
# *Mobile/NFC Standards Landscape Reference Guide*

*A Smart Card Alliance Mobile and NFC Council Resource*

*Publication Date: November 2012*

*Publication Number: MNFCC-12001*

**Smart Card Alliance**
191 Clarksville Rd.
Princeton Junction, NJ 08550
www.smartcardalliance.org

## *About the Smart Card Alliance*

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Copyright © 2012 Smart Card Alliance, Inc. All rights reserved. Reproduction or distribution of this publication in any form is forbidden without prior permission from the Smart Card Alliance. The Smart Card Alliance has used best efforts to ensure, but cannot guarantee, that the information described in this report is accurate as of the publication date. The Smart Card Alliance disclaims all warranties as to the accuracy, completeness or adequacy of information in this report.

# TABLE OF CONTENTS



Smart Card Alliance © 2012

# 1 Introduction

Mobile NFC applications follow a wide variety of standards and specifications, some that govern the core technology and functionality of mobile NFC devices and some that are specific to applications. The Smart Card Alliance Mobile and NFC Council developed this standards landscape document and accompanying interactive PowerPoint tool to educate industry stakeholders broadly on the standards, specifications and certification requirements for the NFC ecosystem.

Section 2 lists relevant standards and specifications by the standards body, industry organization or industry segment. This document is intended to evolve and be updated with new standards and specifications for mobile NFC applications as they become prominent in the market.

Note that the standards or specifications referenced in this document are available from the organization listed as the author. The documents may be freely available, available for a fee, or available only with a licensing agreement. Please contact the organizations listed as the authors for additional information on how to obtain the documents.

The PowerPoint tool is available on the Smart Card Alliance web site at [insert URL].

# 2 References: Standards and Specifications

Please note that listed versions and dates reflect the latest version of documents at the time of writing. Please check with the responsible authority for the latest release. This is especially important for documents that are indicated as being drafts. Future versions of this document will be updated with the latest versions of referenced documents.

## 2.1 EMVCo

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [1] | EMV Profiles of GlobalPlatform UICC Configuration, version 1.0 | Dec 2010 |
| [2] | EMVCo Mobile Device Requirements for Contactless Mobile Payment, version 1.0 | June 2010 |
| [3] | EMVCo Contactless Mobile Payment - Application Activation User Interface - Overview, Usage Guidelines, and PPSE Requirements, version 1.0 | Dec 2010 |
| [4] | Book A – Architecture and General Requirements, version 2.2 | June 2012 |
| [5] | Book B – Entry Point, version 2.2 | June 2012 |
| [6] | Book C-1 – Kernel 1 Specification, version 2.2 | June 2012 |
| [7] | Book C-2 – Kernel 2 Specification, version 2.2 | June 2012 |
| [8] | Book C-3 – Kernel 3 Specification, version 2.2 | June 2012 |
| [9] | Book C-4 – Kernel 4 Specification, version 2.2 | June 2012 |
| [10] | Book D - EMV Contactless Communication Protocol Specification, version 2.2 | June 2012 |
| [11] | EMV Security Guidelines - EMVCo Security Evaluation Process, version 4.0<br>Note: This document summarizes EMVCo's plans for IC, platform and ICC security evaluation services and related policies in the EMVCo Card Type Approval process. | Dec 2010 |
| [12] | EMV Issuer and Application Security Guidelines, DRAFT version 2.3<br>Note: This document contains very general security requirements for issuer systems and banking cards (UICCs). | July 2011 |
| [13] | EMVCo Contactless Mobile Payment Type Approval Administrative Process, v0.8<br>Note: This document summarizes EMVCo's plans for Contactless Mobile Payment (CMP) Type Approval testing services and policies. This document pertains to secure elements. EMVCo issues a Letter of Compliance for a CMP product when the CMP product has successfully completed the following evaluations:<br>• EMVCo IC security evaluation<br>• GlobalPlatform secure element evaluation<br>• EMVCo PPSE and/or SECM application evaluation<br>• EMVCo platform security evaluation | Oct 2011 |

**Testing and Approval**

| Ref. | Title and Version | Date |
|---|---|---|
| [14] | EMVCo Contactless Mobile Payment AAUI Test Plan, version 1.0a - Draft | Oct 2011 |
| [15] | EMVCo Card and Mobile Testing Framework for Contactless, version 2.0<br>Note: This document specifies the EMVCo general test approach for testing the contactless properties of contactless cards and mobile devices, for a number of different technical architectures. | Jan 2012 |
| [16] | Level 1 Test Equipment Specifications – PICC Manual, PCD Manual, CMR Manual, Gerber Files, version 2.0 | July 2008 |

**http://www.emvco.com/specifications.aspx**

## *2.2 MasterCard*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [17] | PayPass on Mobile Requirements Document<br>Note: This document is only applicable for PayPass MagStripe. | May 2008 |
| [18] | Mobile MasterCard PayPass – M/Chip 4 Technical Specifications, version 1.0<br>Note: This document is relevant for payment applications, not handsets or secure elements (SEs). | Apr 2010 |
| [19] | MasterCard PayPass Application Note #3, v1.0<br>Note: This PayPass Application Note sets the performance requirements for the PayPass application on a contactless card to 400 ms for a PayPass M/Chip application. | Jan 2009 |
| [20] | Mobile MasterCard PayPass User Interface Application Requirements, version 1.2 | Aug 2011 |
| [21] | Mobile MasterCard PayPass User Interface Application Design Guide, version 1.0 | Sep 2011 |
| [22] | Security Guidelines for Mobile Payment Solutions<br>Note: This MasterCard document contains a generic description of assets in and threats to a system for mobile payments. The document also contains a list of security guidelines that a mobile payments system should adhere to. Most of these guidelines apply to the system in its entirety and not specifically to any individual element. | June 2010 |
| [23] | Mobile MasterCard PayPass TSM Functional Requirements, version 1.0 | Nov 2009 |
| [24] | MasterCard PayPass Brand Standards, version 9.0 | June 2009 |
| [25] | Logical Security Requirements for Card Personalization Bureaus | June 2007 |
| [26] | Security Requirements for Mobile Payment Provisioning<br>Note: This document is currently being updated. It is intended for TSMs, which are defined as a party provisioning mobile payment applications to mobile devices, and contains a large number of requirements, many of which are | Dec 2008 |

| | | |
|---|---|---|
| | geared toward physical site security. Requirements for key management, lengths and algorithms are present as well. | |
| [27] | Mobile MasterCard PayPass M/Chip - Issuer Implementation Guide<br>Note: The purpose of this general document is to help MasterCard issuers implement MasterCard PayPass programs using mobile phones as the payment device. These requirements are limited to the implementation of Mobile MasterCard PayPass—M/Chip 4. | Dec 2011 |
| [28] | MasterCard CAST Security Guidelines<br>Note: These "Security Guidelines" comprise a variety of documents that are subject to continuous updates. The latest versions of these documents are issued to vendors upon signing a CAST Agreement and are reissued as updates become available. Issuers may access these documents via MasterCard OnLine. | - |
| [29] | MasterCard Mobile Over-the-Air Provisioning Service Issuer Implementation Guide, without version<br>Note: This document explains how issuers can implement the MasterCard Mobile™ Over-the-Air Provisioning Service (MOTAPS), which enables the handset personalization process that transfers the cardholder's card details to the mobile phone and enables it for use at a MasterCard PayPass terminal. | Jan 2011 |

**Testing and Approval**

| Ref. | Title and Version | Date |
|---|---|---|
| [30] | Mobile MasterCard PayPass Testing and Approval Guide, version 2.0 | Dec 2009 |
| [31] | Mobile MasterCard PayPass TSM Approval Guide, version 1.0 | Nov 2009 |
| [32] | Compliance Assessment and Security Testing Program (CAST) | Sep 2009 |
| [33] | PayPass Vendor Product Approval Process Guide (Cards and Devices) | May 2009 |
| [34] | Mobile MasterCard PayPass SWP Handset Approval Guide, version 1.0 | Dec 2009 |
| [35] | Mobile MasterCard PayPass SWP UICC Approval Guide, version 1.2 | May 2011 |
| [36] | Mobile MasterCard PayPass User Interface Application Approval Guide, version 1.0 | Nov 2009 |

**http://www.mastercard-mobilepartner.com/documentation.html**

## *2.3 Visa*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [37] | Visa Mobile Contactless Payment Specification (VMCPS), version 1.4<br>Note: This document is available under license. | Mar 2011 |
| [38] | Visa Mobile Payment Application Multi Access Specification, version 1.1<br>Note: This document describes how to configure the Visa Mobile Payment Application (VMPA) to allow personalized data to be shared among different VMPA instances residing on the same secure element. An example would be a VMPA instance supporting Visa Debit and another instance supporting an ATM | Sep 2011 |

| | | |
|---|---|---|
| | application.<br>Note: This document is available under license. | |
| [39] | Visa Mobile Contactless Payment Specification – Toolkit and Process Message Specification, version 1.1<br>Note: This document describes the Toolkit Application and its interfaces. The Toolkit Application uses the Card Toolkit Application framework defined by ETSI to enable issuer updates to mobile payment applications. As such, it is the on-card component of the Visa Mobile Gateway infrastructure.<br>Note: This document is available under license. | July 2011 |
| [40] | Visa Mobile Gateway Specification Overview, version 1.0<br>Note: This document is available under license. | Apr 2011 |
| [41] | Visa Mobile Gateway Secure Channel Protocol Specification, version 1.0<br>Note: This document is available under license. | Apr 2011 |
| [42] | Visa Mobile Gateway Issuer Update Protocol Specification, version 1.0<br>Note: This document is available under license. | Apr 2011 |
| [43] | Visa Global Security Requirements for Secure Element Vendors and OTA Service Providers | Nov 2011 |

**Testing and Approval**

| Ref. | Title and Version | Date |
|---|---|---|
| [44] | Visa payWave for Mobile Testing and Compliance Guidelines for Mobile Device Manufacturers and Mobile Network Operators, version 1.0<br>Note: This is a high-level generic document outlining the test process for mobile devices, including:<br>• Requirements for MNOs and handset manufacturers (Company Authorization Program for vendor eligibility to start testing process; Visa Approved Vendor Program for eligibility for commercial roll-out).<br>• Visa Approval Services for actual testing of mobile devices. Mobile device testing includes analog and NFC protocol testing. SE testing is included in case of embedded SE or if a mobile device and an SE are registered for testing as one package. Visa takes into account the SE hardware, platform (operating system, GlobalPlatform, Java Card) and payment application. Note: This document currently requires a non-disclosure agreement. | May 2011 |
| [45] | Testing & Compliance Requirements for Handsets and Secure Elements | May 2012 |
| [46] | Testing & Compliance Requirements for MicroSDs and Mobile Accessories | June 2011 |
| [47] | Visa Chip Security Program – Security Testing Process v1.1<br>This document details how security testing of the chip card product should take place. | Apr 2011 |
| [48] | Chip Card Products - Testing and Approval Requirements, Version 6.1<br>This document provides information needed by card manufacturers, chip suppliers, and Visa staff to support the testing process that is required for all chip card products that are capable of completing a Visa payment transaction | June 2011 |

| | | |
|---|---|---|
| | and will carry the Visa brand. The testing process includes (where applicable):<br>• Testing of basic electrical and protocol characteristics for contact cards<br>• Testing of radio frequency and protocol for contactless cards and other related contactless payment products<br>• Testing of GlobalPlatform Card Specification commands<br>• Testing of Visa payment applications<br>• Security testing of the chip card product and operating system | |
| [49] | Visa Contactless Payment (VCPS) Specification 2.1 and all published updates<br>This document defines the requirements for conducting Visa payWave transactions at point-of-sale (POS) devices and includes requirements for cards, POS devices and chip data messages. This specification is necessary to comply with globally interoperable Visa payWave programs. Note: This document is available under license. | July 2010 |

**https://partnernetwork.visa.com**

## 2.4 American Express

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [50] | Expresspay 2.0 Card Specification | - |
| [51] | Expresspay Terminal Specification v3.0 | - |
| [52] | Expresspay Mobile Specification v1.1 | - |
| [53] | Expresspay Mobile TSM Security Requirements v1.0 | - |
| [54] | Expresspay Mobile Distribution Security Requirements | - |
| [55] | Issuer Mobile Proximity Payment Device Implementation Guide | - |
| [56] | Expresspay Mobile Certification Secure Elements Process Guide v1.0 | - |
| [57] | Expresspay Mobile Certification Handset/OEM Process Guide v1.0 | - |
| [58] | Expresspay Mobile Wallet Interface Guide | - |
| [59] | Expresspay Mobile Personalization Guide | - |

## 2.5 Discover

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [60] | Discover Network Zip Payment Specification V.3.1.2 | Oct 2011 |
| [61] | DFS Payment Device Evaluation Scheme Security Evaluation Processes v2.0 | Dec 2011 |
| [62] | DFS Payment Device Evaluation Scheme Security Requirements for Vendors v2.0 | Dec 2011 |
| [63] | Discover Trusted Service Manager - Functional and Security Requirements Version 1.0.0 | May 2011 |
| [64] | Discover Network Zip TA Administrative Process v1.24 | Oct 2011 |

| | | |
|---|---|---|
| [65] | Discover Network Test Plan for Contactless Payment Devices (PICC) v5.4 | Dec 2011 |
| [66] | DFS TSM Qualification Process v1.0 | Aug 2011 |

This section includes Discover's Zip specifications. The contactless D-PAS specifications based on EMVCo specifications will be issued later in 2012.

## *2.6 GlobalPlatform*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [67] | GlobalPlatform Card Specification, version 2.2.1<br>Note: This document describes the GlobalPlatform architecture, which is designed to provide card issuers and other stakeholders with the system management architecture for dynamically managing multi-application smart cards. | Jan 2011 |
| [68] | GlobalPlatform Card Specifications - Amendment A, Confidential Card Content Management, version 1.0.1<br>Note: This Amendment mainly specifies (additional properties of) the Controlling Authority, to enable fully confidential card content management. | Jan 2011 |
| [69] | GlobalPlatform Card Specifications - Amendment B, Remote Application Management over HTTP, version 1.1.1<br>Note: This Amendment specifies how to perform remote application management, using the HTTP protocol and PSK TLS security over-the-air. | Mar 2012 |
| [70] | GlobalPlatform Card Specifications - Amendment C, Contactless Services, version 1.0.1<br>Note: This Amendment defines mechanisms, parameters and interfaces to set up and maintain the configuration of applications and control their access to system resources such as communication interfaces and memory. | Feb 2012 |
| [71] | GlobalPlatform Card Specifications - Amendment D, SCP03, version 1.0<br>Note: This document specifies the SCP03 secure channel protocol, which is similar to SCP02 but based on AES. In addition, the document defines the formats and requirements for DAPs, tokens and receipts if AES is used for card content management activities. | Mar 2011 |
| [72] | GlobalPlatform Card Specifications - Amendment E, Security Upgrade for Card Content Management, version 1.0<br>Note: The purpose of this amendment is to expand those specifications to include new cryptographic schemes based on Elliptic Curve Cryptography (ECC) and upgraded cryptographic schemes for RSA. | Nov 2011 |
| [73] | GlobalPlatform Card UICC Configuration, version 1.0.1<br>Note: This is an implementation guide for deploying GlobalPlatform Card Specification v2.2 within the mobile services sector and managing the secure delivery over-the-air of new services. | Jan 2011 |
| [74] | GlobalPlatform Card ID Configuration, version 1.0<br>Note: This document describes a specific implementation of the GlobalPlatform Card Specification providing a suitable framework for card content management | Dec 2011 |

| | | |
|---|---|---|
| | in the context of the identity market. | |
| [75] | GlobalPlatform UICC configuration – Contactless Extension, version 1.0<br>Note: This document defines an extension of the GlobalPlatform UICC Configuration for UICCs equipped with contactless functionality. | Feb 2012 |
| [76] | GlobalPlatform Device Specifications - TEE System Architecture, version 1.0<br>Note: This document explains the hardware and software architectures behind the Trusted Execution Environment (TEE). It introduces the security concepts involved and explains some concepts relevant to the TEE functionality available in a device. | Dec 2011 |
| [77] | GlobalPlatform Device Specifications - TEE Internal API Specification, version 1.0<br>Note: This document defines the communication between applications running in a rich operating environment and the applications residing in the TEE. | Dec 2011 |
| [78] | GlobalPlatform Device Specifications - TEE Client API Specification, Version 1.0<br>Note: This specification defines a set of C APIs for the development of Trusted Applications (TAs) running inside a TEE. | July 2010 |
| [79] | GlobalPlatform Device Specifications - Secure Element Access Control, version 1.0<br>Note: This document specifies how the access policy is stored in the secure element, and how it can be accessed and applied by the device. | Mar 2012 |
| [80] | GlobalPlatform Device Specifications - Secure Element Remote Application Management, version 1.0<br>Note: The aim of this document is to define a single administration protocol to perform remote management of applications residing on any type of secure element in a mobile phone. | May 2011 |
| [81] | GlobalPlatform Systems Specifications - GlobalPlatform System Messaging Specification for Management of Mobile-NFC Services, version 1.0<br>Note: This document specifies the GlobalPlatform messages allowing for provisioning and managing mobile NFC services using a TSM. | Feb 2011 |
| [82] | GlobalPlatform Systems Specifications - GlobalPlatform System Web Services profile for GlobalPlatform Messaging, version 1.0<br>Note: This document specifies the usage of W3C and OASIS standards to support the GlobalPlatform Messaging Specification. | Feb 2011 |
| [83] | GlobalPlatform Card Composition Model v1.0<br>Note: The objective of this document is to define a composition model for the security evaluation of composite products. A composite product is a secure element that consists of an open platform and one or more applications. The model relies on the recognition of existing security evaluation certificates and significant re-use of these certificates and evaluation activity results. The model specifically addresses the composition of products that are evaluated under the EMVCo and Common Criteria schemes. | Jan 2011 |
| [84] | GlobalPlatform Card Composition Model – Security Guidelines for Basic Applications v1.0<br>Note: This document proposes a minimal set of guidelines for basic applications (non-payment applications) intended to protect sensitive applications, other applications and the platform. | June 2012 |

**Testing and Approval**

| Ref. | Title and Version | Date |
|---|---|---|
| [85] | GlobalPlatform UICC Test Suite v1.0.2 | - |
| [86] | Contactless Extension of UICC Configuration Test Suite | - |

**http://www.globalplatform.org/specifications.asp**

## *2.7 ISO / IEC*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [87] | ISO/IEC 7816-1, Identification cards - Integrated circuit cards – Cards with contacts — Physical characteristics | Feb 2011 |
| [88] | ISO/IEC 7816-2, Identification cards - Integrated circuit cards – Cards with contacts - Dimensions and location of the contacts | Oct 2007 |
| [89] | ISO/IEC 7816-3, Identification cards - Integrated circuit cards – Electrical interface and transmission protocols | Nov 2006 |
| [90] | ISO/IEC 7816-4, Identification cards - Integrated circuit cards – Organization, security and commands for interchange | Jan 2005 |
| [91] | ISO/IEC 7816-6, Identification cards - Integrated circuit cards – Interindustry data elements for Interchange | May 2004 |
| [92] | ISO/IEC 7816-8, Identification cards - Integrated circuit cards – Commands for security operations | June 2004 |
| [93] | ISO/IEC 7816-9, Identification cards - Integrated circuit cards – Commands for card management | June 2004 |
| [94] | ISO/IEC 7816-13, Identification cards - Integrated circuit cards – Commands for application management in a multi-application environment | March 2007 |
| [95] | ISO/IEC 7816-15, Identification cards - Integrated circuit cards – Cryptographic information application | Jan 2004 |
| [96] | ISO 14443 – Part 1 - Identification cards – Contactless integrated circuits(s) cards – Proximity cards - Part 1: Physical Characteristics | Apr 2000 |
| [97] | ISO 14443 – Part 2 - First Edition Identification cards – Contactless integrated circuits(s) cards – Proximity cards - Part 2: Radio frequency power and signal interface | June 2001 |
| [98] | ISO 14443 – Part 3 - First Edition Identification cards – Contactless integrated circuits(s) cards – Proximity cards - Part 3: Initialization and anticollision | Feb 2001 |
| [99] | ISO 14443 – Part 4 - First Edition Identification cards – Contactless integrated circuits(s) cards – Proximity cards - Part 4: Transmission Protocols | Feb 2001 |
| [100] | ISO/IEC 18092, Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) | Apr 2004 |

| | | |
|---|---|---|
| [101] | ISO/IEC 22536, Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol (NFCIP-1) — RF interface test methods | July 2005 |
| [102] | ISO/IEC 21481 Information technology — Telecommunications and information exchange between systems — Near Field Communication Interface and Protocol -2 (NFCIP-2) | Jan 2005 |
| [103] | ISO/IEC 23917, Information technology — Telecommunications and information exchange between systems — NFCIP-1 — Protocol Test Methods | Nov 2005 |

**http://www.iso.org/iso/home/standards.htm**

## *2.8 NFC Forum*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [104] | NFC Data Exchange Format (NDEF) Technical Specification | July 2006 |
| [105] | NFC Forum Type 1 Tag Operation Specification 1.1 | Apr 2011 |
| [106] | NFC Forum Type 2 Tag Operation Specification 1.1 | May 2011 |
| [107] | NFC Forum Type 3 Tag Operation Specification 1.1 | June 2011 |
| [108] | NFC Forum Type 4 Tag Operation Specification 2.0 | June 2011 |
| [109] | NFC Record Type Definition (RTD) Technical Specification | July 2006 |
| [110] | NFC Text Record Type Definition (RTD) Technical Specification | July 2006 |
| [111] | NFC URI Record Type Definition (RTD) Technical Specification | July 2006 |
| [112] | NFC Smart Poster Record Type Definition (RTD) Technical Specification | July 2006 |
| [113] | NFC Generic Control Record Type Definition (RTD) Technical Specification | Mar 2008 |
| [114] | NFC Signature Record Type Definition (RTD) Technical Specification | Nov 2010 |
| [115] | NFC Forum Connection Handover 1.2 Technical Specification<br>Note: This specification defines how NFC can initiate a connection on an alternative wireless technology. | July 2010 |
| [116] | NFC Logical Link Control Protocol (LLCP) 1.1 Technical Specification<br>Note: This specification defines a way to create reliable peer-to-peer communication over NFC. | June 2011 |
| [117] | NFC Digital Protocol Technical Specification<br>Note: This specification defines the “building blocks” to set up and maintain an NFC connection between two devices. | Nov 2010 |
| [118] | NFC Activity Technical Specification<br>Note: This specification defines how to use the building blocks of the Digital Protocol specification for particular use cases (e.g., P2P, reading tag data). | Nov 2010 |
| [119] | NFC Simple NDEF Exchange Protocol (SNEP) Technical Specification<br>Note: This specification defines how an application on an NFC-enabled device can exchange NFC Data Exchange Format (NDEF) messages with another NFC Forum device while operating in peer-to-peer mode. | Aug 2011 |

| | | |
|---|---|---|
| [120] | NFC Controller Interface (NCI) Technical Specification<br>Note: This specification defines an interface within an NFC device between an NFC controller (NFCC) and the device's main application processor. | Nov 2012 |
| [121] | NFC Analog Technical Specification<br>Note: This specification addresses the analog characteristics of the RF interface of an NFC-enabled device; it is intended for manufacturers wanting to implement such devices. | Nov 2012 |
| [122] | Bluetooth Secure Simple Pairing Using NFC | Nov 2011 |

**Testing and Approval**

| Ref. | Title and Version | Date |
|---|---|---|
| [123] | NFC Forum Device Requirements | Oct 2010 |
| [124] | Device Test Application Specification for NFC Digital Protocol and NFC Forum Type 1/2/3/4 Tags 1.2.2 | Jan 2012 |
| [125] | Test Cases for NFC Digital Protocol | Nov 2011 |
| [126] | Test Cases for Type 1 Tag | Nov 2011 |
| [127] | Test Cases for Type 2 Tag | Nov 2011 |
| [128] | Test Cases for Type 3 Tag | Nov 2011 |
| [129] | Test Cases for Type 4 Tag | Nov 2011 |

**http://www.nfc-forum.org/specs/**

## 2.9 SIM Alliance

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [130] | Open Mobile API specification, version 2.02<br>Note: The API specified in this document enables mobile applications to have access to different secure elements in a mobile device, such as SIMs or embedded SEs. This specification can be implemented on various mobile platforms and in different programming languages. | Nov 2011 |

**http://www.simalliance.org/en/resources/specifications/**

## 2.10 ETSI

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [131] | ETSI TS 102 124 - Smart Cards; Transport Protocol for UICC based Applications; Stage 1 (Release 6), version 6.1.0 | Dec 2004 |
| [132] | ETSI TS 102 127 - Smart Cards; Transport Protocol for CAT Applications; Stage 2 (Release 6), version 6.13.0 | Apr 2009 |
| [133] | ETSI TS 102 221 - Smart Cards; UICC-Terminal interface; Physical and logical | Dec 2011 |

| | | |
|---|---|---|
| | Characteristics (Release 10), version 10.0.0 | |
| [134] | ETSI TS 102 223 - Smart Cards; Card Application Toolkit (Release 11), version 11.0.0 | Mar 2011 |
| [135] | ETSI TS 102 225 - Smart Cards; Secured packet structure for UICC based applications (Release 11), version 11.0.0 | Mar 2012 |
| [136] | ETSI TS 102 226 - Smart Cards; Remote APDU structure for UICC based applications (Release 11), version 11.0.0 | Mar 2012 |
| [137] | ETSI TS 102 613 - Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 9), version 9.2.0 | Mar 2003 |
| [138] | ETSI TS 102 622 - Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release 11), version 11.0.0 | Sep 2011 |

**Testing and Approval**

| Ref. | Title and Version | Date |
|---|---|---|
| [139] | ETSI TS 31.122<br>Note: This document is the test specification for ETSI TS 102 221. | - |
| [140] | ETSI TS 102 694 – Test specification for the Single Wire Protocol (SWP) interface<br>Note: This document is the test specification for ETSI TS 102 613. | - |
| [141] | ETSI TS 102 695 – Test specification for the Host Controller Interface (HCI)<br>Note: This document is the test specification for ETSI TS 102 622. | - |

**http://www.etsi.org/website/standards/standard.aspx**

## *2.11 GSMA*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [142] | Requirements for Single Wire Protocol NFC Handsets, version 4.0 | Mar 2011 |
| [143] | NFC Handset APIs & Requirements, Version 2.0 | Nov 2011 |
| [144] | NFC UICC Requirement Specification, Version 2.0 | Nov 2011 |
| [145] | Mobile Contactless Payments Service Management – Roles, Requirements and Specifications, version 2.0<br>Note: This document contains requirements and specifications for the purpose of enabling UICC-based NFC-enabled mobile contactless card payments application deployment and management interoperability across multiple issuers and MNOs. | Oct 2010 |
| [146] | Trusted Service Manager, Service Management Requirements and Specifications | Jan 2010 |

## *2.12 PCI*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|

| | | |
|---|---|---|
| [147] | PCI DSS (PCI Data Security Standard) - PCI DSS v2.0 | Oct 2010 |
| [148] | PA DSS (Payment Application Data Security Standard) - PA-DSS Requirement and Security Assessment Procedures v2.0 | Oct 2010 |
| [149] | PCI PTS (PIN Transaction Security) - PIN Security Requirements v1.0 | Sep 2011 |
| [150] | PCI PTS (PIN Transaction Security) - Hardware Security Module (HSM) v2.0 | May 2012 |
| [151] | PCI PTS (PIN Transaction Security) - Point of Interaction (POI) Modular Security Requirements v3.1 | Oct 2010 |
| [152] | PCI P2PE (Point-to-Point Encryption) – P2PE Hardware Solution Requirements and Testing Procedures | Apr 2012 |

**https://www.pcisecuritystandards.org/security_standards/documents.php**

## *2.13 Association Francaise du Sans Contact Mobile (AFSCM)*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [153] | NFC Mobile Handset High Level Requirements, version 2.0 | Sep 2011 |
| [154] | NFC UICC High Level Requirements, version 2.0.1 | Mar 2012 |
| [155] | Interface Specification – Between Telecom Operators and NFC Service Providers, version 2.1 | Feb 2012 |

**http://www.afscm.org/en/specifications/download.php**

## *2.14 Transit*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [156] | MIFARE4Mobile V1.01 - specification for managing MIFARE credentials in the secure element | Sep 2009 |
| [157] | MIFARE4Mobile V1.01 Extension V0.4 – extensions to support multiple credentials | Nov 2011 |
| [158] | MIFARE4Mobile V2.0 – extension of MIFARE4Mobile to support additional card types, multiple TSMs, compliance with GlobalPlatform V2.2, and end-to-end security between service provider and MIFARE application. | TBD, Summer 2012 |
| [159] | CIPURSE V1.1 – open standard for secure, interoperable transit fare collection solutions (OSPT Alliance) | July 2012 |
| [160] | CIPURSE V2.0 – open standard for secure, interoperable transit fare collection solutions (OSPT Alliance) | Sept 2012 |
| [161] | American Public Transportation Association (APTA) Contactless Fare Media System (CFMS) – U.S. standard | - |
| [162] | ITSO – Integrated Transport Smartcard Organisation. ITSO Technical Specification 1000: Interoperable public transport ticketing using contactless smart customer media. Version V2.1.4 | Feb 2010 |

| | | |
|---|---|---|
| [163] | Calypso – Electronic ticketing standard which defines the secured dialogue between cards and terminal | - |
| [164] | VDV Core Application (VDV-KA) – Verband Deutscher Verkehrsunternehmen – German e-ticketing standard | - |
| [165] | SDOA - Specification Document Open Architecture | - |

## *2.15 Access Control*

**Specifications and Requirements**

| Ref. | Title and Version | Date |
|---|---|---|
| [166] | UL 294 Ed 5, Standard for Access Control Systems Units | Jan 2011 |
| [167] | UL 1076 Ed 5, Proprietary Burglar Alarm Units and Systems | Feb 1999 |
| [168] | INCITS 504-1: Information Technology - Generic Identity Command Set Part 1: Card Application Command Set | - |
| [169] | INCITS 504-2: Information Technology - Generic Identity Command Set Part 2: Card Administrative Command Set | - |
| [170] | NIST FIPS 140-2: Security Requirements for Cryptographic Modules | May 2001 |
| [171] | FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors | Mar 2006 |
| [172] | FIPS 201-2: revised draft Personal Identity Verification (PIV) of Federal Employees and Contractors | July 2012 |
| [173] | NIST SP 800-73-3: Interfaces for Personal Identity Verification – Part 2: End-Point PIV Card Application Card Command Interface | Feb 2010 |
| [174] | NIST SP 800-116: A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS) | Nov 2008 |

# 3 Publication Acknowledgements

This resource was developed by the Smart Card Alliance Mobile and NFC Council to educate stakeholders broadly on the standards, specifications and certifications used by the mobile/NFC ecosystem.

Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

The Smart Card Alliance wishes to thank the Mobile and NFC Council members for their contributions. Participants involved in the development of this white paper included: Accenture LLP; American Express; Chase Card Services; Collis/UL; CorFire; CPI Card Group; Cubic Transportation Systems, Inc.; Datawatch Systems, Inc.; Discover Financial Services; First Data Corporation; Giesecke & Devrient; Heartland Payment Systems; HID Global; Identification Technology Partners; Identive Group; Infineon Technologies; Ingenico; IRCO; INSIDE Secure; Interac Association/Acxsys Corporation; Intercede Ltd.; IQ Devices; Isis; MasterCard Worldwide; NFC Forum; NXP Semiconductors; Quadagno & Associates; SafeNet, Inc.; SecureKey Technologies; TSYS; VeriFone Systems; Visa Inc.; ViVOtech, Wells Fargo

Special thanks go to **Bart van Hoek**, Collis/UL, who led the project, contributed content, and integrated input from Council members in the standards landscape document and who created the interactive PowerPoint tool.

Special thanks go to the following Council members who contributed to developing to this document:

- **Lucia D'Acunto**, Collis / UL
- **Rene Bastien**, SecureKey Technologies
- **Brent Bowen**, INSIDE Secure
- **Peter Cattaneo**, Intercede
- **Javed Chaudry**, ViVOtech
- **David deKozan**, Cubic
- **Michael English**, Heartland Payment Systems
- **Guillaume Grincourt**, CPI Card Group
- **Shishir Gupta**, NFC Forum / Kovio
- **Peter Ho**, Wells Fargo
- **Philip Hoyer**, HID Global
- **Liz Jackson**, American Express
- **Grace Jung**, Interac
- **Deana Karhuniemi**, Chase Card Services
- **Josh Kessler**, MasterCard Worldwide
- **Sanne Ketelaar**, Collis / UL
- **Werner Koele**, Infineon Technologies
- **Peter Lee**, CorFire
- **Gurpreet Manes**, SafeNet
- **Cathy Medich**, Smart Card Alliance
- **Jeff Neafsey,** IRCO
- **Beth Odom**, TSYS
- **Akif Qazi**, Discover Financial Services
- **Peter Quadagno**, Quadagno & Associates
- **Sanjiv Rawat**, Giesecke & Devrient
- **JC Raynon**, VeriFone Systems
- **Kenny Reed**, Datawatch Systems
- **Steve Rogers**, IQ Devices
- **Tony Sabetti**, Isis
- **Gerry Schoenecker**, Ingenico
- **Didier Serra**, INSIDE Secure
- **Deb Spitler**, HID Global
- **Chandra Srivastava**, Visa Inc.
- **Brian Stein**, Accenture
- **Lars Suneborn**, Identive
- **Sridher Swaminathan**, First Data Corp.
- **Joe Tassone**, Identive Group
- **Bart van Hoek**, Collis / UL
- **Erick Wong**, Visa Inc.
- **Greg Wong**, American Express
- **Mike Zercher**, NXP Semiconductors
- **Rob Zivney**, ID Technology Partners

## Trademark Notice

All registered trademarks, trademarks, or service marks are the property of their respective owners.

## About the Smart Card Alliance Mobile and NFC Council

The Smart Card Alliance Mobile and NFC Council was formed to raise awareness and accelerate the adoption of payments, loyalty, marketing, promotion/coupons/offers, peer-to-peer, identity, and access control applications using NFC. The Council focuses on activities that will help to accelerate the practical

application of the technology, providing a bridge between technology development/specification and the applications that can deliver business benefits to industry stakeholders.

The Council takes a broad industry view and brings together industry stakeholders in the different vertical markets that can benefit from mobile and NFC applications. The Council collaborates on: educating the market on the technology and the value of mobile and NFC applications; developing best practices for implementation; and working on identifying and overcoming issues inhibiting the industry