STATUS OF MOBILE PAYMENTS:
AN EXECUTIVE SUMMARY OF ISO 12812 – Parts 1-5

May 1, 2015

Status of DIS Ballots and Next Steps

On November 13, 2014, the ISO Central Secretariat released the ISO 12812 Draft International Standard (DIS), for mobile banking/payments, for country notification, which gives all ISO members, including those who have not previously worked on it, an opportunity to request a copy of the DIS documents prior to release of the DIS ballot. Subsequently, on April 8, the DIS ballots were released; these are 90-day ballots, so ISO member countries must vote by July 8, 2015. The deadline for adoption of a final International Standard is May, 2016.

The DIS ballots come following two Committee Drafts (CDs) of the five-part standard, the last of which was approved in July 2014. However, there were a number of comments that needed to be addressed by the ISO Working Group responsible for the standard (WG10), including comments from five countries that voted "no" on the standard and others who voted "yes with comments." Accordingly, WG10 met for three days in September to complete another round of edits, along with a recommendation on how to proceed with the documents. The final recommendation to ISO TC68/SC7 was sent by WG10 on October 15, 2014, to proceed with an International Standard (IS), rather than convert one or all of the documents into a Technical Report (TR) or a Technical Specification (TS).

The Choice Between an IS and a TR

The WG10 participants at the September 2014 meeting firmly committed to continue developing an IS. Inasmuch as a TR/TS cannot contain any requirements ("shall statements"),failing to adopt an IS would result in the production of merely "academic" papers that would only educate developers of mobile applications but would NOT put any "teeth" in place to enhance the implementation of standardized mobile applications and security. Without an IS, many potential players in the mobile arena would avoid using the ISO documents, and no one seeking to issue an RFP would be able to cite standardized requirements for solutions they want. Particularly with respect to development of payment applications and security, the absence of requirements would leave the mobile environment largely adrift – there would be no rules, so literally developers and implementers would say "anything goes."

Some countries, notably Japan, contend that the mobile marketplace is still emerging and, as such, it is impossible to write a standard today that can adequately capture the proper requirements. Most participants have responded that the vagaries of the marketplace actually provide the best reason for adopting a standardized approach as soon as possible – it is better to put a stake in the ground to tell all implementers that these are the requirements if you want to conform to the standard. Japan has also raised concerns that a mobile standard for chip technology should be able to align with chip card standards; WG10 has no jurisdiction over card standards, so ISO 12812 may ONLY address transactions using a mobile device.

The Substance of ISO 12812

The initial CD documents (2013) had many weaknesses that WG10 has attempted to rectify through two rounds of editing. It is significant that the proposed DISs represent great improvements over where we started, providing requirements, better guidelines, and broader, richer use cases for implementers to follow.

First and foremost, the original drafts contained few actual "requirements" – especially as to security – which meant that no standard was really present. At that point, the documents were written more as academic papers, rather than setting out specific requirements. Each part of the proposed DIS has been "punched up" so that a meaningful set of requirements are spelled out, along with best practices, guidelines and use cases.

Second, the original drafts were geared exclusively to financial institutions (i.e., banks), focused on European payments, and urging adoption of NFC contactless solutions. Accordingly, one of the most significant

changes has been to ensure that the standard articulates that any entity that is providing mobile financial services (referred to as MFSs) must be covered; to that end, the standard now defines a "mobile financial services provider" and most requirements are directed to MFS providers. The proposed DIS expands the standard to cover all mobile payments, including those where the application resides on a remote server (including in the cloud).

The current draft standard now balances between use cases tied to the requirements of the Single Euro Payments Area (SEPA), including EMV, and those based on US processes. Further, the current documents state that payment messages supported by mobile payments must conform to existing payment transaction data elements and message structures, as found in either ISO 8583 or ISO 20022. And the revised documents make it clear there are no new financial instruments involved in the provision of mobile services, just "mobilizing" existing ones and using existing financial services infrastructures to support them.

Finally, the original CDs expressly limited the discussion of security to the use of a Secure Element (SE) in the mobile device or the existence of a Trusted Execution Environment (TEE), an emerging form of hardware/ software security. Recognizing that not every mobile payment application must reside in an SE or a TEE, the proposed DIS expands security considerations to the use of a "secure environment" so long as specific security requirements are met (see the discussion of Part 2 below).

It should also be noted that the original CDs included a Part 6 on Mobile Banking, which has been deleted and the information has been incorporated into the other parts, especially details related to how mobile apps for banking functions should be managed (Part 3).

Highlights of Parts 1-5

Part 1: General Framework

An important aspect of Part 1 is its set of definitions of most of the terms used in the rest of the standard; thus, it provides an overview that every implementer of a mobile financial service (MFS) should use regardless of the type of application it is developing or using operationally. Although Part 1 itself contains no "requirements," it does speak to general principles for how the other four parts interact with one another and provides guidance on how mobile financial services should operate (along with background information explaining how and/or why some services operate the way they do in today's payment environment). As such, Part 1 is intended to "set the stage" for everyone who uses the international standard.

Another critical change from the original CD is that it addresses ALL mobile financial service providers, who literally can be any type of entity (e.g., banks, mobile network operators, trusted service managers, non-bank hosts). While this definition is very broad, Part 1 does recognize that national laws and regulations may affect what financial services can be offered in a particular country and who may engage in those services.

Part 1 also discusses the need for interoperability of MFSs, including the ability of partners to certify that their products/services will work on a particular payment platform or that one MFS can work with another MFS.

Part 2: Security and data protection for mobile financial services

The most significant changes in Part 2 are that: (1) it includes specific requirements applicable to all mobile financial service providers; and (2) a "secure environment" may be created by a variety of different methods (see above). This set of requirements was provided by ISO TC68/SC2 (WG13), which is responsible for data security standards. This input provided the most significant missing piece to the original CD. The essential security requirements are summarized below (although they are not verbatim to the language in Part 2).

1. An MFS provider SHALL provide mutual authentication and follow specific requirements.

2. An MFS provider SHALL take commercially reasonable steps to protect sensitive data from unauthorized disclosure.

3. An MFS provider SHALL take commercially reasonable steps to protect sensitive data from unauthorized modification or substitution.

4. An MFS provider SHALL provide message authentication by following specific requirements.

5. An MFS provider SHALL treat authentication credentials (e.g., passwords, PINs) and account numbers (e.g. PAN) as sensitive data.

6. An MFS provider SHALL ensure that the mobile device and/or MFS be capable of logging specific events.

Beyond the addition of clear requirements, as referenced above, the key clarification in the DIS is the definition of secure environment to include supplementary software controls in addition to an SE or a TEE. Another key issue has been addressed in the proposed DIS; language clarifying that a MFS provider must tie the mobile device and applications uniquely to an individual and thus, the standard does NOT envision a person entering a mobile code (including a bank-issued PIN) into a mobile device that is not his or her own (i.e., a device provided by someone else, including a merchant). A related requirement in Part 2 is that a mobile device cannot enable entry of a PIN unless it conforms to the requirements of ISO 9564.

Part 3: Financial Application Management

This part has been modified to include credentials as a subset of applications. Thus, application lifecycle management requirements apply equally to both (whether the application is for retail payments or banking services). Part 3 needed to be heavily cross-referenced to Part 2 to ensure that all security requirements are met. Another major issue involved clarifying that an application can either reside on the mobile device or be accessed by the consumer through the mobile device (i.e., where the application resides on a remote server or in the cloud. Additional components have been added to expand the functions of the application lifecycle, especially in terms of services to be provided by a MFS provider to its customers.

The proposed DIS ensures that every consumer is made aware of his or her rights. The MFS provider must provide a consumer with all Terms of Service, including rights and obligations related application lifecycle management. As required in the proposed DIS, the Terms of Service document shall address at least the following points:

- Maintenance of applications (embedded or downloaded) to enable consumers to gain access to updates, new features, and security patches;
- One possibility is to discuss a mechanism for applications to communicate with the software level of the Mobile Device (and/or security environment in the mobile device) in order to verify any maintenance of existing applications;
- A process for an MFS provider to decommission an application, including when a business decision has been made not to provide the application after a certain date;
- Articulation of rights or options a consumer has if he/she wants to retain an application purchased from a MFS provider after decommissioning, as well as discussion of any security vulnerabilities associated with retaining an application that is no longer supported by a MFS provider; and
- A process to enable the consumer to remove an application at his/her option.

Finally, because application management may entail the use of other vendors or service providers, the proposed DIS requires that the MFS provider must manage the responsibilities of each entity it uses in providing mobile payment/banking service.

Part 4: Mobile Payments to Persons

The proposed DIS title was changed largely to be consistent with the change made to Part 5 (see below). Nevertheless, after a lengthy debate, WG10 decided that a “person” for the purpose of this Part can be an individual or a small legal entity where an informal or casual relationship exists (e.g., among family members, paying a friend for a share of a meal, paying the babysitter/gardener, etc.). As previously mentioned, the standard now clarifies that the mechanisms involved in mobilizing the transfer of funds are essentially identical regardless of who is involved in the process, or whether such remittance is cross-border or purely within a single country. Thus, it does not matter if the funds are transferred between a payer and a payee, or between a consumer and a merchant – implementers of mobile payment solutions to persons would look at Part 4 of ISO 12812, while potential implementers of retail payment solutions should look at Part 5. As such, both Parts 4 and 5 of ISO 12812 need to support all possible technologies and are not intended favor any specific technology

in the competitive marketplace. Additionally, both parts identify transactions as either proximate (where the parties are physically present) or remote (where the parties can be located anywhere).

Because of the similarities between Part 4 and Part 5 transactions, the proposed DIS contains a set of requirements that have become key provisions in both parts. These requirements assure that a customer is free to choose (under certain conditions) the mobile device and mobile network operator he or she will use to gain access to mobile financial services (MFSs), as well as the specific applications he or she has embedded (or subsequently downloaded) on the mobile device. This set of requirements also covers transaction logging and notice about transfers of funds so that the consumer has adequate information about the exchange of funds.

The proposed DIS contains use cases for fund transfers under SEPA (Single Euro Payments Area) and EMV rules, as well as use cases for automated clearinghouse (ACH) mechanisms. For example, use cases now exist for both credit transfers (SEPA) and ACH, as well as for a variety of remittance situations, and for mobile wallets/electronic money. In that sense, the current document is balanced and useful for implementers under virtually every scenario of mobile payments to persons.

Part 5: Mobile Payments to Businesses

Consistent with the points noted above with respect to Part 4, mobile payments to a business are either proximate or remote and the set of fundamental requirements that apply to the MFS provider are basically the same (customer choice, logging, notice). However, Part 5 of the proposed DIS goes beyond those in part 4 to include requirements for receipts, data protection and privacy and security. Because of specific national legal/regulatory requirements related to consumer protection, WG10 eventually decided to change the terminology and label this part "mobile payments to businesses." This part addresses how a consumer interfaces with the merchant, whether that involves use of a Point of Initiation (e.g., a point of sale terminal) or use of the Internet to reach a merchant website, and whether how the mobile device functions to deliver transaction information (e.g., in card emulation mode, accessing a payment app hosted on a remote server or in the cloud).

Consistent with the rest of the standard, a payment to a business is either proximate or remote, and types of payment instruments range from credit and debit cards, direct debit, stored value, and wallets. The use cases in this part also distinguish between online and off-line payment authorizations, especially focused on how a user verification method (UVM) gets involved in each type of transaction. As with Part 4, the use cases in Part 5 present both SEPA and ACH methods to provide a balanced perspective.

Conclusion

With these requirements, developers of mobile payment apps AND providers of mobile payment services have clear guidelines and/or requirements spelled out for how they must operate, including what security protections must be achieved and possible methods for achieving them. Accordingly, all such providers (existing or prospective) will have to contend with ISO standards. Financial institutions, MNOs, retail merchants, and other potential implementers will be in a position to write RFPs based on the ISO standards so that any successful vendor must demonstrate how its products or services conform to the standard. As such, all stakeholders will benefit from the ISO standards in their respective implementations.