in Table 14 in **Annex K**. Regulatory Oversight Principles.

A key feature of the principles is that the burden of responsibility is firmly placed on the board of directors and senior management to establish and maintain an effective risk management environment.

While the principles were written with Internet banking in mind, and specific reference is made in several places to this channel, the principles in general apply pari passu to the mobile financial services channels as well, as the shaded column reflects. Note that Principle 5, requiring secure transaction authentication, highlights the key distinction discussed in the previous sections about the difference in security provided through the different mobile Use Cases.

While the principles refer explicitly to banks, their application should be considered by any mFSP: indeed, in cases involving non-bank mFSPs, where the financial regulator may have only general or indirect authority, there is a good case for enquiring how the mFSP deviates from these principles and requiring justification.

Over time, in response to emerging risk scenarios, regulators have often encoded specific aspects of these guidelines in regulation. For example, in implementing Principle 4 referring to the secure authentication of customers, many jurisdictions now require two factor authentication for Internet banking (such as requiring the use of one time passwords or tokens). Since many mobile Use Cases automatically build in two factor (the handset MSISDN and a user PIN number), such requirements may even favour the provision of mobile over Internet financial services.

Some countries have taken the approach of adopting more comprehensive e-banking regulations:

- In the *Philippines*, a leader in mFS in the developing world, two regulations (Circulars 240 and 269 of 2000[3]) lay out the process by which a bank can obtain permission to offer or amend electronic banking services. The regulations themselves do not explicitly require specific technical standards, but instead prescribe a two-step process in which regulators first consider the general health and performance of the bank applying; and then consider the adequacy of controls around the proposed new offering. This process has also been followed to approve the m-payment offering of a non-bank (Globe).
- In *Mexico*, e-banking regulations promulgated in 2006 provide for more rule-based measures to implement the guidance above, including specifying minimum encryption standards for e-banking.
- In *Pakistan*, a new act with supporting regulations has recently been passed; and in addition, draft guidelines on Branchless Banking released in November 2007[4], explicitly mention the risks relating to m-banking technology: Section 8 makes a series of suggestions for mFSPs to consider, including highlighting the lack of end-to-end security in certain Use Cases as discussed in this report.

The more specific the regulations are with respect to technology, the more likely that they will need to be revised or else hinder the development of the market. In less developed

[3] http://www.bsp.gov.ph/regulations/regulations.asp?id=541
[4] http://www.sbp.org.pk/bprd/2007/Guidelines-Branchless-Banking.pdf

markets, where providers look to regulators for extensive guidance on how to approach risk issues in new areas, the use of guidance notes to describe the areas and create a common language for engagement may be especially useful.

For regulators, the BIS Guidelines on Operational Risk (2003) are also relevant, even though operational risk is a much broader subject as the Introduction to this report pointed out. In Table 15 in **Annex K**, we extract the two principal requirements on bank supervisors, namely to require that there is an effective risk framework and a regular review of it.

In most jurisdictions, substantive engagement between regulators and mFSPs will take place upfront, once the mFSP has developed a business model and evaluated the different risks. The regulator will have cause to consider then whether the list of vulnerabilities considered is in fact complete, relative to a master list, such as that presented in this report. Then, through engagement with the mFSP, the regulator will have to consider whether to concur with the scaled final risk assessment, given the controls in place. If so, then permission may be given to proceed; if not,, the mFSP may be required to consider additional controls or changing elements of its proposed service offering to reduce risk to acceptable limits. Then once launched, the regulator will have reason to include as part of on-site inspection whether the proposed controls are implemented effectively and whether the emerging risk experience fits with the proposed framework.

Box C in **Annex K** contains a helpful checklist of the elements to be considered by regulators in the course of engagement with mFSPs.

Consumer Protection: In evaluating risk, while the mFSP and regulator may be most concerned with business type-risks (i.e. those where the loss levels may affect the very ability of the business to continue), they must also adequately consider individual level risks—the possibility of loss to the customer in a single incident. This is especially true in environments where customers may be vulnerable (for example, where loss of access or of money in an account may result in a household going hungry) but also where such incidents, which may be mentioned in the newspapers, may affect the mFSP's brand and consumer confidence around new offering.

To address these individual risks, regulators often impose regulations aimed to protect consumers directly, rather than indirectly through the provider managing the risk adequately. Such regulations, which often follow the elements of Regulation E promulgated by the US Federal Reserve Bank, usually mandate certain forms of disclosure and enshrine minimum timeline and process for the reversal of errors or the adjudication of disputes. In this light, the Philippines Central Bank passed specific regulations for consumer protection in e-banking in 2006 while the general e-banking regulations in Mexico also make provisions for this.

Some consumer protection guidelines go further to require forms of consumer education prior to or at the time of signup. Given the heightened risks of a first time banked customer, regulators may need to play a more active role in standardizing and supporting the dissemination of appropriate consumer education materials.

SECTION 5. EMERGING ISSUES AND CONCLUSIONS

5.1 Emerging risk scenarios

The environment in which mFS are implemented is dynamic in the following senses:

- It is common for those who attack a system to use the least sophisticated and easiest techniques against the available vulnerabilities. As countermeasures are introduced the difficulty of mounting an attack that exploits a vulnerability increases and the likelihood of success decreases. Eventually the attackers have to move their focus to attack other more difficult to exploit vulnerabilities. This gives rise to an "un-virtuous cycle". As countermeasures in terms of new technology and processes are put in place, other vulnerabilities previously not economic to attack become more attractive to attack and exploits are found and executed. This, in turn, triggers new countermeasure technology and processes to be implemented. A current example is the SIM swap attack. A case study on this threat can be found in Box E **Annex L**.
- Attackers are gaining more experience and are thus able to mount increasingly sophisticated exploits. The "un-virtuous" cycle will continue to bring vulnerabilities whose feasibility and likelihood of attack were previously small into the mainstream. In the way that phishing and key logging were not considered likely in the late 1990s and then became mainstream in the early 2000s, attacks such as DNS poisoning (pharming), man-in-the middle, and mobile network element penetration will slowly become mainstream attacks.
- The increasing take-up of advanced phones, even in the developing world, is facilitating the introduction of malware to the mobile phone just as PCs were infected from the mid-1990s. It is expected that the threats will increase more quickly on mobile phones due to larger bases and their continual connection to the Internet. mFSPs and MNOs need to address this.
- Introduction of NFC chips into mobile handsets, while outside scope of this report, is occurring. It is expected that large scale adoption will occur in advanced handsets in the mid-term. Vulnerabilities such as "in-pocket" stealing of amounts below PIN thresholds and social engineering to trigger unintended purchases will be exploited.
- The malware risk associated with Smartphones is discussed in Box D, **Annex L.**

5.2 Conclusions: Risk Approach

New Initiatives: Especially with the adoption of new technology, a closer understanding and analysis of operational risk is necessary, not to frighten off potential providers or to make regulators over-cautious, but exactly so as to enable entities with appropriate technologies and adequate processes to assume new risks. The purpose of this report is to enable better understanding through a structured way of identifying and assessing the risks associated with different use scenarios which are now common.

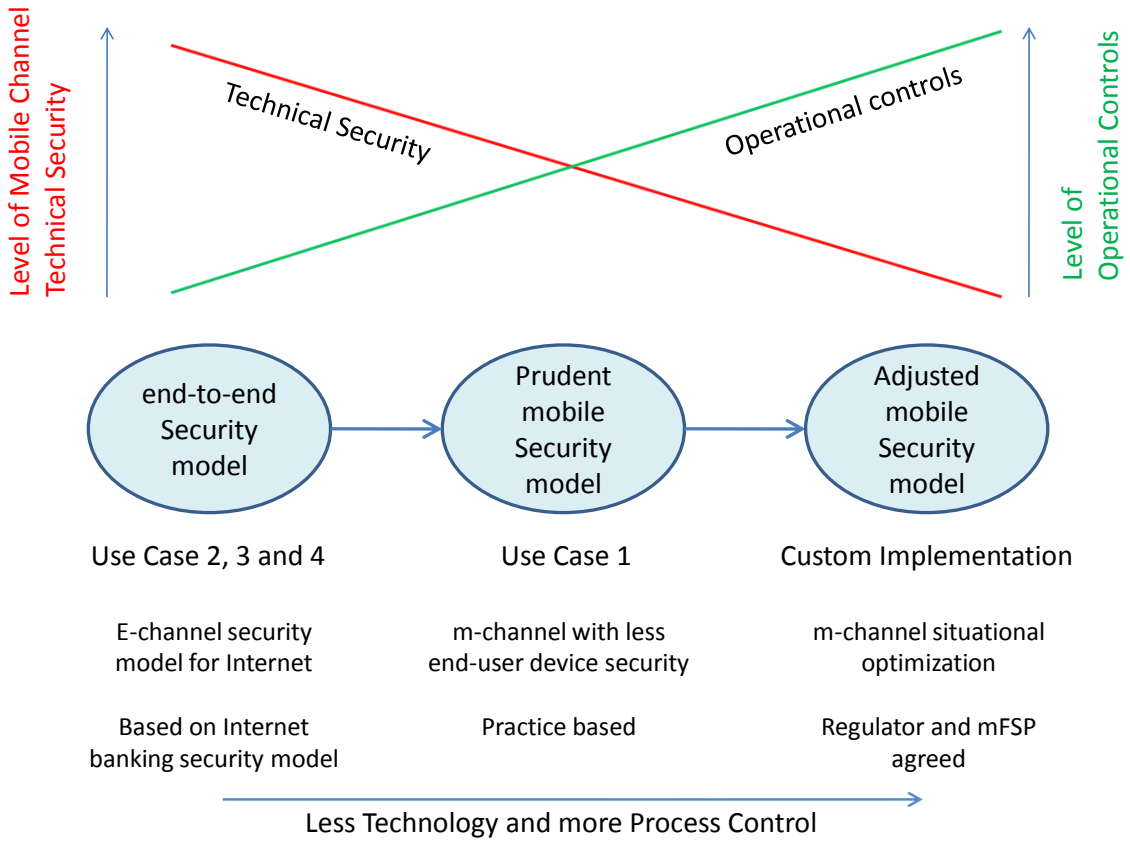
m-FS clearly have great potential to be transformational by extending access to financial services to underserved people in developing countries. However, in the developing world today and for the foreseeable future, most customers will have only standard handsets. Hence, for mass or transformational offerings, mFSPs are in general limited to the Use Cases (1 and 4) which can work with these handsets.

While end-to-end security can be provided on standard handsets through approaches such as SIM toolkit, this requires MNO cooperation and usually limits the market to the subscriber base of a particular MNO. Depending on the market share of the MNO, this proportion may still be sizable.

Use Case 1 (in which there is no end-to-end security but also no tie to a specific MNO) is likely to remain a popular approach in developing countries for banks and other new providers seeking to reach new client bases in a convenient fashion.

As this report has shown, Use Case 1 also involves particular heightened risks, compared with other forms of m- or e-banking. However, the higher inherent technology risk of this Use Case should not per se cause regulators or providers to rule it out. As Figure 7 below shows, the less one relies on features of the technology to eliminate certain risks, the more reliance should be placed on process controls to create custom implementations.

Figure 7: The Trade-off of technology and controls



Implement Process Controls: Common examples of process controls used by leading mFSPs operating in Use Case 1 were embodied in the variants of Use Case scenario 1 sketched in the report. However, it is possible that in certain environments such as where the average level of wealth is very low, some of the common practice controls may be less relevant or necessary. This enhances the possibility that mFSPs and regulators will agree on a risk approach which is optimized for a particular environment in a custom implementation. However, it would still be wise to consider how such an implementation deviates from common practice in order to focus on the areas of possible additional risk.

Starting Point: It is also possible to start from a common practice position and thereafter implement changes as the risk environment becomes better known and the risk framework fully implemented. An example of this could be the removal of the restriction of payments to only pre-registered beneficiaries and the introduction of beneficiary specification at moment of payment.

Optimism and Opportunity: Above all, it is important not to send the message that higher risk technical solutions are to be avoided by providers or blocked by regulators simply

because they may be inherently higher risk. Rather a dynamic approach should be taken which recognizes the values of countervailing controls, and which applies them in an incremental fashion in the face of risk experience. Essential for a more flexible approach is, however, that the new entrant has a commitment to risk management, understands the risks and sufficient experienced manpower and resources to do it well, and cover possible levels of business loss and customer loss resulting from risk materialisation. If so, then regulators may find it well worth allowing the approach to launch, and learning from the experience.

5.3 Recommendations

5.3.1 For mFSPs:

a. To accomplish transformational banking, the mFSP should choose a technology that provides quick and widespread access to its services but with the minimum of technical issues. For example the mFSP could consider USSD with SMS notification (UC1E). The tradeoff is that both the business and individual client risk increase. Countermeasures such as volume and value limitations will reduce individual related risk. If high security and lower technical risk is needed, then SIM based security (UC4) should be considered.

b. The boards and management of mFSPs should develop a comprehensive risk framework. This is true for banks and non-banks alike. For starting a business, a probable Use Case should be the basis for this framework.

c. mFSPs should either implement the BIS risk management principles or highlight where they intentionally intend to deviate from them.

d. After initial business launch, the risk framework (in the form of a risk matrix) should be updated in light of risk experience as well as other vulnerabilities identified. The board of the mFSP should be kept informed of high risk areas and the status of controls to address them. Senior management should routinely scan the updates profiles. Internal audit and compliance departments have an important role in ensuring that controls are enforced.

e. Just as large international financial institutions are increasingly sharing their experiences of operational risk on an ongoing, confidential basis through information exchanges such as ORX, mFSPs operating in particular Use Cases may benefit from an arrangement to pool their risk experiences. While competition among mFSPs on an international basis may preclude direct bi-lateral sharing of such information, this could be facilitated through a confidential channel so as to maintain a current industry level assessment of vulnerabilities and risk as a benchmark for operational risk assessment.

5.3.2 For financial regulators:

f. Regulators should be careful not to entrench technology specific standards in regulations which may unnecessarily stifle m-banking development. They should create a flexible, proportionate framework within which an on-going, active supervision of mFSPs can take place. This ensures adequate attention to identifying, monitoring and controlling the mobile channel risks while providing adequate room for risk appropriate innovations that might be excluded if entrenched, inflexible technology standards exist..

g. Because the technology risks are common worldwide, regulators engaging with domestic mFSPs should share their learning with colleagues in other jurisdictions in a structured manner so as to contribute to and benefit from an emerging global perspective.

5.3.3 For both mFSPs and financial regulators:

h. Transformational mobile financial services are best provided following a careful appraisal of the operational controls (including user education) necessary to offset the higher technical risks inherent in technologies available on standard handsets. Figure 7 in Section 5.2 illustrates the trade-off of technology and operational controls.

i. The basic level of knowledge required by board, senior management and financial regulators to meet Basel Guidelines for awareness of operational risk management in this new area should be defined. Training curricula should be developed to meet this need.

j. Financial regulators should engage potential mFSPs to determine whether they have adequately understood the risks of the mobile channel and have proposed adequate measures to address these. Regulators' own assessment of generic risks can be compared to those of the mFSP and divergences can be discussed.

k. As the rapid pace of technological change continues, a trusted central organization should maintain a list of all known vulnerabilities of the mobile channel, updated by experience, to which regulators and mFSPs should have access as a baseline for their risk frameworks.

5.3.4 For organizations supporting the extension of financial services:

l. The development and provision of training courses for regulators and/or senior management of mFSPs should be supported.

m. A ongoing process of sharing experiences, especially around emerging vulnerabilities, risk experience and controls within transformational models of m-FS, would benefit the sector and may best be financed by an independent body.

REFERENCES

Anderson, Ross J (2001) “Security Engineering”, Wiley http://www.cl.cam.ac.uk/~rja14/book.html

BFA (2006) “Enabling Environment for M-Banking in Africa”, available via www.bankablefrontier.com/publications.php

BIS (Feb 2003) “Sound Practices for the Management and Supervision of Operational Risk”, Basel Committee on Bank Supervision February 2003 www.bis.org/publ/bcbs96.pdf

BIS (July 2003) “Risk Management Principles for Electronic Banking”, Basel Committee on Bank Supervision July 2003 www.bis.org/publ/bcbs98.pdf

CGAP-DFID (No.43 Jan 2008) “Regulating Transformational Branchless Banking: Mobile Phones and Other Technology to Increase Access to Finance” Consultative Group to Assist the Poor and DFID http://www.cgap.org

Demartini, James (2007) “CGAP Mobile Banking Technology Matrix” CGAP Technology Program http://cgap.org/portal/site/technology/research/technology/phone/

Eads, David (Feb 2008) “Mobile Security Whitepaper” mFoundry

FFIEC (Aug 2003) “E-Banking Booklet” FFIEC Information Technology Examination Handbook Federal Financial Institutions Examination Council August 2003 www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf

Gadaix, Emmanuel (2001) “GSM and 3G Security” Black Hat Hong Kong

Gadaix, Emmanuel (2003) GSM “Operators Security” X’CON 2003

Glaessner, Thomas et al (2004) “Electronic Safety and soundness: securing finance in a new age”, World Bank Working Paper No.26:

Mobile Payments Forum (2003) “Risks and Threats Analysis and Security Best Practices”, Version 1

Operational Riskdata eXchange Association (ORX) (2006) - ORX Reporting Standards - ORX Members’ Guide to Operational Risk Event/Loss Reporting, available via www.orx.org

State Bank of Pakistan (2007) “Draft: Policy Paper on Regulatory Framework for Mobile Banking in Pakistan“ http://www.sbp.org.pk/bprd/2007/Policy_Paper_RF_Mobile_Banking_07-Jun-07.pdf

Schneier, Bruce (September 2003) “Beyond Fear - Thinking Sensibly about Security in an Uncertain World” Copernicus Books

Troytyla (2007) “Mobile Banking Technology Options”, report for FinMark Trust, available via www.finmarktrust.org.za

Van der Merwe, Pieter B (2004) “Mobile commerce over GSM: A banking perspective on security” Masters Dissertation, Faculty of Engineering, University of Pretoria

US FFIEC *E-Banking Examination Handbook*¸ August 2003 http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf

ANNEX A: Categories of Operational Risk

(shaded are especially relevant to technology chosen)

Event category—level 1	Definition	Category—level 2	Examples
Internal fraud	Loss due to acts of a type intended to defraud, misappropriate property or circumvent regulations…which involve at least one internal party	Unauthorized activity	• Transactions not reported (Intentional) • Transaction type unauthorized
		Theft and fraud	• Fraud/ worthless deposits • Theft/ extortion. Embezzlement/ robbery
External fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent the law by a third party	Theft and fraud	• Theft/robbery • Forgery • Check kiting
		Systems security	• Hacking damage • Theft of information leading to loss
Clients, products & Business practices	Losses arising from an unintentional or negligent failure to meet a professional obligation to specific clients or from the nature or design of a product	Suitability, disclosure & fiduciary	• Fiduciary breaches • Suitability/ disclosure issues (KYC etc) • Retail consumer disclosure violations • Breach of privacy • Misuse of confidential information
		Improper business or market practices	• Improper trade practice • Money laundering
		Product flaws	• Product defects
Business disruption & system failures	Losses arising from loss or damage to physical assets from natural disasters or other events	Systems	• Hardware • Software • Telecoms • Utility outages
Execution, delivery and process management	Losses from failed transaction processing or process management, from relationship with counterparts and vendors	Transaction capture, execution and maintenance	• Data entry, maintenance or loading error • Delivery failure
		Monitoring & reporting	• Inaccurate external report (loss incurred)
		Customer intake & documentation	• Legal documents missing or incomplete
		Customer/client account management	• Unapproved access given to accounts
		Vendors & suppliers	• Outsourcing

Source: BIS (2003)

ANNEX B: Functional Survey of m-FS Technologies

Table B-1: Analysis from a Customer perspective of the technologies used for delivering banking services on mobile devices

Technologies used	Customer Interaction with service	Customer skills necessary to do financial transactions	entity/ies responsible to format up messages	Customer skills necessary to provision data service	handset side provisioning	SIM provisioning
IVR	respond to voice prompts	make calls and respond to prompts	bank server - IVR	none	none	n/a
SMS	send SMS to initiate transaction or respond with SMS to authorise transaction	send SMS, read SMS	customer	none	none	n/a
USSD1	send USSD to initiate transaction or respond with USSD to authorise transaction	send USSD and read USSD	customer	none	none	n/a
USSD2	send USSD to initiate transaction and then use interactive menu or respond with USSD to authorise transaction	send USSD, read USSD, respond to prompts and enter data	customer to initiate then session USSD server	none	none	n/a
STK WIB/S@T	select menu and interact using text menus to initiate transaction	select menu, respond to prompts and enter data	SIM Toolkit and WML from WIG/S@T server	none if pre-provisioned, else select download on menu	none	at personalisation or by download
WAP	select menu and interact in text and/or mini-web pages to initiate transaction	select browser, enter URL/select bookmark and use browser	bank server - WML	setup of data and WAP services on handset	setup download and/or manual settings of GPRS and WAP server address	n/a
HTTPS	select menu and interact in HTML web pages to initiate transaction	select browser, enter URL/select bookmark and use browser	bank server - HTML	setup of data services on handset	setup download and/or manual settings of GPRS	n/a
J2ME	select menu and interact in text and/or mini-web pages to initiate transaction	select application and use menus	bank server - application	setup of data services on handset	setup download and/or manual settings of GPRS and application download	n/a

Table B-2: Analysis from a Security perspective of the technologies used for delivering banking services on mobile devices

Technologies used	Supported on handset	encrypted path from handset to server	Bearer Information transfer	Comments	Possible to stop replay of instructions possible	Encryption keys in hardware at handset (note 5)	Possible to make transactions non-repudiable (note 9)	Ability to control the application on the handset (note 6)
IVR	all GSM	only wireless portion (note 1)	Voice and DTMF	Can add voice print verification as a 2nd biometric factor	no	no	no	n/a
SMS	all GSM	only wireless portion (note 1)	SMS	Supports access to a mFSP from multiple networks	no	no	no	n/a
USSD1	all GSM	only wireless portion (note 1)	USSD	Supports access to a mFSP from multiple networks	no	no	no	n/a
USSD2	most GSM	only wireless portion (note 1)	USSD	not possible to do checks on what is entered on handset, this has to be done on receipt at server	no	no	no	mostly
STK WIB/S@T	most GSM since 2003	SIM to bank server	SMS		yes	yes	yes	yes
WAP	middle and high end	WAP browser to bank server (note 2)	GPRS (and sometimes SMS)	may be pre-provisioned on handsets by MNO, needs GPRS and WAP browser on handset	yes	only if WIM or J177 present	yes	mostly (note 8)
HTTPS	high end	HTML browser to bank server (note 2)	GPRS		yes	no	yes	mostly (note 8)
J2ME	middle and high end	application to bank server (note 3)	SMS, USSD and/or GPRS	may be pre-provisioned on handsets by MNO, needs GPRS and J2ME on handset	yes	only if WIM or J177 present	yes	no (note 7)

Notes:

1 Dependant on MNO switching on radio encryption

2 Assuming that SSL is implemented

3 Assumes that encryption is implemented

4 It is possible to use combinations of the technologies eg initiate the transaction using a structured SMS and get called back by the bank to DTMF in a PIN

5 Having encryption keys in hardware (usually the SIM) ensures that they cannot be copied making the SIM an authentication device proving uniqueness and ensuring secure end-to-end communication

6 Being able to control the application on the handset ensures that it's integrity can be maintained

7 There are techniques to make these applications unique per session - if so then yes

8 The usual Internet banking attacks and vulnerabilities apply

9 The level to which transactions can be made non-repudiable depends upon the acceptability of electronic transactions / records as evidence as well as the legal standing of electronic signatures in the country. There are also the burden of proof requirements in criminal and civil law. Typically asymmetric cryptography is used for digital signatures, however symmetric cryptography with appropriate key management schemes can be used in some cases

ANNEX C: Use Cases – Definitions and Technology

Business considerations will likely drive the choice by an mFSP of one (or more) of these cases highlighted in Table 2.

Table 3: Main Use Cases Identified

Approach	Technologies available	Associated Risk
1 "**Use what is there**" Use existing generic mobile bearer services provided on all phones accessible directly by a user	SMS Voice/IVR USSD	There is no encryption of information so the channel from the mobile to the mFSP is open to monitoring, replay, modification and impersonation
2 "**Use mobile browsing services**" that are provided on phones - not MNO dependent	HTTPS = normal web browsing WAP phase 1 WAP phase 2	Same risks as for a PC on the Internet. Channel is less exposed than regular Internet as much of it is within MNOs
3 "**Use advanced application services**" provided on phones - not MNO dependent	J2ME	Same as client side applications on PCs. Mobiles less exposed to the Internet and the threats. However issues around the trust (integrity and authenticity) of the applications exist and need to be managed
4 "**Use a secure environment on the mobile** " provided by the MNO or MNOs	SIM Toolkit WIB, S@T and Java cards	The highest technical end-to-end security as the application runs securely within the SIM and the encryption keys are kept within the SIM.

Additionally if Use Case 1 is selected then there are the following Sub-use Cases that can be considered

Table 4: Sub-Use Cases of Use Case 1

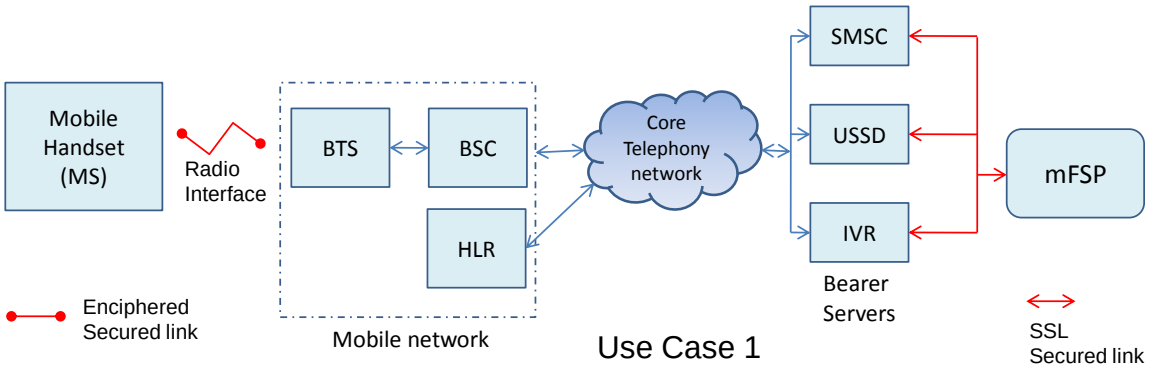
1A. Structured SMS	Send plaintext SMS with instruction mnemonic, value and PIN to the mFSP number, the SMS content is processed and a response sent back to the handset
1B. Structured SMS with confirmation and PIN authorisation via IVR	Send plaintext SMS with instruction mnemonic and value to the mFSP number, the SMS content is processed. IVR calls back asking for confirmation of transaction and PIN. PIN entered as DTMF. A SMS response sent back to the handset
1C. Structured SMS with confirmation and PIN authorisation via USSD	Send plaintext SMS with instruction mnemonic and value to the mFSP number, the SMS content is processed. USSD message sent back to handset requesting confirmation of transaction and PIN. PIN entered in USSD menu. A SMS response sent back to the handset
1D. IVR call to setup transaction and IVR call-back for PIN authorisation	Call in to IVR to setup transaction via IVR voice prompts and DTMF responses. Transaction is processed and checked. IVR calls back asking for confirmation of transaction and PIN. PIN entered as DTMF
1E. USSD menu with PIN login	USSD shortcode entered by user to initiate a USSD session, prompt for PIN sent from USSD server, PIN entered and session opened and menu displayed. Follow menu to set up transaction and then submit it for processing. USSD transaction confirmation and thereafter a confirmatory SMS

The following depict the TECHNOLOGIES IN EACH USE CASE

Use Case 1 - The mobile channel for SMS, USSD and IVR DTMF

In this Use Case, the intrinsic security available in the network is used. This intrinsically available security is not end-to-end but is instead built up of the security available at each of the individual elements that make up the path that the transaction takes from the Mobile handset through to the mFSP. Thus at insecure elements the transaction can be copied, altered, resent (replayed) and or destroyed. The vulnerabilities of the channel are analysed in Section 3.

Figure 4A: The mobile channel for SMS, USSD and IVR DTMF – Use Case 1



First, the radio link between the mobile handset and the Base Transmission Station (BTS) may or may not be secured, depending on the network. The mobile network typically comprises the BTS and Base Station Controller (BSC) and the Home Location Register (HLR). The traffic between these elements is usually not enciphered and can be read by those with access to the MNO elements and the links between them. Gadaix, E (2001), Gadaix, E (2003), Van der Merwe, Pieter B (2004) and Mobile Payments Forum (2003) provide overviews.

Thereafter the network is a standard telecommunications network "core network" containing service nodes, main switching centres and data links. From the core network, the bearer (SMS, USSD or DTMF) traffic is routed to the 'bearer servers' that turn the bearer into IP borne traffic to be sent to and received from the mFSP's servers over secure SSL links:

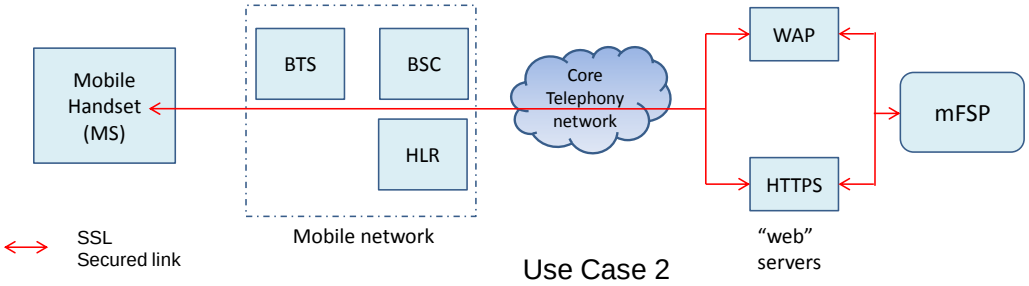
- SMS Centre (SMSC) receives and sends SMS messages from and to handsets
- USSD server communicates with handsets sending and receiving messages over USSD
- IVR server plays voice prompts, receives DTMF numbers.

When the subscriber is roaming, the mobile network will be in another country and the core telephony network will span two or more countries.

Use Case 2 – The mobile channel for IP Data Browsing

In this Use Case, because it is possible to run an explicit security program on the handset in the form of a browser with SSL it is possible to secure the data link end-to-end from the handset to the WAP or HTTPS Web Servers. The handset HTTPS browsing is the Internet banking from a mobile handset scenario.

Figure 4B: The mobile channel for IP Data Browsing – Use Case 2



This handset based browser secures all the data sent and received through a SSL link (secure tunnel or 'pipe') that passes through the mobile network all the way to the WAP or HTTPS Servers. These servers in turn communicate over a SSL secured links to the mFSP servers. In most cases these Web Servers are located at the mFSP and so form part of the mFSP's secured infrastructure. The end-to-end security is thus from the application on the handset through to the mFSPs systems.

The SSL link security is explicit running end-to-end from the handset through to the WAP or HTTPS Servers. Thus any insecurities that may exist in any of; the radio link between the mobile handset and the BTS, the path through the mobile network or through the core telephony network are bypassed.

The servers communicate with the mobile handset through the secure SSL link:

- WAP server sends WML to the handset and receives WML responses
- HTTPS server (a standard web server) sends and receives HTML messages

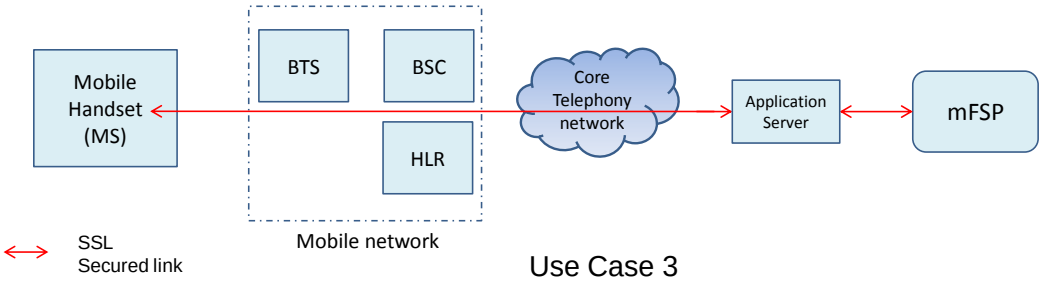
When roaming, the Mobile Network will be in another country and the Core Telephony network will span two or more countries, but since the security is end-to-end this does not affect the risk.

In this use case the threats that apply to Internet banking also apply, such as DNS poisoning, Man-in-the-middle and phishing.

Use Case 3 – The mobile channel for IP Data Applications

In this Use Case, because it is possible to run a custom made client program with explicit security on the handset, in this case a J2ME application with a cryptographic capability, it is possible to secure the data link end-to-end from the handset to the Application Server. The custom program can take the form of a banking application or a payment wallet.

Figure 4C: The mobile channel for IP Data Applications – Use Case 3



This handset based application secures all the data sent and received typically through a SSL link (secure tunnel or 'pipe') that passes through the mobile network all the way to the Application Server. This server in turn communicates over a SSL secured links to the mFSP servers. In most cases the Application Server is located at the mFSP and so forms part of the mFSP's secured infrastructure. The end-to-end security is thus from the application on the handset through to the mFSPs systems.

The SSL link security is explicit running end-to-end from the handset through to the Application Server. Thus any insecurities that may exist in either of; the radio link between the mobile handset and the BTS, the path through the mobile network or through the core telephony network are bypassed.

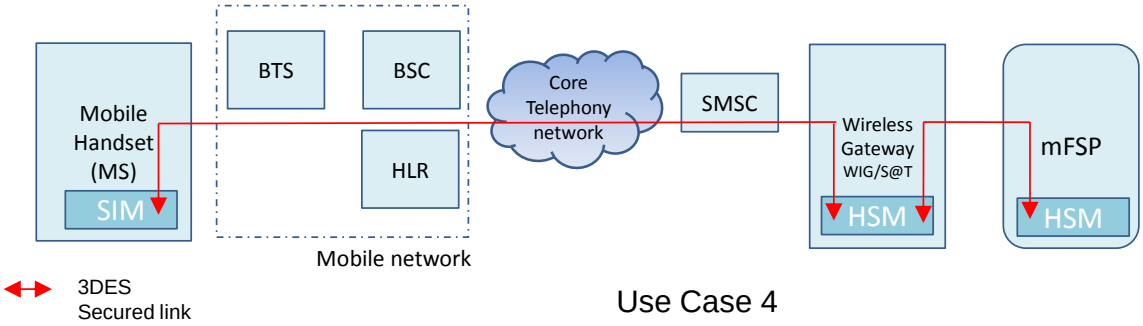
The Application server communicates with the mobile handset through the secure SSL link. The Application Server communicates to the J2ME application on the handset. This could be using HTML, WAP, XML or a proprietary protocol and using SSL or proprietary end-to-end security.

When roaming, the Mobile Network will be in another country and the Core Telephony network will span two or more countries, but since the security is end-to-end this does not affect the risk.

Use Case 4 – The mobile channel for SIM toolkit

In this Use Case an application is securely placed into the SIM. The handset communicates with the SIM and thus the application using a set of commands called SIM Toolkit. The communication allows the application on the SIM to appear as part of the celphone's menu. The display and selection of menu items and the entry of data is then possible.

Figure 4D: The mobile channel for SIM toolkit – Use Case 4



Use Case 4

The SIM has a set of security keys securely stored within it that are linked to keys in the secure High Security Module (HSM) attached to the Wireless Gateway. In this way the SIM can communicate to the Wireless Gateway securely as the traffic between the two is enciphered using these shared keys. Similarly the HSM at the Wireless Gateway shares keys with the mFSP HSM.

The application on the SIM is selected as a cellphone menu item and a transaction command then selected by the user and the necessary data entered (eg amount and destination account). On completion of the command the SIM requests the entry of a PIN. The PIN is enciphered on the SIM and then passed with the transaction in a SMS to the Wireless Gateway. Here the pin is deciphered in the HSM and then re-enciphered and sent to the mFSP where it is checked to be valid in the mFSP's HSM. In this way end-to-end assured end point links are created to send sensitive information. This is identical to the way that ATMs are set up to send PINs and other information securely from the ATM to a bank.

In most cases the Wireless Gateway is located at a MNO and so does not form part of the mFSP's own secured infrastructure. As the HSM in the wireless gateway is a secure device the path remains secure.

The explicit end-to-end security is thus from the application on the handset through to the mFSPs systems. What is more this is a guaranteed end point link in that each of the endpoints has pre-shared keys and thus the transactions sent by one end can only be opened at the other end. This is more secure than SSL links which usually do not have client side authentication or use hardware security modules.

The explicit end-to-end security is from the handset through to the mFSP Servers. Thus any insecurities that may exist in either of; the radio link between the mobile handset and the BTS, the path through the mobile network or through the core telephony network or within the Wireless Gateway are bypassed.

When roaming, the Mobile Network will be in another country and the Core Telephony network will span two or more countries, but since the security is end-to-end this does not affect the risk.

ANNEX D: Particular vulnerabilities of the Mobile Channel

General view	Comments
1. Relating to the handset:	
(i) Because the handset is more portable than say a laptop or PC, it is also more easily lost	True, but loss of handset does not compromise m-FS unless combined with compromise of the owner's PIN
(ii) The limited keypad functionality of standard handsets may effectively limit the choice of PINs, and/or resulting in PINs which can be compromised.	There is a difference between a PIN and password. Most PINs in practice are 4 or 5 digits long irrespective of what device is used for their entry. Combined with the fact that the access to the m-FS is coupled to the possession of a specific SIM card the risk is no different to the possession of a credit card and a PIN for access to an ATM and the banking functions thereon. Password choice is important where access is not tied to a specific device i.e. single factor authentication.
(iii) The small screen of the handset limits the type and form of disclosure which can be made with financial transactions	It is not obvious that more detailed disclosure forms are read or understood by customers. The usual 160 characters available in an SMS has proved sufficient to indicate transaction data – namely source and destination accounts, amount, reference numbers, remaining balance and time and date. For detailed conditions of service – these need to be made available physically.
2. Relating to the mobile channel:	
(i) Encryption is not necessarily end-to-end, creating vulnerabilities at various points where data can be intercepted and read by third parties which may act on it	This is a material issue for Use Case 1. Unauthorised information disclosure and transaction modification, replay and denial are covered in the risk analysis. However the risks associated with the vulnerabilities can be mitigated by the introduction of procedures and controls.
3. Relating to the m-payments application	
(i) Since this is often out-sourced, the interface with the provider may create additional vulnerabilities	While true, this is no different from e-banking environments and their connection to web servers and the Internet. The interface is the place where all the transactions pass and thus usually is a point of high risk.
4. Relating to developing economy environments in particular	
(i) Channel dependence: in the absence of widespread alternative e-banking channels, the risk of unavailable or unreliable service from the m-channel may be greater for users, for	The mobile network often goes where the Internet, bank branches and ATMs do not necessarily reach. "availability" has two components – the coverage of the network and the actual availability when there is coverage. On the first issue mobile networks reach many places where there is no other form of electronic communication,

the provider, and even for the economy as a whole	on the second, there will be an 'in-use' assessment of the availability of the m-FS service and if the availability is not sufficiently reliable, then the users will use it less and rely on cash more. The value of m-FS on a mobile network is in most cases not enough to financially justify the business case to an MNO to provide additional base stations to increase coverage and or reliability.
(ii) High volumes: the widespread penetration of phones and the rapid take up of some existing m-banking platforms suggests that the pressures on the system may be heightened by comparison with Internet banking	The possibility of rapid adoption simply makes it more important that the risk factors are adequately considered upfront. In two areas – the capacity of the mFSP's own systems and the congestion on the MNOs' networks. The ability of the mFSP to cope with the arrival of large numbers of financial transactions at it's computer systems is usually where the bottleneck occurs and care must be exercised to ensure that the mobile banking channel has sufficient capacity to handle the m-banking transaction load. There will still be many more voice calls, SMS and Data traffic that load the mobile networks thank m-FS transactions. M-FS transactions are usually a very small fraction of the overall mobile network load. (a SMS represents the equivalent of about 0.1 seconds of speech on a GSM network). It is important for the mFSP to verify the congestion levels existing and predicted on the mobile network with their MNO. If the mobile network is congested then the m-FS service will also be impacted. A mobile network is no different to the Internet, if the Internet is overloaded due to heavy traffic then running a financial service through it will be problematic.
(iii) Use of cash agents: given the shortage of other means of accessing cash (such as ATMs), some new services place heightened reliance on new networks of agents for handling cash. The management of these networks create operational risks.	The use of cash agents is not specific to m-FS, although it may be more pervasive. There are certainly general heightened operational and reputational risks to be managed by mFSPs; but the use of mobile technologies may in fact help to reduce risk through providing real-time value movement and real-time confirmation of transactions. Certain vulnerabilities of the mobile model to the agent are discussed in Box B in section 4.1

ANNEX E: Use Case Scenarios

The technology and processes referenced for Use Case 1 are detailed in the following tables

Common to all sub-Use Case 1
The MSISDN is pre-registered to the account, the account is opened through a agent, branch or call centre
Wrong PIN entered 3 times disables access
All transactions are initiated by the user from the handset so the user can assume that any PIN requests that they do not expect should not be answered
Value can only be sent to pre-defined beneficiaries who are registered using processes not involving the mobile channel (eg call call centre)
Only Mnemonics no actual account data is used in the menus
Transaction executed immediately on receipt by bank and defined as non-reversible instant value
All transactions after valid execution will generate a SMS notification being sent to the user (even if not initiated via the mobile channel)
Response and Alert/notification SMSs show mFSP name as the sender's originator ID as a 'Text string' not number source (prevents source spoofing off mobiles)
Users will never be sent SMS text messages that have to replied to (Pull only for transactions)
No security technology on handset to secure PINs, ensure transaction integrity or prevent resubmission
Air-gap Signalling Channel security is switched on
SMS path from Base stations through the core telecommunications network is not secured
Connection from the SMSC to the banking system is cryptographically secured

The following are the differences due to the technology deployed for Use Case 1

	1A. Structured SMS	1B. Structured SMS with confirmation and PIN authorisation via IVR	1C. Structured SMS with confirmation and PIN authorisation via USSD	1D. IVR call to setup transaction and IVR call-back for PIN authorisation	1E. USSD menu with PIN login
Transaction Initiation	Plaintext structured SMS sent from handset to initiate transaction	Plaintext structured SMS sent from handset to initiate transaction	Plaintext structured SMS sent from handset to initiate transaction	Transaction established by user selecting options using DTMF after listening to voice prompted menus	USSD service request sent from the handset to initiate the transaction
Transaction process	Send SMS with instruction mnemonic, value and PIN to an address, the SMS content is processed and a response sent back to the handset	Send structured SMS to an address, the SMS content is pre-processed and checked	Send structured SMS to an address, the SMS content is pre-processed and checked	Select transaction via IVR voice prompts and DTMF responses, it is pre-processed and checked. User told that they will be called back for authorisation	Type USSD shortcode, Prompt for PIN, follow menu to set up transaction and then submit it for processing
Transaction validation	Checked to see that the PIN is valid for the MSISDN sending the SMS message	Checked to see that the PIN is valid for the MSISDN sending the SMS message and responding via the IVR with the PIN	Checked to see that the PIN is valid for the MSISDN sending the SMS message and responding with the PIN	Checked to see that the PIN is valid for the MSISDN initiating the transaction on the IVR and responding via the IVR with the PIN	All sessions are checked to see that the PIN is valid for the MSISDN initiating the USSD session
Confirmatory response and PIN entry	A confirmatory response and request to enter a PIN is not sent back to the handset as the PIN is in the initial SMS	A confirmatory response and request to enter a PIN is initiated by the IVR calling and reading out the transaction and requesting a PIN. The user enters the PIN as a DTMF sequence. The transaction is then processed and a result SMS sent.	A confirmatory response and request to enter a PIN is sent back to the handset using USSD. The user enters the PIN and responds via USSD. The transaction is then processed and a result SMS sent.	A confirmatory response and request to enter a PIN is initiated by the IVR calling and reading out the transaction and requesting a PIN. The user enters the PIN as a DTMF sequence. The transaction is then processed and a result SMS sent.	A confirmatory response is sent back to the handset using USSD and possibly a result SMS sent as well.
Transaction passage security	Transaction passes in the clear through an insecure SMS channel from the handset through to the SMSC	Transaction passes in the clear through an insecure SMS channel from the handset through to the SMSC	Transaction passes in the clear through an insecure SMS channel from the handset through to the SMSC	Transaction passes in the clear through the core telecommunications network (voice and DTMF) from the handset through to the IVR	Transaction passes in the clear through an insecure USSD channel from the handset through to the USSD Server (and back)

PIN passage through network	Transaction and authenticator (PIN) pass in the clear through an insecure SMS channel from the handset through to the SMSC	Authenticator (PIN) passes in the clear through an insecure DTMF channel from the handset through to the IVR	Authenticator (PIN) passes in the clear through an insecure USSD channel from the handset through to the USSD server	Authenticator (PIN) passes in the clear through an insecure DTMF channel from the handset through to the IVR	Authenticator (PIN) passes in the clear through an insecure USSD channel from the handset through to the USSD server
Insecure portion of bearer	SMS path from Base stations through the core telecommunications network is not secured	Voice and DTMF path from Base stations through the core telecommunications network is not secured	USSD path from Base stations through the core telecommunications network is not secured	Voice and DTMF path from Base stations through the core telecommunications network is not secured	USSD path from Base stations through the core telecommunications network is not secured
Channel Separation	No channel separation between instruction (SMS content) and PIN as they go together over same SMS channel	Some channel separation between instruction (SMS content) and PIN. They go over the same channels however using different protocols and to different servers SMS to SMSC and PIN to IVR server	Some channel separation between instruction (SMS content) and PIN. They go over the same channels however using different protocols and to different servers SMS to SMSC and PIN to USSD server	No channel separation between instruction DTMF and PIN. They go over the same channel however using different calls (and possibly call routes)	No channel separation between instruction and PIN. They go over the same channels
Security of connection to bank	Connection from the SMSC to the banking system is cryptographically secured	Connection from the IVR server to the banking system is cryptographically secured	Connection from the USSD server to the banking system is cryptographically secured	Connection from the IVR server to the banking system is cryptographically secured	Connection from the USSD server to the banking system is cryptographically secured
User awareness of bearer failure	There is no interactivity and SMS bearer failure may not be noticed	The call is interactive so the user is aware of voice bearer failure	The USSD session is interactive so the user is aware of USSD bearer failure	The calls are interactive so the user is aware of voice bearer failure	The USSD session is interactive so the user is aware of USSD bearer failure
Message storage on the handset	Cleartext message with PIN stored in outbox of handset	SMS sent to initiate the transaction stored on the handset SMS outbox. The PIN is entered later in a IVR session and may be stored in the last dialled list	SMS sent to initiate the transaction stored on the handset SMS outbox. As the PIN is entered later in a USSD session it is not stored	DTMF to initiate the transaction and the PIN may be stored in the last dialled list	USSD sent to initiate the transaction is not stored on the handset. As the PIN is entered later in a USSD session it is not stored either
Check-back confirmation	No check-back confirmation of instruction that allows the user to confirm that they initiated the transaction	There is check-back confirmation of the SMS instruction as part of the verbal PIN request from the IVR	There is check-back confirmation of the SMS instruction as part of the PIN request sent from the USSD server	There is check-back confirmation of the IVR instruction as part of the verbal PIN request from the IVR	There is check-back confirmation of the USSD instruction as part of the PIN request sent from the USSD server
To capture a full transaction or initiate a full transaction the fraudster needs to	Have the handset or be able to spoof the SMS message path and know the MSISDN and PIN	Have the handset or be able to spoof the SMS and IVR message paths and know the MSISDN and PIN	Have the handset or be able to spoof the SMS and USSD message paths and know the MSISDN and PIN	Have the handset or be able to spoof the ingoing IVR call and respond to the IVR call and know the MSISDN and PIN	Have the handset or be able to spoof the USSD message paths and know the MSISDN and PIN

ANNEX F: List of Transaction available by Use Case

The allocation of transactions per use case was based on prudent practice as identified in interviews with existing mFSPs.

	UC1 "Use what is there"					*UC2 "Use mobile browsing services"*		UC3 "Use advanced application services"	UC3 "Use secure environment"
	UC1A	UC1B	UC1C	UC1D	UC1E				
Transactional functions	Structured SMS	Structured SMS with IVR callback for confirmation and PIN auth	Structured SMS with USSD prompt for confirmation and PIN auth	IVR with IVR callback for confirmation and PIN auth	USSD phase 2 menu with PIN login	*HTTPS / WAP*	*HTTPS / WAP with SMS OTP for value*	J2ME	SIM Toolkit S@T/WIB
Single account access	Y	Y	Y	Y	Y	*Y*	*Y*	Y	Y
Balance enquiry	Y	Y	Y	Y	Y	Y	Y	Y	Y
statement enquiry	Y	Y	Y	Y	Y	Y	Y	Y	Y
Person to Person	-	-	-	-	-	-	-	-	-
Payment to predefined on-us beneficiary	Y	Y	Y	Y	Y	Y	Y	Y	Y
Payment to predefined not-on-us beneficiary	Y	Y	Y	Y	Y	Y	Y	Y	Y
Payment to random on-us beneficiary	-	-	-	-	-	-	Y	-	Y
Payment to random not-on-us beneficiary	-	-	-	-	-	-	Y	-	Y
Generate a value transfer token	-	-	-	-	-	Y	Y	-	Y
Cash in a value transfer token	-	-	-	-	-	Y	Y	-	Y
Define a on-us payment	-	-	-	-	-	-	Y	-	Y

	UC1 "Use what is there"					*UC2 "Use mobile browsing services"*		UC3 "Use advanced application services"	UC3 "Use secure environment"
	UC1A	UC1B	UC1C	UC1D	UC1E				
Transactional functions	Structured SMS	Structured SMS with IVR callback for confirmation and PIN auth	Structured SMS with USSD prompt for confirmation and PIN auth	IVR with IVR callback for confirmation and PIN auth	USSD phase 2 menu with PIN login	*HTTPS / WAP*	*HTTPS / WAP with SMS OTP for value*	J2ME	SIM Toolkit S@T/WIB
beneficiary									
Define a not-on-us payment beneficiary	-	-	-	-	-	-	Y	-	Y
Bill Pay pre-defined beneficiary (not-on-us)	-	-	-	-	-	Y	Y	Y	Y
Buy airtime for self	Y	Y	Y	Y	Y	Y	Y	Y	Y
Buy airtime for others	-	-	Y	-	Y	Y	Y	Y	Y
Buy electricity	-	-	-	-	-	Y	Y	Y	Y
Buy from a pre-defined merchant	-	-	-	-	-	Y	Y	-	Y
Buy from any e-commerce site	-	-	-	-	-	-	Y	-	Y
Buy and sell shares	-	-	-	-	-	-	Y	-	Y
Authenticate a web session	-	-	-	-	-	-	-	-	Y
Authorise a purchase	-	-	-	-	-	Y	Y	-	Y
Switch a Debit/Credit card on / off	-	-	-	-	-	Y	Y	-	Y
Permanently disable Debit/Credit Card	Y	Y	Y	Y	Y	Y	Y	Y	Y
Activate card momentarily for web purchase	-	-	-	-	-		Y	-	Y

	UC1 "Use what is there"					*UC2 "Use mobile browsing services"*		UC3 "Use advanced application services"	UC3 "Use secure environment"
	UC1A	UC1B	UC1C	UC1D	UC1E				
Transactional functions	Structured SMS	Structured SMS with IVR callback for confirmation and PIN auth	Structured SMS with USSD prompt for confirmation and PIN auth	IVR with IVR callback for confirmation and PIN auth	USSD phase 2 menu with PIN login	*HTTPS / WAP*	*HTTPS / WAP with SMS OTP for value*	J2ME	SIM Toolkit S@T/WIB
Send your account details to someone	Y	Y	Y	Y	Y	Y	Y	Y	Y
Change the channel PIN	Y	Y	Y	Y	Y	Y	Y	Y	Y
modify alerts settings	-	-	-	-	-	-	Y	-	Y
manage scheduled payments	-	-	-	-	-	-	Y	-	Y
Alerts									
Informational	Y	Y	Y	Y	Y	Y	Y	Y	Y
Deposit alerts	Y	Y	Y	Y	Y	Y	Y	Y	Y
Profile change alerts	Y	Y	Y	Y	Y	Y	Y	Y	Y
Payment confirmation alerts	Y	Y	Y	Y	Y	Y	Y	Y	Y
Threshold alerts	Y	Y	Y	Y	Y	Y	Y	Y	Y

ANNEX G: Vulnerabilities in specific Use Cases

	Use Case 1 – SMS, IVR and DTMF End-to-end security NOT available	Use Cases 2&3 – Browsing & Applications End-to-end security available	Use Case 4 – SIM Toolkit applications End-to-end security available
1.	Storage of sent SMSs in the handset Outbox is default on handsets	Storage of cached data in input fields and auto-prompts	n/a
2.	Spoof USSD and/or SMS to phish the user Spoof SMS to phish the user, IVR confirmation spoof and PIN request phish USSD confirmation spoof and PIN request phish	e-mail, USSD and/or SMS phishing or Pharming of the user (identical to Internet attack) WAP2 allows for a push message from a server which can launch the browser and direct it to a phishing or Pharming site	Spoof USSD and/or SMS to phish the user
3.	SIM swap	SIM swap	SIM swap
4.	Movement of funds beyond defined beneficiaries	Movement of funds beyond defined beneficiaries	Movement of funds beyond defined beneficiaries
5.	Replay of messages by attacker	Replay of messages by attacker	n/a
6.	Messages between the handset to the bank that get lost	Messages between the handset to the bank that get lost	Messages between the handset to the bank that get lost
7.	Failure of the SMS and/or IVR and/or USSD Channel to the bank	Data Channel to the bank fails	Failure of the SMS and/or Data Channel to the bank
8.	The lack of protection of the SMSC and/or IVR and/or USSD servers	The lack of protection of the SMSC server	The lack of protection of the Wireless Gateway server

			The lack of protection of the SMSC server
9.	The lack of protection of the interface between SMSC and/or IVR and/or USSD servers to mFSP	The lack of protection of the interface between SMSC to the mFSP	The lack of protection of the interface between SMSC to the mFSP
10.	Infection of handset by a virus - Standard phones	n/a	Infection of handset by a virus - Standard phones
11.	Infection of handset by a virus - Advanced (programmable) Feature and Smart phones	Infection of handset by a virus, man in the middle, man in the browser and keyboard loggers – advanced (programmable) phones	Infection of handset by a virus, man in the middle, man in the browser and keyboard loggers – advanced (programmable) phones
12.	Injection of transactions into the network purporting to come from the User's MSISDN (spoofed originator ID)	n/a	n/a
13.	Capture of transaction information during radio transmission over the air	n/a	Capture of transaction information during radio transmission over the air
14.	Message path insecurity (insecure BTS/BSC, Abis and SS7 link traffic monitoring, network element exposure, false BTS)	n/a	Message path insecurity (insecure BTS/BSC, Abis and SS7 link traffic monitoring, network element exposure, false BTS)
15.	n/a	n/a	Compromise of the encryption key scheme in the SIM and Hardware Security Modules

ANNEX H: Summary Risk Evaluation by Use Case

Risk Evaluation for UC1B, UC1C, UC1D and UC1E – two phase transactions – request and PIN authorisation separate

Weak Areas	Vulnerabilities	Risk to Business	Risk to Individual	Countermeasure/s
Weak PINs	User choosing weak pin	Low	Medium	Customer Education
Process Failure	Reset of PIN by fraudster Linkage of imposter MSISDN Issuing of PIN to imposter	Medium Low Low	High High Medium	Training of staff, customer verification questions Control processes and authorizations Process inspections
Theft	Theft of handset	-	High	Customer Education Accessible and simple theft reporting and mobile channel locking
Spoofing	SMS and USSD spoofing SMS, IVR and USSD PIN request phishing	Medium Low	Medium Medium	Customer Education on what should and should not happen on the phone
Credential reroute	SIM Swap	Low	High	Processes at MNO to ensure valid SIM swaps MNO and mFSP communicating SIM Swap data mFSP SIM Swap verification processes
OTA capture Transaction	GSM security	Low	Medium	MNO monitor security settings in network and ensure traffic enciphering remains on
Channel failure	USSD, IVR or SMS links to the mFSP fail	High	Low	MNO and mFSP install redundant links and servers
Transaction harvesting	Protection of SMSC and link Protection of USSD and IVR servers and the links to the mFSP	Medium High	Medium High	MNO to control access to SMSC, separate traffic to dedicated links and ensure cryptographic and physical security is maintained
Smart Phones	Infection by malware	Medium	High	Encourage the use of low-end phones Encourage Advanced Handset users to install anti-malware software and to use UC2, UC3 and UC4

Risk Evaluation for UC1A – single phase transactions – SMS request and PIN together

Weak Areas	Vulnerabilities	Risk to Business	Risk to Individual	Countermeasure/s
Weak PINs	User choosing weak pin	Low	Medium	Customer Education
Process Failure	Reset of PIN by fraudster Linkage of imposter MSISDN Issuing of PIN to imposter	Medium Low ***Medium***	High High ***High***	Training of staff, customer verification questions Control processes and authorizations Process inspections
Theft	Theft of handset	-	High	Customer Education Accessible and simple theft reporting and mobile channel locking
Record of detail	Storage of SMS with PIN on handset	-	**High**	User education to delete sent transactions off handset
Spoofing	SMS spoofing	***High***	***High***	Customer Education on what should and should not happen on the phone
Replay and Injection	Replay of messages by attacker Spoofed originator ID injection of transactions	***Medium*** ***High***	***Medium*** ***High***	Monitor accounts for repeated execution of similar transactions over short periods
Credential reroute	SIM Swap	Low	High	Processes at MNO to ensure valid SIM swaps MNO and mFSP communicating SIM Swap data mFSP SIM Swap verification processes
OTA capture Transaction	GSM security	Low	Medium	MNO monitor security settings in network and ensure traffic enciphering remains on
Channel failure	USSD, IVR or SMS links to the mFSP fail	High	Low	MNO and mFSP install redundant links and servers
Transaction harvesting	Protection of SMSC and link	***High***	Medium	MNO to control access to SMSC, separate traffic to dedicated links and ensure cryptographic and physical security is maintained
Smart Phones	Infection by malware	Medium	High	Encourage the use of low-end phones Encourage Advanced Handset users to install anti-malware software and to use UC2, UC3 and UC4

Risk Evaluation for UC2 – Use mobile browsing services (no OTP)

Weak Areas	Vulnerabilities	Risk to Business	Risk to Individual	Countermeasure/s
Weak PINs	User choosing weak pin	Low	Medium	Customer Education
Process Failure	Reset of PIN by fraudster Linkage of imposter MSISDN Issuing of PIN to imposter	Medium Low Low	High Medium Medium	Training of staff, customer verification questions Control processes and authorizations Process inspections
Record of detail	Storage of login details in browser	-	Medium	User education to not use auto-complete functions
Credential theft	e-mail, USSD, SMS phishing or pharming WAP2 push message pharming	Medium High	High High	Customer Education on what should and should not happen on the phone
Credential reroute	SIM Swap	Low	Medium	Processes at MNO to ensure valid SIM swaps MNO and mFSP communicating SIM Swap data mFSP SIM Swap verification processes
Channel failure	Data links to the mFSP fail	High	Low	MNO and mFSP install redundant links and servers
Transaction harvesting	Protection of SMSC and link	Medium	Medium	MNO to control access to SMSC, separate traffic to dedicated links and ensure cryptographic and physical security is maintained
Smart Phones	Infection by malware	Medium	High	Encourage Advanced Handset users to install anti-malware software

Risk Evaluation for UC3 - Use advanced application services

Weak Areas	Vulnerabilities	Risk to Business	Risk to Individual	Countermeasure/s
Weak PINs	User choosing weak pin	Low	High	Customer Education
Process Failure	Reset of PIN by fraudster Linkage of imposter MSISDN Issuing of PIN to imposter	Medium Low Low	High High High	Training of staff, customer verification questions Control processes and authorizations Process inspections
Theft	Theft of handset	-	Low	Customer Education Accessible and simple theft reporting and mobile channel locking
Credential theft	e-mail, USSD, SMS phishing or pharming	Low	Medium	Customer Education on what should and should not happen on the phone
Credential reroute	SIM Swap	Low	Medium	Processes at MNO to ensure valid SIM swaps MNO and mFSP communicating SIM Swap data mFSP SIM Swap verification processes
Transaction harvesting	Protection of SMSC and link	Medium	Medium	MNO to control access to SMSC, separate traffic to dedicated links and ensure cryptographic and physical security is maintained
Channel failure	Data links to the mFSP fail	High	Low	MNO and mFSP install redundant links and servers
Smart Phones	Infection by malware	Medium	High	Encourage Smart phone users to use secure channels and install anti-malware software Make applications available from trusted sources Educate users to only use applications from trusted sources Where available switch on handset authentication services to ensure only signed and trusted applications run on handset

Risk Evaluation for UC4 - Use Advanced Application Services

Weak Areas	Vulnerabilities	Risk to Business	Risk to Individual	Countermeasure/s
Weak PINs	User choosing weak pin	Low	High	Customer Education
Process Failure	Reset of PIN by fraudster Linkage of imposter MSISDN Issuing of PIN to imposter	Medium Low Low	High High High	Training of staff, customer verification questions Control processes and authorizations Process inspections
Theft	Theft of handset	-	Low	Customer Education Accessible and simple theft reporting and mobile channel locking
Spoofing	SMS and USSD spoofing for PIN request phishing	Medium	Medium	Customer Education on what should and should not happen on the phone
Credential reroute	SIM Swap	Medium	High	Processes at MNO to ensure valid SIM swaps MNO and mFSP communicating SIM Swap data mFSP SIM Swap verification processes
Funds movements	Movement of funds beyond defined beneficiaries	Low	High	Monitor for payments outside the norm
OTA capture Transaction	GSM security	Low	Medium	MNO monitor security settings in network and ensure traffic enciphering remains on
Channel failure	USSD, IVR or SMS links to the mFSP fail	High	Low	MNO and mFSP install redundant links and servers
Transaction harvesting	Protection of SMSC and link Lack of protection of the Wireless Gateway server	Low Medium	Low Low	MNO to control access to WG and SMSC, Separate traffic to dedicated links and ensure cryptographic and physical security is maintained
Hardware security compromise	Compromise of the encryption key scheme in the SIM and Hardware Security Modules	Low	Low	Ensure that HSMs and key management processes are best practice and are properly executed
Smart Phones	Infection by malware	Medium	High	Encourage the use of low-end phones Encourage Advanced Handset users to install anti-malware software

ANNEX I: Business Model Choices - Elements of the service offering

Each mFSP will decide on its service offering which may include one or more of the service elements depicted below, each with varying scope and different risk implications.

	Service element	Sub-category	Definition	Examples	Risk implication
1	Authentication	1.1 Transactional authorisation 1.2 Session opening	Before any electronic services can be accessed the accessor must be authenticated to have valid access to the service. This can be on a per transaction basis, on a per session basis or both	Entering a PIN to authenticate a payment off a cellphone Logging onto an Internet banking site from a cellphone using a user ID and password (session)	Authentication failure could allow either • access by others to a customer's account allowing fraudulent use of the account • denial of access to the legitimate account owner
2	Informational	2.1 Information request 2.2 User transaction generated (confirmatory) 2.3 System event generated (notification)	A message from the Financial Service Provider generated in response to: • a Customer initiated request for information or • a transaction or • an event in the banking system	A mini statement request initiates a SMS text response with the last two transaction details and a available balance A card transaction is authorised on the account and a SMS text alert sent to the account holder with the merchant ID and amount A monthly amount owing on a loan and the monthly payment amount and due date is sent as a text message	The risk of compromise would be a loss of privacy and or the disclosure of information which could cause loss for the customer e.g. if delivered to the wrong phone or if intercepted, provided account number details are not included

3	Transactional	3.1 Account management	Ability to change selected key parameters of an account such as mobile PIN and notification settings	Change the mobile PIN from a known old value to a new one Change the amount above which a SMS text message is sent on the withdrawal of cash from an ATM	These functions bring much higher risk as they change authorisation, notification and control parameters
		3.2 Financial movement management	Management of payment limits and beneficiaries	Register a new beneficiary Set a maximum limit for daily transfers	These functions bring much higher risk as they change authorisation, notification and control parameters
		3.3 Transfer of value, which may be further divided into:			
		• On self	A monetary transfer between two accounts of the same user at the same institution	Move money from Savings to Credit card	Limited risk
		• On us	A monetary transfer between two users within the same financial provider	Person to person mobile transfer at a single mFSP	Risk increases of fraudulent transfer, although one institution oversees both ends and accounts, and may be able to reverse erroneous transfer
		• Not on us	A monetary transfer across two users at two different financial providers	Person to account transfer from a mFSP to another bank	Greatly increases the risks, especially if process allows one user (e.g. a merchant) to pull funds from another

Note on remittances: a remittance may be as simple as a transfer of value (2.2 and or 2.3) above, provided both sender and recipients have accounts from which and to which respectively, value may be transferred. However, even if the recipient does not have an account, it is possible for the sender to send a token, representing value which can be cashed out by the recipient at an agent.

ANNEX J: Examples of Fielded mFSP Implementations

mFSP	Business	Mode	Reg Xm	Country	Multi MNO	Multi Bank	SMS Alerts	SMS	USSD	IVR	WEB	SIM toolkit	J2ME
ABSA	Bank	Add	No	South Africa	Yes	No	▲	-	▲	-	▲	▲	-
Celpay	AA	Add	-	DRC, Zambia	Yes	Yes	▲	-	-	-	▲	▲	-
First National Bank	Bank	Add	No	South Africa	Yes	No	▲	▲	▲	▲	▲	-	-
eTranzact	PG	Add	-	Nigeria, Zimbabwe	Yes	Yes	▲	▲	-	▲	▲	-	-
GCash	AA AB	XFM	Y	Philippines	1	Yes	▲	▲				▲	
LUUP	PG AA	XFM	-	Norway EU	Yes	Yes	▲	▲					
Monitise	PG	Add	-	UK and USA	Yes	Yes	▲	▲	-	-	▲	▲	▲
mPesa	OA	XFM	No	Kenya	1	No	▲					▲	
MTN Banking	AB	XFM	Yes	South Africa	1	No	▲	-	-	-	▲	▲	-
Nedbank	Bank	Add	No	South Africa	Yes	No	▲	-	▲	-	▲	-	-
Obopay	PG	Add/XFM	No	USA	Yes	Yes	▲	▲	-	▲	▲	-	▲
Smart	AB	XFM	No	Philippines	1	No	▲				▲	▲	
Wizzit	AB	XFM	Yes	South Africa	Yes	No	▲	-	▲	▲	▲	-	-

Note: Only technologies in general commercial use are indicated. Technologies in trial or available but not commercial not shown

Key:
mFSP = mobile financial service provider
PG = payment gateway
AA = Agency Account – account balance at mFSP, main relationship at Bank
AB = Agency Bank – operate as a stand alone entity under a Bank licence
OA = Own accounts
Bank = Own Bank licence
Add = additive – extension of existing banking operation to mobile channel (account exists, registration exists, mobile channel opened)
XFM = transformational – start of new banking relationship with (account created with mobile access, new registration)
Reg Xmtn = Regulatory exemption/s

ANNEX K: Regulatory Oversight Principles

Table 14: BIS Risk Management Principles for Electronic banking, applied to m-FS

	Developing an appropriate risk management environment:	**Implications for mFS**
1	Board of directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks	The oversight should be extended to cover new mobile channels
2	The Board of Directors and senior management should review and approve the key aspects of the bank's security control process	The security control process should be extended to cover mobile channels
3	The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third party dependencies supporting e-banking	This applies equally to mobile platforms used by the mFSP
4	Banks should take appropriate measures to authenticate the identity and authorization of customers with whom they conduct business over the Internet	m-FS also requires authentication controls, which may be one or two factor
5	Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions	Only end-to-end encryption can ensure this
6	Banks should ensure that appropriate measures are in place to promote adequate segmentation of duties within e-banking systems, databases and applications	Applies equally to mobile channel, especially around vulnerabilities in SMSC or USSDC in mobile operators in Use Case 1
7	Banks should ensure that proper authorization controls and access privileges are in place for e-banking systems, databases and applications	Applies equally to mobile channel
8	Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information	Applies equally to mobile channel
9	Banks should ensure that clear audit trails exist for all e-banking transactions	Applies equally to mobile channel

10	Banks should take appropriate measures to preserve the confidentiality of key e-banking information, commensurate with the sensitivity of the information being transmitted or stored.	Applies equally to mobile channel
11	Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status prior to entering an e-banking relationships	m-FS do not necessarily combine with Internet access; therefore the issue of how best to inform customers on rights and responsibilities requires some further consideration
12	Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions in which supplying e-banking services	Applies equally to mobile channel
13	Banks should have effective capacity, business continuity and contingency planning processes to ensure the availability of e-banking systems and services	Applies equally to mobile channel
14	Banks should develop appropriate incident response plans to manage, contain and minimize problems from unexpected events including internal and external attacks that may hamper provision of services and products	Applies equally to mobile channel

Reference: BIS (July 2003)

Table 15: BIS Guidelines for Operational Risk (ORX):

No	Principles for supervisors	Comment
8	Banking supervisors should require that all banks have an effective framework for ORX	This report has highlighted some of the risk components and proposed the structure of what should be in a risk framework
9	Supervisors should conduct regular independent evaluation of a bank's ORX process	In addition to regular evaluation of the ORX process, supervisors need to keep updated knowledge of emerging vulnerabilities from new technology and risk experience in other jurisdictions

Reference: BIS (February 2003)

Box C: Regulators' checklist

The following are discussion points or information which should be sought from mFSPs:

1. First engagement with a new mFSP

   - Information to seek in advance:
     - Strategy and business plan for rollout of mFS
     - Handset minimum requirements and channels to be used
     - Nature of services proposed
     - Transaction work flow procedures and standards
     - System architecture depicting the core mFSP systems, interconnections to other financial systems and the mobile network and it's elements involved in m-banking
     - Organogram showing responsibilities for risk management clearly
     - Names and descriptions of software packages used, and vendors
     - Completed risk matrix as above

     This information should give a background which would enable the regulator to understand:
     - The Use Case (1-4) to be identified
     - An assessment of the environmental risk factors relating to the entity
     - A comparison of the risk ratings with conventional practice (such as shown in this report)
     - An assessment of the adequacy of the control measured proposed

   - Meeting: in the course of meeting with the mFSP, discussion would then centre around:
     - Divergences in risk opinion (esp. where mFSP has rated risk lower or higher), where the reasons should be understood and noted
     - Risk mitigation strategies—how these are to be embedded in organizational procedures and controls
     - Regularity of review or update

2. Ongoing engagement and regular review: regular reviews of the m-FS offering should centre around:

   a. What elements of service offering or technology have changed, if any, and why
   b. Statistics and trends on intrusions, fraud incidents, customers complaints
   c. New vulnerabilities identified
   d. New countermeasures introduced
   e. System and process security audits to verify that the expected operational and security standards are being maintained within the mFSP, and identify any shortcomings that need attention
   f. Evidence that control measures are implemented and working e.g. audit or compliance reports
   g. Evidence that the overall risk framework has been updated to take into account these risks
   h. Evidence that the significant risks have been considered and reviewed at the appropriate governance level.

For further detail on requirements, see FFIEC (Aug 2003) E-banking request letter items (page A-19)

ANNEX L: Emerging Issues and Case Study

Box D: The malware risk associated with Smartphones

"Companies brace for mobile maliciousness" CNN 23 November 2007
http://edition.cnn.com/2007/BUSINESS/11/21/digital.malware/index.html

"Most computer users live with the knowledge of online scammers and malicious code. But what about cell phone users? Handsets, after all, are getting more advanced all the time. As the tagline for Nokia's N95 smart phone suggests: 'It's what computers have become.'

"So if computers are susceptible to attacks, why not computer-like handsets? After all MMS, Bluetooth and Internet access are increasingly standard features on phones, and they all have the potential to spread malicious software, or 'malware.'

"Possibilities include spyware geared to send information to a third party, or viruses designed to disable functions. You might also receive fraudulent links on your cell phone -- just as you do you on your PC -- trying to trick you into giving away, say, your voicemail PIN.

"In the U.S. last year, mobile operators reported five times more virus or spyware infections on mobile devices than in 2005, according to Frost & Sullivan. And 'other regions follow a similar pattern of increasing numbers of security events,' adds Katie Gotzen, a mobile security analyst with the firm.

"Frost & Sullivan predicts the global market for anti-malware products for mobiles will jump from $61.4 million in revenues this year to more than $2 billion in 2014."

Comment:

From a risk perspective Smart phones must be treated the same as PCs accessing the mFSP services. All the traditional malware exploits against Internet connected PCs are applicable to Advanced Handsets, specifically Smart phones and some feature phones too.

This is an example of where technology convergence of the PC and the mobile handset has opened vulnerabilities from the PC world in the mobile handset world.

Anti-malware software for mobiles is maturing and consideration should be given to user awareness programs and promotion of anti-malware programs.

Standard handsets do not have the user programmability vulnerability making the choice of UC1 and or UC4 on standard handsets a countermeasure to the malware vulnerability.

Box E: Case study: technology-related operational risk incident

Ten suspects nabbed in SIM-swop scam
Pretoria News; January 02, 2008; pg.2

"The Novalis Ubuntu Institute lost almost R100 000 when the Johannesburg-based syndicate hacked into its bank account.

"The syndicate managed to obtain the institute's one-time security password needed to carry out online transactions. They persuaded MTN to swop a SIM card so that the one-time password was sent to them, and not to Ubuntu's chief financial officer, Anne-Lise.

"A sim-swop allows a cellphone user to replace a lost SIM card while keeping the same cellphone number.

"Jones said unit investigators discovered that bank officials were linked to the syndicate. 'The intensive investigation led detectives to check cellphone records of bank officials and cellphone service provider staff (mostly franchise staff), thereby linking them to the syndicate,' said Jones. 'The investigation revealed that staff within the banking sector profiled potential victims and provided vital information to the two suspects and their syndicate while cellphone franchise (staff) provided the syndicate with information about the victims to facilitate fraudulent sim swops.' " - Staff Reporter

Comment:

A SIM swap essentially moves your phone number onto another phone. Typically on log-in to an Internet banking site a One Time Password (OTP) is sent to the user's cell phone. This ensures that even if their ID and password are known the attacker still needs to receive and use the OTP SMSed to their cellphone to succeed. The vulnerability was that the person's phone number could be moved to another SIM in the possession of a fraudster.

The attack was to engineer a process failure and get customer care employees to swop the target's phone number to a SIM held by the attacker. The attacker gets the ID and password for the target account through social engineering (eg Phishing) or insider fraud and then logs in on the Internet. The bank sends the OTP to the phone number which is now linked the attacker's phone and the attacker thus completes the impersonation attack, now having the ID and password and the OTP and has access to the account.

This is an example of where a new technology was introduced – namely OTP SMSed to a user's cellphone, in response to an existing vulnerability that was materialising, namely log-in credential theft. The new technology forced the attackers to search for a vulnerability, which they found and exploited.

This vulnerability exists for all mobile banking use cases that make use of the possession of a SIM linked to a cellphone number (MSISDN) as an authentication factor.

The SIM swap vulnerability is addressable through increased process controls around the SIM swap. The ID and Password theft vulnerability is addressable through increased customer education and awareness programmes.

Once the risk of account access compromise is reduced through more stringent process controls the attackers move on to attack other vulnerabilities.

This attack also raises interesting liability issues at a business level. Who is liable? The bank for relying on the assumption that the SMS message will go to the correct recipient, the MNO for an exploitable SIM swap process, the SIM swapping agent for improper process execution or the customer for using the OTP system and for the ID and password compromise?

ANNEX M: Comparison of GSM and CDMA Mobile Channel Technology

The services supported by CDMA and GSM technology are compared below.

Channel Technology	**GSM**	**CDMA**	**Comments**
IVR	Available	Available	Calls to IVRs and DTMF dialling standard
Structured SMS	Available	Available	Text messaging available
USSD	Available	Not available	Not implemented
SIM toolkit (WIB / SAT / custom)	Available	R-UIM / CCAT	Not available on all phones. Not as widely used as SIM Toolkit in the GSM world
J2ME	Available	Available	Available on feature phones and smart phones. Feature phones tend to be functionally locked down
WAP	Available	Available	Available on feature phones and smart phones. Feature phones tend to be functionally locked down
HTTPS – Internet browser	Available	Available	Available on feature phones and smart phones. Feature phones tend to be functionally locked down

Notes:

- CDMA have defined a R-UIM which is the same as a USIM the 3G defined SIM card. This is available on an MNO required level and is ordered from the handset manufacturer. Some CDMA handsets (eg many in the USA) do not have the capability to take a SIM/U-RIM
- CCAT - CDMA Card Application Toolkit has been developed. Operator specific deployments
- A “Dedicated secure application environment” on a handset has to date not had adoption in the GSM mobile environment. The main issue being the control over the environment as well as the security available/provided. This is however an area that may develop in future. To date a good example of a secure, managed and controlled environment on a handset is the BREW environment developed by Qualcomm for CDMA handsets.

ANNEX N: List of Interviewed Organisations

Organisation	Person	Title
ABSA Bank	Christo Very	Managing Executive : Digital Channels
Celpay	Michael Kitsisa	Acting Chief Technical Officer
First National Bank	Len Pienaar	CEO - Mobile and Transact Solutions
Fundamo	Hannes van Rensburg	CEO
GSM Association	Charles Brooksen	
G-Xchange Inc	Rizza Maniego-Eala Rodell Garcia	CEO CIO, Globe Telecom
LUUP	Thomas Pietsch	Business Development Director International
MTN Banking	Dave Parratt	COO
Monitise	Steven Atkinson	CIO
Nedbank	Lee Albertyn	Head: Virtual Channels
Obopay	Johan Tumminaro	CTO
Qualcomm / Firethorn	David Wood	Sr. Director, Business Development, Firethorn/MCommerce
Symantec Corporation	Paul Miller	Managing Director, Mobile Security
Vodafone	Richard Murray	
Wizzit	Brian Richardson	CEO

ANNEX O: Glossary of Terms

Abbreviation	Term	Description
m-FS	Mobile Financial Services	Financial Services delivered over mobile telephony networks through mobile handsets
mFSP	Mobile Financial Services Provider	The entity which is directly interfacing with the end customer to provide mobile financial services
ATM	Automated Teller Machine	A machine that dispenses money when you use an authorized bank card and PIN number
ASP	Application Service Provider	A business that provides computer-based services to customers over a network. Software offered using an ASP model is also sometimes called On-demand software or software as a service (Wikipedia)
BSC	Base Station Controller	A Base Station Controller controls a set group of BTSs. Together the BTS and BSC systems are known as the BSS or Base Station System (BSS)
BTS	Base Transceiver Station	Technical term for a mobile phone base station. A BTS contains the transmit and receive technology and also the aerials to supply a radio cell
DTMF	Dual-tone multi-frequency signalling	DTMF used for telephone tone dialling. It is a method for instructing a telephone switching system of the telephone number to be dialled, or to issue commands to switching systems or related telephony equipment
GSM	Global System for Mobile Communications	The system used by most countries for mobile cellular communications
HSM	Hardware Security Module	A tamperproof Hardware based security module that is used to secure security keys and is usually located in a security server
J2ME	Java 2 Platform, Micro Edition	A Wireless Toolkit supplied by Sun for developing Java based applications for mobile devices. Now known as Sun Java Wireless Toolkit.
MNO	Mobile Network Operator	Mobile traffic passes through the mobile operator's network as voice, SMS, DTMF, IP data or USSD
NFC	Near Field Communication	A short-range high frequency wireless communication technology which enables the exchange of data between devices
OTA	Over the Air	Standard used for transfer of information between device and wireless network. Usually it is used to upload new software to mobile phones, or download/upload content (such as ringtones, pictures)
OTP	One Time Password	The password (usually a random sequence of digits and or letters) sent from a bank to a customer's mobile handset for entry by the customer to authenticate themselves into the banking channel that they are using eg Web browser. Considered as a second authentication factor.
Malware	Malware	Any type of malicious software program, typically installed illicitly, including viruses, Trojans, worms, key loggers,

		spyware, and others
MSISDN	Mobile Systems International Subscriber Identity Number	A number uniquely identifying a subscription in a GSM or UMTS mobile network. The mobile phone's telephone number by which it is known to the world.
Pharming	Pharming	An attack to redirect a traffic to a bogus website or server. The result is that individuals are directed to web sites that seem to seem to be genuine, but are actually false. An attack in which a user can be fooled into entering sensitive data such as a password or credit card number into a malicious website that impersonates a legitimate website
Phishing	Phishing	A social engineering technique whereby an attempt is made to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication eg SMS exchange or e-mail (Wikipedia)
PIN	Personal Identification Number	A sequence of digits used to verify the identity of the holder of a token. The PIN is a kind of password.
POS	Point-of-Sale	The physical machine that allows a merchant to swipe a credit card through to initiate a transaction, most common in retail environment. The location where a sale is completed
S@T	SIM Alliance Toolkit	An industry standard from the SIM Alliance for WAP based services via any GSM phase 2+ phone that is not WAP enabled. Based on a SIMtoolkit browser resident in the SIM
SAT or STK	SIM Toolkit	SIM Toolkit provides a set of commands which allow applications, existing in the SIM, to interact and operate with a mobile client which supports the specific command(s) required by the application. Using the SIM Toolkit, applications can be downloaded to the SIM in a secure manner. S@T and WIB are mini-browsers implemented in the SAT environment
SIM	Subscriber Identity Module	A mini-smartcard that is inserted into a mobile handset It is used to authenticate the mobile to the mobile radio network The SIM may be programmed to provide security services on the mobile
SMS	Short Message Service	The term used to refer to a text message sent to or from a handset.
SMSC	Short Message Service Centre	A network element in a mobile telephone network which delivers SMS messages
Social engineering	Social engineering (computer security)	A collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most cases the attacker never comes face-to-face with the victim (Wikipedia)
Spoofing	Spoofing	Fraudulent electronic communication (eg SMS) in which the sender address is altered to appear as though the SMS originated from a different source
SSL	Secure Sockets Layer	A security protocol used for sending encrypted information for Internet transactions and communications between client

		web browsers and web servers
SS7	Signalling System 7	An architecture for performing out-of-band signalling in support of the call-establishment, billing, routing, and information-exchange functions of the public switched telephone network
USSD	Unstructured Supplementary Service Data	defined within the GSM standard in the documents GSM 02.90 (USSD Stage 1) and GSM 03.90 (USSD Stage 2). USSD provides session-based communication. It is a technology used by the network to send information (usually text menus) between a mobile phone and an application on the network. USSD will allow the subscriber to request information in short codes (starting with * and ending with #), or menus from the network via their cellphone
WAP	Wireless Application Protocol	A set of communication protocol standards to make accessing online services from a mobile phone simple
WIB	Wireless Internet Browser	Specified by SmartTrust the WIB is a SIM-based micro browser for interpreter environments. Based on a SIMtoolkit browser resident in the SIM
WML	Wireless Mark-up Language	An XML language used to specify content and user interface for WAP devices
XML	eXtensible Mark-up Language	A widely accepted way of sharing information over the Internet in a way that computers can use, regardless of operating system

Definitions sourced off the WWW using Google “Define:” and then modified as appropriate for this report.

Alliance for Financial Inclusion
Bringing smart policies to life

Mobile Financial Services Working Group (MFSWG)

Servicios financieros móviles
Riesgos tecnológicos

La presente nota de orientación fue desarrollada por el Grupo de Trabajo de Servicios Financieros Móviles (MFSWG) de AFI, con el fin de identificar los tipos de riesgos tecnológicos inherentes a los servicios financieros móviles y las estrategias para su gestión.

Nota de orientación No.2
Julio de 2013

Contenido

Al reconocer el potencial de los servicios financieros móviles (SFM), el Grupo de Trabajo de Servicios Financieros Móviles (MFSWG) se creó para brindar una plataforma dentro de la red de AFI para el debate de los formuladores de políticas públicas en cuanto a problemas normativos relacionados con los SFM. El grupo de trabajo promueve el amplio uso de los SFM como solución clave para una mayor inclusión financiera en países emergentes y en desarrollo. El objetivo del grupo es estimular el debate y el aprendizaje entre los formuladores de políticas públicas y promover una mayor coordinación entre los diversos actores de los SFM, tales como los entes reguladores financieros y de telecomunicaciones, así como proveedores bancarios y no bancarios.

Contexto

Los servicios financieros móviles (SFM) ofrecen la posibilidad de una mayor eficiencia y conveniencia en las aplicaciones de pago y también podrían proporcionar una base para iniciativas de inclusión financiera.Sin embargo, para que los SFM puedan cumplir su promesa, los proveedores de servicios y los entes reguladores deben considerar seriamente la seguridad de la plataforma dentro de este nuevo mercado.

Debido a que los modelos de negocio, las necesidades del mercado y la abstención normativa varían entre países, esta nota no establece un único conjunto de políticas adecuado para todos los contextos. En cambio, tiene la intención de ayudar a orientar la formulación de políticas públicas, al identificar los tipos de riesgos tecnológicos que son habituales en los servicios financieros móviles y las estrategias para manejarlos. Por lo tanto, esta nota registra gráficamente el flujo de información en operaciones de SFM, identifica los tipos de riesgos tecnológicos que se aplican a dichos flujos de información, y elabora marcos para la gestión y monitoreo de los riesgos. El objetivo de esta nota es ayudar a que los entes reguladores empiecen a pensar acerca de los riesgos tecnológicos en los SFM de una manera flexible que será útil para la toma de decisiones futuras.

Un comentario acerca del lenguaje: A lo largo de esta nota, se utiliza el término **"amenazas"** para describir las clases de disfunciones en la oferta de SFM y el término **"riesgos"** se refiere a la aplicación de dichas amenazas a los procesos actuales implícitos en una oferta de SFM. En este sentido, los riesgos son casos de amenaza que pueden observarse en operaciones reales.

Flujos de información en SFM

Los entes reguladores necesitan familiarizarse con la forma en que la información fluye dentro de la red de SFM, con el fin de analizar los riesgos tecnológicos que evolucionan en dicho ambiente. Si usted entiende la forma en que cada elemento de la red maneja la información, usted podrá identificar los tipos de controles que se requieren para garantizar la seguridad de dicha información. La Figura 1 es una representación esquemática de dichos flujos de información para SFM basados en la banca que se ofrecen en colaboración con un operador de redes móviles (ORM).

Los usuarios de SFM inician procesos utilizando sus teléfonos. La información proporcionada por cada usuario se envía a la estación base del ORM.[1] En una red GSM, la estación base recibe una solicitud de canal del teléfono móvil y la reenvía al ORM del usuario. En operaciones de SMS, los paquetes de datos que contienen información se procesan en un centro de servicio de mensajes cortos (SMSC, por sus siglas en inglés) y se enrutan al servidor de la aplicación de SFM. A su vez, el servidor de la aplicación de SFM entrega la información de la operación a una puerta de enlace *(gateway)* — la interfaz entre la red del ORM y la red del banco. Entonces, el paquete de datos se somete a una verificación de seguridad y, sujeto a aprobación, se enruta a la red interna del banco para autorización y procesamiento posterior. La red del banco almacena la información financiera y no financiera del usuario y autoriza la operación solicitada por éste. Debido a que este proceso funciona al revés, en este punto el usuario recibe la notificación de que la operación se ha concluido.

Figura 1: Infraestructura de los servicios financieros móviles (utilizando tecnología STK)

[1] Los mensajes enviados por el teléfono tienen un código de identificación que utilizará entonces la estación base para determinar si la red utilizada por el remitente le pertenece. Si es así, el mensaje se reenviará a la red de la empresa de telecomunicaciones. De lo contrario, el mensaje se omitirá. El teléfono continuará buscando una estación base que atienda su solicitud, hasta que haya ocurrido la conexión completa.

Clasificación de amenazas tecnológicas

Resulta importante comprender el flujo de información en operaciones de SFM debido a la variedad de riesgos tecnológicos que están presentes en cada etapa de este flujo. De hecho, resulta útil clasificar los riesgos tecnológicos de acuerdo con su categoría más amplia de amenaza. Dhillon (2007) identifica seis categorías generales de amenazas en los sistemas de información:

Modificación: cuando se tiene acceso no autorizado a la información en el sistema y ésta se cambia sin permiso.

Destrucción: cuando se destruye o pierde el hardware, software, datos o canal de comunicaciones.

Revelación: cuando los datos se ponen a disposición sin el consentimiento del titular.

Interceptación: cuando una persona o software no autorizados obtiene acceso a fuentes de información, permitiendo que programas y otra información confidencial se copie sin autorización.

Interrupción: cuando el servicio o los recursos no están disponibles para su uso, ya sea accidental o intencionalmente.

Fabricación: cuando un usuario no autorizado inserta operaciones falsas en un registro o las agrega a una base de datos.

Este marco de amenazas puede aplicarse al diagrama de proceso de los flujos de información en SFM.

La Figura 2 presenta una visión no exhaustiva de los puntos en los cuales las amenazas pueden introducirse en los flujos de información de SFM.

Tabla 1: Clasificación de amenazas tecnológicas de los SFM

Amenazas	Datos	Software	Hardware	Canal de Comunicaciones
Modificación	Ocurre durante el almacenamiento, transmisión y cambio en el hardware físico	Sucede cuando se altera el software para realizar funciones o cómputos adicionales	–	Ocurre cuando los paquetes se enrutan hacia un destino diferente
Destrucción	Causada por fallas en el hardware y/o software	Destrucción debido a intenciones maliciosas, es decir, software malicioso *(malware)*	Ocasionada por desastres naturales, tales como inundaciones, incendios o por ataques terroristas	Causada por cortes en las líneas de fibra óptica o líneas arrendadas debido a eventos inesperados, es decir, inundaciones, robo o construcción de vías
Revelación	Ocurre cuando hay un acceso no autorizado a los datos/información de otra persona	–	–	–
Interceptación	Sucede cuando usuarios no autorizados reproducen la información confidencial	Ocurre cuando los programas de software se copian en forma ilegítima a partir de una fuente informática	Sucede cuando los usuarios no autorizados obtienen acceso físico al hardware	Ocurre cuando un tercero es capaz de interceptar (escuchar) puertos sin el conocimiento del usuario legítimo
Interrupción	–	Causada por el borrado de programas de software y/o funcionalidades específicas Puede ser el resultado de corrupción en el sistema operativo	Ocasionado por hardware dañado	Causado por ataques maliciosos, tales como saturación y denegación de servicio Puede ser el resultado de desastres naturales, interrupción del suministro eléctrico, problemas con las estaciones base o problemas en la red
Fabricación	Ocasionada por ataques de suplantación de identidad *(phishing)*	–	–	–

Referencia: Dhillon, G. (2007). Principios de seguridad de los sistemas de información: Texto y casos *(Principles of Information Systems Security: Text and Cases)*.

Identificación de riesgos tecnológicos de los SFM

El marco de clasificación que brinda el lenguaje de las amenazas puede ayudarnos a darle sentido a la profusión de riesgos tecnológicos que aquejan a los SFM. Estos riesgos son específicos y variados, pero colocarlos en una ontología de amenazas puede ayudar a organizarlos, evitarlos y eventualmente remediarlos. Este apartado destaca los riesgos específicos y los clasifica de acuerdo con la clase más amplia de amenazas a la que pertenecen.

Amenaza: Modificación

Infección por software malicioso *(malware)* móvil (riesgo)

Los ataques de software malicioso son comunes en el entorno PC y se espera que pronto se extiendan a los dispositivos móviles de manera repentina. Los ataques de software malicioso en teléfonos celulares pueden ocurrir de las siguientes maneras:[2]

- Los virus/troyanos/gusanos del software malicioso pueden diseminarse vía Bluetooth y MMS.
- El software malicioso puede manipular al usuario al enviar un mensaje SMS.
- El software malicioso puede infectar archivos.
- Los atacantes pueden obtener acceso remoto a los teléfonos celulares al propagar software malicioso.
- Cuando se descarga, el software malicioso puede cambiar los íconos y las aplicaciones del sistema.
- El software malicioso puede instalar funciones y aplicaciones no operativas.
- El software malicioso es un canal útil que puede utilizarse para instalar otros programas maliciosos.
- El software malicioso puede robar datos o información que capture el usuario y bloquear el uso de las tarjetas de memoria.

Amenaza: Revelación

Legibilidad de información financiera crítica de los clientes vía SMS (riesgo)

La legibilidad resulta una gran inquietud cuando se utilizan SMS para tener acceso a cuentas y recibir notificaciones sobre actividades previas. Los SMS se transmiten y reciben en texto simple y dicho protocolo no utiliza ninguna técnica de cifrado. En los casos de robo del dispositivo y software malicioso, los usuarios no autorizados pueden tener acceso total a la cuenta de un cliente.

Figura 2: Amenazas del sistema de información a los SFM

Amenazas del Sistema de Información en los SFM

[2] Gostev, A., 2006.

Amenaza: Revelación

Exposición de datos críticos debido a cifrado no seguro de extremo a extremo (riesgo)

El Protocolo de Aplicaciones Inalámbricas (WAP, por sus siglas en inglés) es una aplicación estándar que permite que los teléfonos móviles tengan acceso a la Internet. Los teléfonos celulares con tecnología WAP utilizan navegadores similares a los que utilizan las computadoras, aunque tienen modificaciones para adecuarse a las restricciones de dichos teléfonos. El WAP utiliza el mismo enfoque estratificado que el TCP-IP. Un sitio web normal basado en la computadora permite a los usuarios tener acceso a la Internet mediante el uso del HTML del protocolo de la capa de aplicación. Asimismo, los consumidores que cuentan con teléfonos móviles con tecnología WAP pueden tener acceso al mismo sitio web utilizando sus teléfonos por medio del protocolo WML (Lenguaje de Marcado Inalámbrico), que es una capa de aplicación del WAP. La única diferencia entre los dos es el tamaño y resolución de la visualización (ya que el sitio web se convierte para atender las restricciones del teléfono móvil). Por lo tanto, las transmisiones no cifradas son vulnerables a quedar expuestas a partes no autorizadas.

Amenaza: Interrupción

Falta de disponibilidad del canal de comunicaciones debido a ataques de denegación de servicio (riesgo)

Los ataques de denegación de servicio (DOS, por sus siglas en inglés) hacen que un recurso computacional no esté disponible mediante la saturación o el consumo del recurso del componente. El objetivo más común de los ataques DOS son los servidores y bases de datos, que también pueden afectar las redes móviles, debido a que tanto el entorno con cables como el inalámbrico utilizan la misma infraestructura.

Amenaza: Interceptación

Ataque por secuencias de comandos entre páginas web *(cross-scripting attack)* en USSD (riesgo)

El protocolo de comunicación USSD permite una transmisión de datos más rápida en comparación con el SMS. A diferencia del SMS, el USSD utiliza una conexión directa entre el remitente y el destinatario. Es un canal de comunicación orientado a la sesión, donde la aplicación USSD se utiliza como interfaz entre el proveedor de telecomunicaciones y la cuenta bancaria del cliente. El USSD también puede manejarse utilizando aplicaciones basadas en la web, por lo que es propenso a ataques por secuencias de comandos entre páginas web. En dichos ataques, un usuario malicioso explota la vulnerabilidad de la aplicación basada en la web instalada en el teléfono móvil del usuario para manipular operaciones (al inyectar una secuencia de comandos Java o SQL a fin de robar la información crítica del usuario). También puede llevar a cabo actos maliciosos en la base de datos, tomar la sesión activa de otro usuario y conectar a usuarios a servidores maliciosos.

La presente lista de riesgos no pretende ser exhaustiva, pero ilustra los tipos de riesgos que cualquier oferta de servicios debe manejar. Tomando en cuenta dichos riesgos, ahora nos abocamos a los principios de la gestión de riesgos y supervisión que los entes reguladores deben conocer.

Riesgos tecnológicos de los SFM: Gestión y monitoreo

PRINCIPIOS

Existen cinco principios clave que sirven de guía para la gestión de riesgos en los SFM: Confidencialidad, Integridad, Disponibilidad, Autenticación e Irrefutabilidad. Cada uno de esos principios se analiza a continuación.

Tabla 2: Modelo del impacto de los riesgos

PROBABILIDAD	IMPACTO				
	Desastroso	Alto	Moderado	Bajo	Insignificante
Casi segura	E	E	E	A	M
Probable	E	E	A	A	M
Posible	E	E	A	M	B
Poco probable	E	A	M	B	B
Rara	A	A	M	B	B

NIVEL DE RIESGO: E= Extremo A= Alto M= Moderado B= Bajo

Confidencialidad: para proteger los datos del usuario de acceso no autorizado o robo. Es importante distinguir entre datos financieros y no financieros, debido a que diferentes principios de confidencialidad se aplican a cada uno de ellos. En general, los datos financieros requieren normas de cifrado más estrictas para su visualización, almacenamiento y transmisión. Los números de identificación personal deben almacenarse en forma cifrada y no estar disponibles para el personal del proveedor del servicio. Fuertes normas de criptografía deben aplicarse a los datos que se transmiten por las redes públicas, tales como la Internet y las redes celulares. Los datos no financieros pueden mantenerse en forma confidencial con medidas un poco menos estrictas, tales como establecer cortafuegos *(firewalls)*, implementar sistemas de prevención y detección de intrusos, y utilizar controles de acceso.

Integridad: la entereza, precisión y confiabilidad de los datos que se presentan. Para validar la integridad de los datos, debe verificarse el proceso que identifica los campos faltantes, llevarse a cabo verificaciones de secuencias y verificarse el resumen criptográfico total[3] así como la longitud variable. La integridad de los datos resulta más importante durante la transmisión, ya que es más probable que la interceptación y manipulación de datos ocurran en esta etapa.

Disponibilidad: los datos y servicios deben ser accesibles cuando los usuarios legítimos deseen utilizar los SFM. Existen diversos escenarios que pueden amenazar la disponibilidad de los datos y servicios. Los riesgos tecnológicos de la disponibilidad del servicio incluyen desastres ambientales (tales como interrupciones del suministro eléctrico, ataques terroristas y causas de fuerza mayor) y actos maliciosos, tales como ataques de denegación de servicio.

Autenticación: establecer la identidad del usuario y del proveedor de servicios.

- Los **usuarios** deben confiar en que el huésped que solicita la conexión está autorizado y que no hay terceros involucrados en la conexión entre la terminal y los servidores huésped. Lo anterior incluye también control de acceso, control de permisos y autenticación de contraseñas.
- Los **proveedores de servicios** deben confiar en que la persona que tiene acceso a los datos es quien dice ser. Los registros de auditoría evalúan la validez y congruencia de los datos que circulan en la red y son herramientas importantes para verificar si los comandos han sido ejecutados por usuarios legítimos. De esta forma, los entes reguladores deben ser capaces de considerar la forma en que los proveedores de servicios monitorean los registros de auditoría. Asimismo, deben establecerse procedimientos y operaciones administrativos para controlar el acceso a la información de los clientes y comprender las vulnerabilidades del sistema.[4]

Irrefutabilidad: la propia protección del proveedor de servicios del posible comportamiento abusivo por parte de los consumidores y empleados, garantizando la conclusión y seguridad de la operación. Asegurarse de que las personas acepten los términos y condiciones del servicio antes de llevar a cabo cualquier acto y utilizar firmas digitales para prevenir que las personas nieguen sus actos. Los certificados de clave pública también permiten a los proveedores de servicios rastrear el origen de la operación en caso de que no haya un intercambio directo de información entre entidades.

Estos principios ofrecen un marco para entender las vulnerabilidades en los SFM, que complementan el debate acerca de las amenazas y riesgos. Considerar las amenazas como infracciones a los principios administrativos claves, puede ayudar a determinar la solución normativa necesaria. El proceso de gestión de riesgos ayuda a formular y calibrar dicha solución más a fondo.

PROCESO

La gestión de riesgos se desarrolla al (1) evaluar los riesgos, (2) analizar dichos riesgos por impacto esperado y probabilidad, y (3) monitorear dichos riesgos de acuerdo con las expectativas y probabilidad del impacto.

1) **Evaluación de riesgos.** Los criterios de evaluación permiten que se analicen a profundidad las posibles amenazas al sistema. Se sugieren los siguientes criterios para los SFM:
   - Viabilidad de la amenaza: ¿Ya ocurrió esta amenaza? ¿Qué elementos se vieron afectados? ¿El software? ¿El canal? ¿Cuánto tiempo pasó antes de que se identificara esta amenaza?
   - Incidentes registrados: ¿Cuántas veces ha ocurrido esta amenaza durante los últimos 10 años? ¿Durante los últimos cinco años? ¿Cuántas dependencias se vieron afectadas?

[3] Se utiliza un resumen criptográfico total para verificar la integridad y precisión de los datos. Si existen cambios o puntos faltantes, el nuevo resumen criptográfico total no se conciliará con el original.

[4] Esos procedimientos pueden utilizarse para entender el flujo de información dentro del proveedor de servicios e identificar dónde pueden explotarse las vulnerabilidades. Más aún, identifica en forma eficaz las autoridades dentro del proveedor de servicios, facilitando la identificación de responsabilidades en caso accidental de revelación de información o uso no autorizado. Los controles de permiso (es decir, leer, escribir, ejecutar, borrar) se diseñan en base a la estructura de responsabilidades y autoridad. Esto proporciona un control más estricto en términos de modificación y fabricación de datos.

- Disponibilidad de contramedidas: ¿Está disponible alguna solución de mejores prácticas en la industria? Si no, ¿existe otra manera de contrarrestar esta amenaza?
- Preparación de los proveedores de servicio: ¿Están observándose las políticas, contratos de nivel de servicio y procedimientos en caso de escalada? ¿Cuánto tiempo les tomará a los proveedores de servicios resolver esta amenaza?
- Susceptibilidad de los suscriptores: ¿Están conscientes los suscriptores de tal amenaza? ¿Cuál es la probabilidad de que los suscriptores revelen su información en forma voluntaria si se enfrentan a dicha amenaza? ¿Puede un suscriptor distinguir fácilmente un acto malicioso de un acto genuino cuando se enfrenta a este tipo de amenaza?

2) **Análisis de riesgos.** Los riesgos pueden analizarse por el nivel del impacto de sus consecuencias y por la probabilidad de que ocurran. Este tipo de análisis proporcionará un conjunto de prioridades ordenadas grosso modo por costos esperados. Un ejemplo de este principio se presenta en la Tabla 2.

3) **Monitoreo de riesgos.** Una vez que se ha reducido el riesgo identificado, es importante que un equipo designado monitoree su desempeño y lo evalúe contra experiencias previas. El equipo deberá elaborar una lista de verificación de los problemas que se encuentren antes de solucionar la amenaza. Después, el mismo equipo deberá monitorear la estabilidad y eficacia de las medidas adoptadas y analizar cuidadosamente el sistema en busca de nuevas amenazas potenciales. Estas observaciones deben registrarse junto con la lista de verificación original y reportarse a los propietarios de los negocios.
   - Auditoría del sistema: Estructura de control fundamental que examina, verifica y corrige fallas y lagunas en ciertas funciones del sistema. Se exhorta a los proveedores de servicios a que lleven a cabo auditorías del sistema en forma regular, para asegurarse de que se resuelvan las vulnerabilidades del sistema y que no esté pasándose por alto ninguna actividad maliciosa. Lo anterior resulta especialmente esencial cuando se prueba la funcionalidad de sistemas desarrollados recientemente.
   - Análisis de brecha: Extensión de la lista de verificación que se menciona anteriormente. Es una herramienta eficaz para diferenciar las brechas de desempeño en términos de la funcionalidad del sistema. Aquí se presenta en una matriz que compara el desempeño actual y el esperado y la clasificación del componente analizado.

Conclusión

Ahora podemos unificar estas discusiones acerca de los flujos de información, amenazas y riesgos de los SFM, así como los principios y procedimientos utilizados para resolver las vulnerabilidades de los SFM.

Cualquier estrategia de solución debe empezar por localizar la vulnerabilidad dentro de la red de los flujos de datos de SFM. Por lo tanto, resulta fundamental que los entes reguladores cuenten con un entendimiento básico de la arquitectura de los sistemas de SFM, en especial la forma en que la información se mueve de un elemento de la red a otro. Con dicho entendimiento, los entes reguladores pueden aislar las vulnerabilidades que se derivan de la manera en que un elemento de la red maneja la información. Al identificar dichas vulnerabilidades del manejo de información, los entes reguladores pueden entonces evaluar cuál de las amenazas identificadas en la Tabla 1 tiene mayor probabilidad de poner en riesgo la red de SFM. La presencia de dichas amenazas infringe los principios de la protección de datos que se resumen en el apartado titulado “Identificación de riesgos tecnológicos de los SFM”. Como resultado, tanto la información financiera como la no financiera están sujetas a riesgos tecnológicos específicos.
El análisis de riesgos puede determinar cuál de los conceptos indicados en el registro de riesgos tiene la probabilidad de ocurrir y tener un mayor impacto en los consumidores.

Cuando se ingresan medidas de probabilidad e impacto, el registro de riesgos los ordena por su clasificación (de mayor a menor). Con una lista de riesgos por orden de prioridad, los entes reguladores pueden identificar, nivel por nivel, los tipos de controles de seguridad que se requieren para reducir dichos riesgos. Estos controles de seguridad se convertirán en la referencia para crear e implementar políticas públicas que aborden riesgos tecnológicos en el entorno de los SFM. La tabla a continuación presenta una muestra de cómo puede realizarse dicho análisis.

Tabla 3: Vulnerabilidades y controles de seguridad recomendados

Lugar del riesgo (elemento de la red)	Amenaza	Principio que se infringe	Riesgo probable	Controles de seguridad recomendados
Aplicación de la red móvil	• Revelación • Interceptación	Confidencialidad	Se ha leído información crítica enviada vía SMS	• Los números de cuenta del cliente se cifran cuando se transmiten • Los NIPs del cliente se cifran cuando se muestran y transmiten
Teléfono del usuario final	• Modificación	• Integridad • Autenticación	Infección causada por software malicioso móvil	• Las políticas de información por el lado de la red pueden descargarse en los teléfonos • Uso de antivirus específico para teléfonos inteligentes
Centro SMS, aplicación de SFM, red bancaria	• Interrupción	• Disponibilidad • Irrefutabilidad	Ataques de denegación de servicio	• Implementar un sistema que restrinja el tiempo de respuesta del paquete • Requerir que los SFM establezcan un entorno de red de alta seguridad, al adaptar las normas de mejores prácticas de seguridad como la ISO9001
Teléfono del usuario final	• Fabricación	• Autenticación • Irrefutabilidad	Ataques de suplantación de identidad *(phishing)*	• Solicitar una campaña activa de concienciación de los clientes, para instruir a los consumidores acerca de mensajes maliciosos • Exhortar a los consumidores/ víctimas a que reporten el número de los atacantes maliciosos a los proveedores de servicios de telecomunicaciones, para que puedan enviarse mensajes de advertencia y bloquear el número celular en forma permanente

Referencias

AUJAS. 2011. Mitigating Security Risks in USSD-based Mobile Payment Applications. http://www.thectoforum.com/content/mitigating-security-risks-ussd-based-mobile-payment-applications. [Accessed 26 July 2011].

BEVIS, J. 2007. Disaster Recovery – Alternate Site Geographical Distance. http://infosecalways.com/2007/12/19/disaster-recovery-%E2%80%93-alternate-site-geographical-distance./ [Accessed 24 July 2011].

BOCAN, V. & CREDU, V. 2006. Mitigating Denial of Service Threats in GSM Networks. In: GSM, C.A.P.I. (ed.).

DEPARTMENT OF PREMIER AND CABINE. 2009. Tasmanian Government Information Security Guideline. http://www.egovernment.tas.gov.au/__data/assets/pdf_file/0004/89185/Information_Security_Guidelines.pdf [Accessed 23 July 2011].

DHILLON, G. 2007. Principles of Information Systems Security: Text and Cases. John Wiley & Sons Inc.

GOSTEV, A. 2006. Mobile Malware Evolution: An Overview, Part 1. SECURELIST [Online].

HICKS, S. 2006. Mobile and Malicious: Security for mobile devices getting critical: best practices and technologies. Enterprise Networks & Servers [Online].

JUUL, N.C. 2002. Security Issues in Mobile Commerce using WAP. http://medusa.sdsu.edu/network/security/wap-bled.pdf.

LEE, P. 2002. Cross-site scripting http://www.ibm.com/developerworks/tivoli/library/s-csscript/ [Accessed 26 July 2011].

PELTIER, T. 2001.Information Security Risk Analysis. In: ASSET IDENTIFICATION: NETWORK AND SOFTWARE, P. A. O. A. (ed.). CRC Press LLC.

SAHIBUDIN, S., SHARIFI, M. & AYAT, M. 2008. Combining ITIL, COBIT and ISO/IEC 27002 in Order to Design a Comprehensive IT Framework in Service providers. IEEE Computer Society, 749-754.

ZROBOK, D. 2001. The Security Issues with WAP. http://hygelac.cas.mcmaster.ca/courses/SE-4C03-01/papers/Zrobok-WAP.html [Accessed 26 July 2011].

Acerca de las Notas de Orientación del Grupo de Trabajo de Servicios Financieros Móviles de AFI

Las notas de orientación del Grupo de Trabajo de Servicios Financieros Móviles de AFI se basan en la experiencia de sus miembros e intentan proporcionar una guía para la definición de normas, enfoques y prácticas comunes para la regulación y supervisión de los SFM dentro de las instituciones miembros de AFI. Las notas no son resúmenes de mejores prácticas ni proponen nuevos principios o modificaciones a los principios fundamentales existentes. En cambio, resaltan los problemas de políticas y regulaciones clave de los SFM e identifican los retos a solucionar. Las definiciones que aquí se presentan tienen la intención de complementar, más que de reemplazar definiciones similares de SFM elaboradas por los Organismos Internacionales que Establecen Normas (SSBs, por sus siglas en inglés).

Acerca de AFI

La Alianza para la Inclusión Financiera (AFI) es una red mundial de bancos centrales y otros entes formuladores de políticas financieras de países en desarrollo. AFI proporciona a sus miembros las herramientas y los recursos para compartir, desarrollar e implementar sus conocimientos acerca de políticas de inclusión financiera. AFI conecta a los formuladores de políticas públicas a través de canales en línea y directos, apoyados por subvenciones y vínculos con organismos estratégicos asociados, con el fin de que dichos formuladores puedan compartir sus perspectivas e implementar las políticas de inclusión financiera más adecuadas para las circunstancias individuales de sus países.

Conozca más: www.afi-global.org

Alianza para la Inclusión Financiera

AFI, 399 Interchange Building, 24th floor, Sukhumvit Road, Klongtoey – Nua, Wattana, Bangkok 10110, Tailandia
t +66 (0)2 401 9370 **f** +66 (0)2 402 1122 **e** info@afi-global.org www.afi-global.org
www.facebook.com/AFI.History @NewsAFI

AFI es financiada por la Fundación Bill y Melinda Gates y administrada por GIZ (Agencia de Cooperación Internacional Alemana)

Mobile Payment Forum, India – March 2008

Analysis of Mobile Infrastructure for Secure Mobile Payments

This paper is intended to evaluate various networks and services being used to conduct secure mobile payments using mobile phones.

Submitted by

Prabu Raju – atom tec hnologies limited
Anil Gajwani – Bharti Teleservices Limited
Prof. T.A. Gonsalves – IIT Madras
Ch.Raja Srinivas – Tata Tele Services Limited

Table of Contents

Overview

Mobile Payments is a new convenient scheme for customers to perform transactions, and is predicted to increase as the number of mobile phone users increases. The use of mobile devices, such as a cellular phones and PDAs, to make payments is increasingly common, particularly in Asia and Europe. Mobile payment can be defined as any payment transaction which involves a mobile device. There are wide ranges of options available to perform mobile payments due to the availability of network technologies.

Mobile network technologies have evolved from analog based systems to digital based systems and from circuit switching to packet switching technologies. This evolution can be described by different generations of mobile technologies, i.e. first-generation (1G), second-generation (2G), 2.5G and third-generation (3G) technologies. Only 1G is based on analog technology. Some of the main standards for each generation technology are:

- 1G: Advance Mobile Phone System (AMPS) in North America, Total Access Communication System (TACS) in UK, Nippon Telegraph & Telephone (NTT)in Japan, Code Division Multiple Access One (CDMAONE).

- 2G: Global System for Mobile Communication (GSM), Code Division Multiple Access 2000 (CDMA2000), High Speed Circuit Switched Data Technology (HSCSD).

- 2.5G: General Packet Radio System (GPRS) & Enhanced Data Rate for GSM Evolution (EDGE).

- 3G: Universal Mobile Telephone Standard (UMTS).

Short Message Service (SMS)

SMS provides a mechanism for transmitting short messages to and from wireless handset.

Short Messaging Service was created as a part of the GSM Phase 1 standard to send and receive short text messages, of 70-160 alphanumeric characters in length, 8 bit Binary Message of 140 characters in length to and from mobile phones.

SMS is a smart service, as it can store messages when to the target mobile device is switched off and forwards the messages when the unit is again in use. SMS applications are voicemail/fax notifications, delivery of replacement ring-tones, operator logos and group graphics, unified messaging, personal communication (text messaging), and information services. Basically, any information that fits into a short text message can be delivered by SMS.

Security

The initial idea for SMS usage was intended for the subscribers to send non-sensitive messages across the open GSM network. Mutual authentication, text encryption, end-to-end security, non-repudiation were omitted during the design of GSM architecture.

SMS Spoofing

SMS spoofing is an attack that involves a third party sending out SMS messages that appear to be from a legit sender. It is possible to alter the originator s address field in the SMS header to another alpha-numerical string. It hides the original sender s address and the sender can send out hoax messages and performs masquerading attacks.

SMS Encryption

The default data format for SMS messages is in plaintext. The only encryption involved during transmission is the encryption between the base transceiver station and the mobile station. End-to-end encryption is currently not available. The encryption algorithm used is A5 which is proven to be vulnerable. Therefore a more secure algorithm is needed. The SMS security mechanism relies on GSM/UMTS signaling plane security mechanism.

SMS may be eavesdropped by the man-in-the-middle attack as no encryption is applied to SMS message transmission.

Conclusion

SMS based mobile payment systems are already in use globally. There might be certain risks when using SMS in the payment transaction. The SMS can be used for mobile payments provided the customized

client built by SIM toolkit or Java application is used for the deployment of SMS transaction to provide end-to-end encryption.

Unstructured Supplementary Services Data (USSD)

USSD is a mechanism of transmitting information via a GSM Network. USSD offers a real-time connection during a session. Turnaround response times for interactive applications are shorter for USSD than SMS because of the session-based feature of USSD.

A USSD message can be upto 182 alphanumeric characters in length. Unstructured Supplementary Service Data allows interactive services between a MS and applications hosted by the Mobile Operator. These messages are composed of digits and the #, * keys, and allow users to easily and quickly get information/access services from the Operator.

The first USSD services were called "Phase 1", or "MAP 1" and were only able to pass information from the handset to the USSD application with a confirmation. There was therefore no session held between the handset and the application.

"Phase 2" (or "MAP 2") USSD added the capability for establishing a session instead of a once-off transaction. This meant that the handset and the USSD application could now have the technical equivalent of a dialogue.

GSM handsets supported USSD from the first days of GSM, so unlike SMS, every single GSM handset in the world supports USSD. Phase 2 has been supported for years and over 99% of handsets currently in use can use sessions on the USSD bearer.

USSD is a session oriented service, and can support a sequence of exchange of information. Phase 2 USSD also allows messages to be pushed onto a MS. It is several times faster than MO SMS messages since there is no store and forward of messages. The USSD gateway supports an open HTTP interface.

Generally the USSD functionality is implemented in the following modes:

- Pull Mode, will handle Mobile Initiated USSD Requests.
- Push Mode will handle network Initiated USSD Requests.

Most handsets also support NI USSD (network initiated USSD), also called "USSD Push". With NI USSD, the network can push information to the subscriber's handset.

Another important fact about USSD, is that messages from handsets always route to the home network. This means that if you are roaming in another network, then dialing a USSD string on your phone will always route to the application on your home network. If you are used to accessing a particular service in your home network, then you will also be able to access it from another country. Conversely, roaming subscribers from other networks cannot access USSD services on a host network.

Security

USSD possesses no separate security properties; instead it relies on GSM/UMTS signaling plane security mechanism.

Conclusion

USSD solutions are already in use for mobile payments across the globe. Some measure of encryption or message integrity verification is required to provide a secure USSD based payment system. USSD cannot provide additional security on its own. Another application is used for the deployment of USSD transaction to provide end-to-end encryption

General Packet Radio Service (GPRS)

GPRS is a high-speed packet data technology, being deployed in GSM networks worldwide. This will greatly enhance the services available to the end-user of mobile data computing. GPRS allows for the sending and receiving of data at much higher speed than available today. Data transmissions speeds go from 9.6 kbps to a theoretical maximum speed of up to 171.2 kbps are achievable with GPRS using all eight timeslots at the same time.

GPRS only uses its radio resources when users are actually sending or receiving data, therefore the available radio resource can be concurrently shared between several mobile data users, rather than dedicating a radio channel to a single user for a fixed period of time. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell.

Security

The GPRS Core network is an integrated part of the GSM network; it is layered over the underlying GSM network, with added nodes to cater for packet switching. GPRS also uses some of the existing GSM network elements; some of these include existing Base Station Subsystems (BSS), Mobile Switching Centers (MSC), Authentication Centers (AUC), and Home Location Registers (HLR). Some of the added GPRS network elements to the existing GSM network include; GPRS Support Nodes (GSN), GPRS tunneling protocol (GTP), Access points, and the (Packet Data Protocol) PDP Context.

GPRS security functionality is equivalent to the existing GSM security. From a security point of view the same advantages and short comings of GSM applies to GPRS service. At session initiation, a user is authenticated using secret information contained on a smart card called a Subscriber Identity Module (SIM). Authentication data is exchanged and validated with records stored in the HLR network node.

The microwave links to the BSSs are extensively used when the operator opens its service. The voice and cipher keys Kc can be intercepted on these links. In order to avoid the attack, the operators should replace the weak A3/A8 algorithm with a strong one.

Conclusion

GPRS solutions are already in use for mobile payments across the globe. Application level security should be used to provide end to end transaction security. Even though most of the mobile phones support GPRS, not all the phone user activates the GPRS connection and in most of the countries GPRS is very expensive.

Code Division Multiple Access (CDMA)

Code Division Multiple Access (CDMA) is a proprietary standard for mobile communication, where GSM is an open standard. CDMA was pioneered by Qualcomm and enhanced by Ericsson. Both standards are in competition for dominance in the cellular world. CDMA is a spread spectrum technology, which means that it spreads the information contained in a particular signal of interest over a much greater bandwidth than the original signal. A CDMA call starts with a standard rate of 9.6 kbps, which is then spread to a transmitted rate of about 1.23 Mbps.

Security

By design, CDMA 2000 1xRTT technology makes eavesdropping very difficult, whether intentional or accidental. Unique to CDMA 2000 1xRTT systems, is the 42-bit PN (Pseudo-Random Noise) Sequence called “Long Code” to scramble voice and data. On the forward link (network to mobile), data is scrambled at a rate of 19.2 Kilo symbols per second (Ksps) and on the reverse link, data is scrambled at a rate of 1.2288 Mega chips per second (Mcps).

CDMA 2000 1xRTT network security protocols rely on a 64-bit authentication key (A-Key) and the Electronic Serial Number (ESN) of the mobile. A random binary number called RANDSSD, which is generated in the HLR/AC, also plays a role in the authentication procedures. The A-Key is programmed into the mobile and is stored in the Authentication Center (AC) of the network. In addition to authentication, the A-Key is used to generate the sub-keys for voice privacy and message encryption.

CDMA 2000 1xRTT uses the standardized CAVE (Cellular Authentication and Voice Encryption) algorithm to generate a 128-bit sub-key called the “Shared Secret Data” (SSD). The A-Key, the ESN and the network-supplied RANDSSD are the inputs to the CAVE that generates SSD. The SSD has two parts: SSD_A (64 bit), for creating authentication signatures and SSD_B (64 bit), for generating keys to scramble voice and encrypt signaling/data messages. The SSD can be shared with roaming service providers to allow local authentication. A fresh SSD can be generated when a mobile returns to the home network or roams to a different system.

Third Generation technologies (3G) add more security protocols, including the use of 128-bit privacy and authentication keys. For CDMA2000 networks, new algorithms such as Secure Hashing Algorithm-1 (SHA-1) are being used for hashing and integrity, and the Advanced Encryption Standard, AES (Rijndael) algorithm for message encryption. The AKA (Authentication and Key Agreement) protocol will be used for all releases following CDMA2000 Release C. The AKA protocol will also be used in WCDMA-MAP networks, along with the Kasumi algorithm for encryption and message integrity.

Conclusion

CDMA solutions are already in use for mobile payments. CDMA is superior to 2G technology to GSM. CDMA is not widely used compared to GSM globally.

Appendix

GSM Network

Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world. Figure 1 shows the basic structure of the GSM architecture.

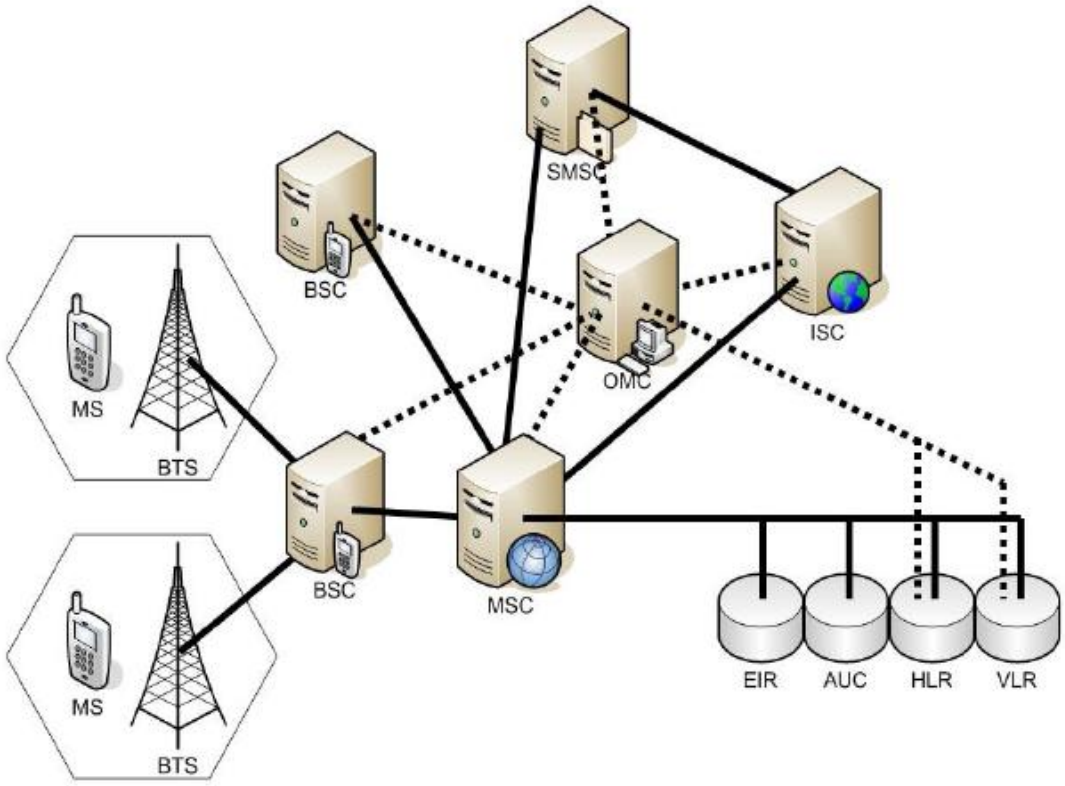


Figure 1 – Basic Structure of GSM Architecture

Key:

MS – Mobile Station
BTS – Base Transceiver Station
BSC – Base Station Controller
MSC – Mobile Switch Centre
OMC – Operation and Management Centre
SMSC – Short Message Service Centre
ISC – International Switching Centre
EIR – Equipment Identity Register
AUC – Authentication Centre
HLR – Home Location Registry
VLR – Visitor Location Registry

Security Mechanisms in GSM Network

The GSM network has some security mechanism to prevent activities like Subscriber Interface Module (SIM) cloning, and stop illegally used handsets. GSM has methods to authenticate and encrypt data exchanged on the network.

GSM Authentication Center

The GSM authentication center is used to authenticate each SIM card that attempts to connect to the GSM network. The SIM card authentication takes place when a mobile station initially attempts to connect to the network, i.e. when a terminal is switched on. If authentication fails then no services are offered by the network operator, otherwise the (Serving GPRS Support Node) SGSN and HLR is allowed to manage the services associated with the SIM card.

Authentication Procedure

The authentication of the SIM depends on a shared secret key between SIM card and the AUC called Ki. This secret key is embedded into the SIM card during manufacture, and it is also securely replicated into the AUC. When the AUC authenticates a SIM, it generates a random number known as the RAND. It sends this RAND number to the subscriber. Both the AUC and SIM feed the Ki and RAND values into the A3/A8 (or operator proprietary algorithm (COMP128)) and a number known as Signed RESponse (SRES) is generated by both parties. If the SIM SRES matches the AUC SRES the SIM is successfully authenticated.

Both the AUC and SIM can calculate a second secret key called Kc by feeding the Ki and the RAND value into the A5 algorithm. This would be used to encrypt and decrypt the session communications. After the SIM authentication the SGSN or HLR requests the mobile identity, this is done to make sure that the mobile station being used by the user is not black listed. The mobile returns the IMEI (International Mobile Equipment Identity) number; this number is forwarded to the EIR (Equipment Identity Register). The EIR authorizes the subscriber and responds back to the SIM with the status, if the mobile is authorized the SGSN informs the HLR and PDP Context activation begins.

Problems with the A3/A8 authentication algorithm

A3/A8 is the term used to describe the mechanism used to authenticate a handset on a mobile phone network. A3 and A8 are not actually encryption algorithms, but placeholders. In A3/A8 the commonly used algorithm is COMP128. COMP128 was broken by Wagner and Goldberg in less than a day. This raises concerns of having GPRS as a secure communication mechanism. After cracking COMP128 Wagner and Goldberg went on to prove that it was possible to obtain the Ki value, therefore making it possible to perform SIM cloning. In 1998, Berkeley Group published their analysis of COMP128 (carrier algorithm to implement A3). It summarized that it would take approximately 219 queries to the mobile unit to determine the secret key. This translates to just eight hours of airtime!

There has been a release of COMP128-2 and COMP128-3 to cater for some of the SIM cloning issues, but the majority of the SIMs still being used use COMP128.

Problems with A5 algorithm

The A5 algorithm is used to prevent casual eavesdropping by encrypting communications between mobile station (handset) and BSS. Kc is the Ki and RAND value fed into the A5 algorithm. This Kc value is the secret key used with the A5 algorithm for encryption between the mobile station and BSS. There are at least three flavours of the A5 algorithm. These include A5/1 which is commonly used in western

countries. The A5/1 is deemed strong encryption but it was reverse engineered some time ago. A5/2 has been cracked by Wagner and Goldberg, the methodology they used required five clock cycles making A5/2 almost useless. One uncovered flaw was ten zeroes introduced into the key, effectively creating a 54 bit key. The most devastating blow, in 1999, Adi Shamir and Alex Biryukov showed that the A5/1 algorithm could get broken on a PC in less than one second. Finally A5/0 is a form of A5 that does not encrypt data at all. All these problems with the A5 encryption algorithms prove that eavesdropping between mobile station and BSS is still possible, making GPRS over the GSM core network very insecure.

Attack on the RAND value

When the AUC attempts to authenticate a SIM card, the RAND value sent to the SIM card can be modified by an intruder failing the authentication. This may cause a denial of service attack.

References

- *State of the Art Review of Mobile Payment Technology - David McKitterick and Jim Dowling*
- *The Future Mobile Payments Infrastructure - Institute for Communications Research Systems @ Work Pte. Ltd*
- *Security of Mobile Banking - Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison*
- *GSM and GPRS Security - Chengyuan Peng*
- *http://www.truteq.com/tips/ussd/*
- *The Future Mobile Payments Infrastructure A Common Platform for Secure M-Payments*
- *CDMA 2000 1xRTT Security Overview*
- *Analysis of mobile payment security measures and different standards by Saleem Kadhiwal and Muhammad Anwar Usman Shaheed Zulfiquar*
- *CGAP MOBILE BANKING TECHNOLOGY MATRIX*