REFERENCE



TCG Trusted Mobility Solutions Work Group

Use Cases – Enterprise, Financial, & NFV

Version 2.0
Revision 47
26 September 2018
PUBLISHED

Contact: admin@trustedcomputinggroup.org

PUBLISHED

Copyright © TCG 2011-2018

TCG

Copyright © 2011-2018 Trusted Computing Group, Incorporated.

Disclaimer

THIS REFERENCE DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, WHITE PAPER, OR SAMPLE. Without limitation, TCG disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this reference document, and TCG disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this document or any information herein.

No license, express or implied, by estoppel or otherwise, to any TCG or TCG member intellectual property rights is granted herein.

Contact the Trusted Computing Group at www.trustedcomputinggroup.org for information on TCG licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

Acknowledgements

The TCG wishes to thank all those who contributed to this reference document. This document builds on work done in other TCG work groups, including Infrastructure, Mobile Platform, Storage, Trusted Network Communications, Trusted Platform Module, TCG Software Stack, and Virtual Platform.

Special thanks to the following current and former members of the TMS WG who contributed to current and/or previous versions of this document:

John Padgette (lead editor of TMS UC v1)	Accenture
Emily Ratliff (UC v1)	formerly AMD
Wael Ibrahim	American Express
John Mersh (UC v1)	formerly ARM Ltd
Padma Krishnaswamy (UC v1)	Battelle Memorial Institute
Rafael Montalvo (UC v1)	Cisco Systems
Nicolai Kuntze	Huawei
Seigo Kotani (UC v1)	Fujitsu Limited
Virginie Galindo (UC v1)	Gemalto NV
Rene Bourquin (UC v1)	General Dynamics C4 Systems
Brooke Burson (UC v1)	General Dynamics C4 Systems
Michael Donovan (UC v1)	Hewlett-Packard
Ira McDonald (TMS co-chair, co-editor of TMS UC v1/v2)	High North Inc
Florian Schreiner (UC v1)	Infineon
Martin Nicholes (UC v1)	Insyde Software Corp
Bo Bjerrum (UC v2)	Intel Corporation
Sung Lee (UC v1)	Intel Corporation
Alec Brusilovsky (TMS co-chair, co-editor of TMS UC v1/v2)	InterDigital Communications, LLC
Kathleen McGill (UC v1/v2)	Johns Hopkins University, Applied Physics Lab
Chris Daly (co-editor of TMS UC v1)	formerly Juniper Networks, Inc
Steve Hanna (UC v1)	Infineon
Hadi Nahari (UC v1)	NVIDIA Corp
Cedric Colnot (UC v1)	NXP Semiconductors
Carlin Covey (TMS co-chair, co-editor of TMS UC v1/v2)	NXP Semiconductors
Ken Nicolson (UC v1)	Panasonic
Dick Wilkins (UC v1)	Phoenix Technologies Ltd
Anders Rundgren (UC v1)	PrimeKey Solutions AB

Esteban Yepez (UC v1)	Sandia National Laboratories
Yoni Shternhell (UC v1)	SanDisk Corporation
Ed Adams (UC v1)	Security Innovations
Hervé Sibert (UC v1)	STMicroelectronics
Mohamed Tabet (UC v1)	STMicroelectronics
Anne-Rose Gratadour (UC v1)	Thales Communications & Security
Beth Abramowitz (UC v1)	The MITRE Corporation
Carlton Northern (co-editor of TMS UC v1)	The MITRE Corporation
Nicolas Ponsini(UC v1)	Trustonic Ltd
Capt. Joshua Dixon (UC v1)	United States Government
Jessica Fitzgerald-McKay (UC v1)	United States Government
Stanley Potter (UC v1)	United States Government

Table of Contents

1. Introduction 1
2. Terminology and References 2
2.1 Terms and Definitions 2
2.2 Actors 7
2.3 References 8
3. Enterprise Mobile Use Cases (BYOD/CYOD/COPE) 9
3.1 Objective and Scope 9
3.2 Description 10
3.2.1 Mobile Device Enrollment 11
3.2.2 Mobile Device Attachment 12
3.3 Benefits for Actors 12
3.4 Solution Assumptions 12
3.5 Post-conditions 12
3.5.1 Success End Condition 12
3.5.2 Failure End Condition 12
3.6 Lifecycle Scenarios 13
3.7 Trust Assertions 13
3.7.1 Trust Assertions for Enterprise Mobile Devices 13
3.8 Security Policies 14
3.9 Threats and Mitigations 14
3.10 Solution Approaches 14
4. Financial Use Cases 15
4.1 Objective and Scope 15
4.2 Description 15
4.2.1 Mobile Banking Use Case 15
4.2.2 Mobile Payment Use Case 15
4.3 Benefits for Actors 16
4.4 Solution Assumptions 16
4.5 Post-conditions 16
4.5.1 Success End Condition 16
4.5.2 Failure End Condition 16
4.6 Lifecycle Scenarios 16
4.7 Trust Assertions 17
4.7.1 Trust Assertions for Financial Use Cases 17
4.8 Security Policies 17

4.9 Threats and Mitigations 17
4.10 Solution Approaches 17
5. NFV Use Cases 18
5.1 Objective and Scope 18
5.2 Description 18
5.2.1 Retailer Credit Check with Consumer Privacy Use Case 20
5.2.2 Network Entity Authentication for Network Admission 22
5.3 Benefits for Actors 24
5.4 Solution Assumptions 24
5.5 Post-conditions 25
5.5.1 Success End Condition 25
5.5.2 Failure End Condition 25
5.6 Lifecycle Scenarios 25
5.7 Trust Assertions 25
5.7.1 Trust Assertions for NFV Use Cases 25
5.8 Security Policies 26
5.9 Threats and Mitigations 26
5.10 Solution Approaches 26
6. Benefits for Actors 27
6.1 End User 27
6.2 Device Owner 28
6.3 Device Manufacturer 28
6.4 Information Owner 28
6.5 Enterprise 28
6.6 Service Providers 29
6.7 Communication Carrier 29
6.8 Application Provider or Content Provider 30
6.9 Operating System Provider 30
7. Lifecycle Scenarios 31
7.1 Device Manufacturer Lifecycle 31
7.2 Communication Carrier Lifecycle 32
7.3 Device Owner Lifecycle 33
7.4 Enterprise Lifecycle 34
7.5 Service Provider Lifecycle 36
7.6 VNF Software Lifecycle 36
7.7 Lifecycle Solution Requirements 38
8. Trust Assertions 39

8.1 Overview of Trust Assertions 39
8.2 Building Blocks for Trust Assertions 39
8.3 End User or Device to Service Provider 40
8.4 Service Provider to Device or End User 41
8.5 Security Infrastructure to Service Provider 41
8.6 Network Access Point to Device or Service Provider 42
9. Solution Approaches 43
10. Security Considerations 44
10.1 Security Policies 44
10.2 Threats and Mitigations 44

List of Figures

Figure 1 – Enterprise Mobile Device Architecture 10
Figure 2 – Escalating Trust Brings Increased Access for Mobile Device Users 11
Figure 3 – NFV Use Case Simplified Functional Diagram 19
Figure 4 – Retailer Credit Check with Consumer Privacy 21
Figure 5 – Network Entity Authentication for Network Admission 23

 Copyright © TCG 2011-2018

1. Introduction

Use cases are narratives that define user expectations and usage contexts that meet those expectations. The use cases defined in this document are intended to be sufficiently general that they are not likely to change in their broad scope over time and can serve as generalizations for a variety of more specific usage scenarios.

The Trusted Computing Group's (TCG) Trusted Mobility Solutions (TMS) Use Cases consider a broad range of scenarios where TCG technology can be applied in Mobile Device usage contexts and ecosystems.

This document is intended to guide subsequent solutions framework development work in the TCG TMS Workgroup (TMS WG) and to provide parties within and outside of TCG with a description of the TMS WG's scope of work. The use cases outlined in this document also provide illustrations for solution developers of the types of capabilities that rely on TCG security technology in Mobile Devices.

2. Terminology and References

2.1 Terms and Definitions

Refer to the TCG Glossary of Technical Terms [10] for additional trusted computing terms and definitions

https://trustedcomputinggroup.org/wpcontent/uploads/TCG-Glossary-V1.1-Rev-1.0.pdf

Accountability [8]	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
Assurance [8]	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes: (1) functionality that performs correctly; (2) sufficient protection against unintentional errors (by users or software); and (3) sufficient resistance to intentional penetration or bypass.
Attestation [10]	The process of vouching for the accuracy of information. External entities can attest to shielded locations, protected capabilities, and Roots of Trust. A platform can attest to its description of platform characteristics that affect the integrity (trustworthiness) of a platform. Both forms of attestation require reliable evidence of the attesting entity.
Availability [8]	The security goal that generates the requirement for protection against intentional or accidental attempts to: (1) perform unauthorized deletion of data; or (2) otherwise cause a denial of service or data via unauthorized use of system resources.
Bluetooth	A standard for short-range (up to 60 meters) wireless interconnection of cellular phones, computers, and other electronic devices.
Bluetooth Low Energy	Marketed as Bluetooth Smart, a wireless personal area network technology designed for novel applications in the healthcare, fitness, security, and home entertainment industries. Compared to classic Bluetooth, Bluetooth Smart is designed to provide considerably reduced power consumption and cost while maintaining a similar communication range.
Bring Your Own Device (BYOD)	A service option for Enterprise support of Mobile Devices purchased by End Users (employees, contractors, guests, etc.) that are not pre-configured with security policies.
Certificate	In cryptography, a Certificate Authority or Certification Authority is an

Authority	entity that issues digital certificates. Each digital certificate certifies the ownership of a specific public key by the named subject of the certificate (e.g., End User).
Choose Your Own Device (CYOD)	A service option for Enterprise support of Mobile Devices purchased by the End User, which can be pre-configured with Enterprise security policies, and assigned to End Users (employees, contractors, guests, etc.).
Confidentiality [8]	The security goal that generates the requirement for protection against intentional or accidental unauthorized data reads. Confidentiality covers data in storage, during processing, and in transit.
Consumer Electronics	Electronic equipment intended for everyday use, such as radio receivers, television sets, MP3 players, video recorders, DVD players, digital cameras, camcorders, personal computers, video game consoles, telephones, and mobile phones.
Corporate-Owned, Personally-Enabled (COPE)	A service option for Enterprise support of Mobile Devices purchased by the Enterprise, pre-configured with security policies, and assigned to End Users (employees, contractors, guests, etc.).
Customer Relationship Management	A system for managing a company's interactions with current and future customers that involves using technology to organize, automate, and synchronize all sales, marketing, customer service, and technical support activities.
Denial of Service [8]	The prevention of authorized access to resources or the delaying of time-critical operations.
Device Manufacturer	A manufacturer that assembles Mobile Mevices or other computing devices from components typically designed by and manufactured by a number of other suppliers (i.e., the supply chain).
Identity Provider	An Identity Provider, also known as Identity Assertion Provider, creates, maintains, and manages identity information for principals and provides principal authentication to other Service Providers within an identity federation.
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
Integrity [8]	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
Man-in-the-Middle	In cryptography and computer security, a form of active eavesdropping in which the attacker makes independent connections

	with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.
MDM Client	Security agent software installed on an End User's Mobile Device to import and enforce Enterprise security policies for the Mobile Device.
MDM Server	Security management software installed on a Mobile Network Operator or Enterprise server to distribute and enforce Mobile Network Operator and/or Enterprise security policies for Mobile Devices.
Mobile Device Management (MDM)	Security software suites that secure, monitor, manage, and support Mobile Devices deployed across Mobile Network Operators, Service Providers, and Enterprises.
Mobile Financial Services	Mobile banking and mobile payment services offered by banks and other financial institutions.
Mobile Device	A laptop, tablet, smartphone, feature phone, basic phone, or other similar device that typically includes cellular connectivity (2G, 3G, LTE, 5G, etc.) and/or Internet connectivity (Ethernet, WiFi, WiMax, etc.) and associated protocol stacks.
Mobile Network Operator (MNO)	A Mobile Network Operator (MNO), also known as a wireless service provider, wireless carrier, cellular company, or mobile network carrier, is a provider of wireless communications services that manages all the elements necessary to sell and deliver services to an end user including radio spectrum allocation, wireless network infrastructure, back haul infrastructure, billing, customer care, provisioning computer systems and marketing and repair organizations.
Network Access Point(NAP)	A Network) Access Point (NAP) is a device, such as a wireless router, that allows wired or wireless devices to connect to a network. Most access points have built-in routers. Other access points must be connected to a router in order to provide network access. In either case, access points are typically hardwired to other devices, such as network switches or broadband modems.
Near Field Communication (NFC)	A set of standards for smartphones and similar devices to establish radio communication with each other or POS terminals by touching them together or bringing them into proximity, usually no more than a few centimeters.
Network Functions Virtualization (NFV)	Network Functions Virtualization (NFV) aims to transform the way that network operators architect networks by evolving standard IT virtualization technology to consolidate many network equipment types onto industry standard high volume servers, switches and storage, which could be located in a variety of NFVI-PoPs (NFV Infrastructure Points-of-Presence) including data centers, network nodes, and in end user premises.
Network Service	A Network Service Access Point address (NSAP address), defined in

Access Point (NSAP)	ISO/IEC 8348, is an identifying label for a Service Access Point (SAP) used in OSI networking. An NSAP address is comparable to an IP address used in the Internet, e.g., it can specify an ADSL modem – see also Network Access Point.
Over-the-Air	Over-the-air provisioning refers to various methods of using RF communication for distributing new software updates and configuration settings to devices such as cellphones and set-top boxes.
Point-of-Sale (POS)	The physical location where a retail transaction is completed when a customer makes a payment to a merchant in exchange for goods or services – see NFC.
Protected Environment	A hardware protected execution environment (e.g., a Global Platform TEE) that provides high integrity separation and protection of critical system security components (e.g., firmware TPM or trusted UI service)
Registration Portal	An Enterprise or Cloud service (typically a web server) that supports Mobile Device enrollment including End User consent to Enterprise or Cloud policy potential installation of security policies, and potential installation of security agents (e.g., MDM Clients or TNC Clients) on the Mobile Device.
Rich Execution Environment(REE)	In smartphones and other modern Mobile Devices, the Rich Execution Environment (REE) is the normal execution environment where applications and user data reside and is separated by strong hardware protection from the TEE or other Protected Environment (if one is implemented on the Mobile Device).
Risk [8]	The negative system impact considering (1) the probability that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and (2) the resulting impact if this should occur. IT-related risks arise from legal liability or system integrity loss due to— 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information 2. Unintentional errors and omissions 3. IT disruptions due to natural or man-made disasters 4. Failure to exercise due care and diligence in the implementation and operation of the IT system.
Security Goals [8]	The traditional five security goals in NIST SP800-27 [8] are integrity, availability, confidentiality, accountability, and assurance.
Secure Sockets Layer (SSL)	Secure Sockets Layer – a Netscape secure end-to-end transport protocol that was the basis of and is now obsoleted by IETF TLS – often used informally though incorrectly as a synonym for IETF TLS. Note: Both SSL2 and SSL3 have been formally abandoned and deprecated by IETF and are unsafe in all current environments.

Secure Storage	Persistent data storage location where the confidentiality and integrity of data stored therein can be assured (e.g., SED).
Threat [8]	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
TNC Client	Security agent software installed on an End User's Mobile Device that collects and reports device posture or "health" information (identity, state, configuration, etc.).
Transport Layer Security (TLS)	The IETF secure end-to-end transport protocol that was based on the original Netscape SSL and is published in TLS/1.0 (RFC 2246), TLS/1.1 (RFC 4346), TLS/1.2 (RFC 5246), and TLS/1.3 (work-in-progress).
Trusted Execution Environment (TEE)	The Global Platform standard for a Trusted Execution Environment (TEE) is designed to reside alongside the normal smartphone or other Mobile Device Rich Execution Environment (REE) (where normal applications execute) and to provide a safe area of the Mobile Device to protect assets and execute trusted code. At the highest level, a Trusted Execution Environment (TEE) is an environment where the following are true: (a) any code executing inside the TEE is trusted in authenticity and integrity; (b) the other assets are also protected in confidentiality; (c) the TEE resists by design all known remote and software attacks, and a set of external hardware attacks; and (c) both assets and code are protected from unauthorized tracing and control through debug and test features.
Trusted Network Communications (TNC)	Trusted Network Communications (TNC) is a vendor-neutral open architecture and a set of open standards for network security developed by the Trusted Computing Group (TCG). TNC standards integrate security components across end user systems, servers, and network infrastructure devices.
User Equipment (UE)	User Equipment (UE) is a telecom-industry synonym for Mobile Device.
Vulnerability [8]	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

2.2 Actors

In this document the following terms are used to describe certain actors in the use cases.

Actor	**Description**
Application Provider	An entity generating and/or selling user applications to be executed on the platform (e.g. web browser, plug-ins).
Attacker	A person or organization trying to circumvent some security policy of one or more of the other Actors (e.g. Device, Service Provider, Application Provider, or Network Provider).
Communication Carrier	An entity that provides wireless communications (e.g. Wi-Fi, Cellular) functionality to the Device.
Content Provider	The distributor of intellectual property (e.g., software, audio content, video content, etc.) that requires protection.
Device Manufacturer	A manufacturer that assembles Mobile Devices or other computing devices from components typically designed by and manufactured by a number of other suppliers (i.e., the supply chain).
Device Owner	The legal owner of the Mobile Device. The owner may be an End User (consumer), an IT Administrator for an Enterprise, or some other entity.
End User	The ultimate consumer of mobile applications, data, and services, particularly the user for whom the device is designed. The End User may or may not be the Device Owner.
Enterprise	An organization that may support Mobile Devices as a means to access corporate or government data and networks. Besides the End User, the Enterprise is the most common Information Owner with respect to Mobile Devices.
Information Owner	An entity whose information is stored and/or processed on a device. The Information Owner may be the Device Owner, the End User, a Service Provider, Application Provider, Communication Carrier, or Content Provider.
Mobile Device	A laptop, tablet, smartphone, feature phone, basic phone, or other similar device that typically includes cellular connectivity (2G, 3G, LTE, 5G, etc.) and/or Internet connectivity (Ethernet, WiFi, WiMax, etc.) and associated protocol stacks.
Operating System Provider	The entity that provides and maintains (e.g. patches) an Operating System (OS) on a Mobile Device. This includes Hypervisor Virtual Machine Managers, hence it is possible that multiple OSs run on a single device and multiple OS providers can be associated with a single device. Further, there may be multiple repositories used to maintain particular OS components including applications, drivers and libraries.

Service Provider	A network-accessible entity that can provide services to a Device.

2.3 References

[1] TCG Trusted Platform Module Library Family "2.0" Revision 1.38, Parts 1-4, September 2016

[2] TCG Architect's Guide to BYOD Security, June 2012

[3] GlobalPlatform Device Technology TEE System Architecture, GPD_SPE_009, 2016

[4] IETF Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, March 1997

[5] IETF Guidelines for Writing RFC Text on Security Considerations, RFC 3522, July 2003

[6] IETF Universally Unique IDentifier (UUID) URN Namespace, RFC 4122, July 2005

[7] IETF Internet Security Glossary v2, RFC 4949, August 2007

[8] NIST Baseline for Achieving Security, SP800-27, June 2004

[9] NIST Electronic Authentication Guideline, SP800-63-2, August 2013

[10] TCG Glossary, https://trustedcomputinggroup.org/wpcontent/uploads/TCG-Glossary-V1.1-Rev-1.0.pdf , May 2017

[11] NIST Guide for Conducting Risk Assessments, SP800-30r1, September 2012

[12] NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise, SP800-124r1, June 2013

[13] NIST Guidelines on Hardware-Rooted Security in Mobile Devices, SP800-164 draft, October 2012

[14] IETF A One-Time Password System, RFC 2289, Internet Standard, February 1998

[15] IETF HOTP: An HMAC-Based One-Time Password Algorithm, RFC 4226, standards-track, December 2005

[16] IETF TOTP: Time-Based One-Time Password Algorithm, RFC 6238, standards-track, May 2011

[17] TCG TPM 2.0 Mobile Reference Architecture, December 2014

[18] TCG TMI WG Trust Assessment Framework, May 2017

[19] ETSI NFV Use Cases, ETSI GS NFV 001, October 2013

3. Enterprise Mobile Use Cases (BYOD/CYOD/COPE)

3.1 Objective and Scope

There are three commonly used ownership policies for Enterprise Mobile Devices:

- Bring Your Own Device (BYOD) refers to an Enterprise policy that allows an End User (employee or other individual, such as partner, contractor, etc.) to access an Enterprise network through their existing personal Mobile Device.
- Choose Your Own Device (CYOD) refers to an Enterprise policy that allows an End User to choose a Mobile Device from an Enterprise-approved list and personally purchase the Mobile Device.
- Corporate Owned Personally Enabled (COPE) refers to an Enterprise policy where the End User is given an Enterprise-purchased Mobile Device.

Note that various hybrids of BYOD, CYOD, and COPE are common in actual Enterprises.

The advantages to both the Enterprise and End Users are obvious:

- The Enterprise can sometimes use (BYOD/CYOD) to avoid the cost of purchasing a Mobile Device for the End User.
- The End User can have the convenience of carrying only one personalized Mobile Device that has been configured to optimize both End User and Enterprise usage criteria.

Enterprise Mobile Device policies can have serious business consequences if the Mobile Devices are not properly configured and secured. Examples of such business consequences include:

- A non-compliant Mobile Device may be introduced to the Enterprise infrastructure and allowed access.
- Unauthorized or non-business oriented applications that are common on personal Mobile Devices can spread malware that affects the integrity of the Mobile Device and the confidentiality of business data on the Mobile Device.
- A non-compliant Mobile Device without installed monitoring agent(s) may not detect and/or prevent malware from spreading through the Enterprise network.
- Enterprise sensitive information could be disclosed if the Mobile Device is stolen or lost.

On dual-purpose Mobile Devices, Enterprise and End User data are stored on the same device. Striking a balance between strict Enterprise management of a Mobile Device and the privacy of End User personal data on the Mobile Device can be challenging. Overly restrictive or whole device data erasure Enterprise policies can compromise the End User's convenience or place the End User's personal data at risk of being erased by an Enterprise security agent running on the Mobile Device.

The objective of this Enterprise Mobile Device use case is to highlight how TCG and other open standard technologies can be combined to mitigate security concerns associated with Enterprise Mobile Devices. This use case addresses policies, processes, trust assertions, and actor benefits throughout the life cycle of Enterprise Mobile Devices.

3.2 Description

Device Manufacturers develop and Communications Carriers regularly distribute feature updates and improvements for Mobile Devices (smartphones, tablets, and laptops) that enable increasingly sophisticated capabilities. In addition, Mobile Devices are enhanced through new applications downloaded by their users. Mobile Device End Users want to leverage this significant new functionality and use their Mobile Devices as a single portal for all their computing activities (both personal and work-related). Because of this End User interest in "dual-purpose" (personal and work) devices, an increasing number of companies support an Enterprise Mobile Device program today. While many Mobile Devices are purchased by End Users for personal and Enterprise purposes, many are also provided by employers for the convenience of their employees and contractors.

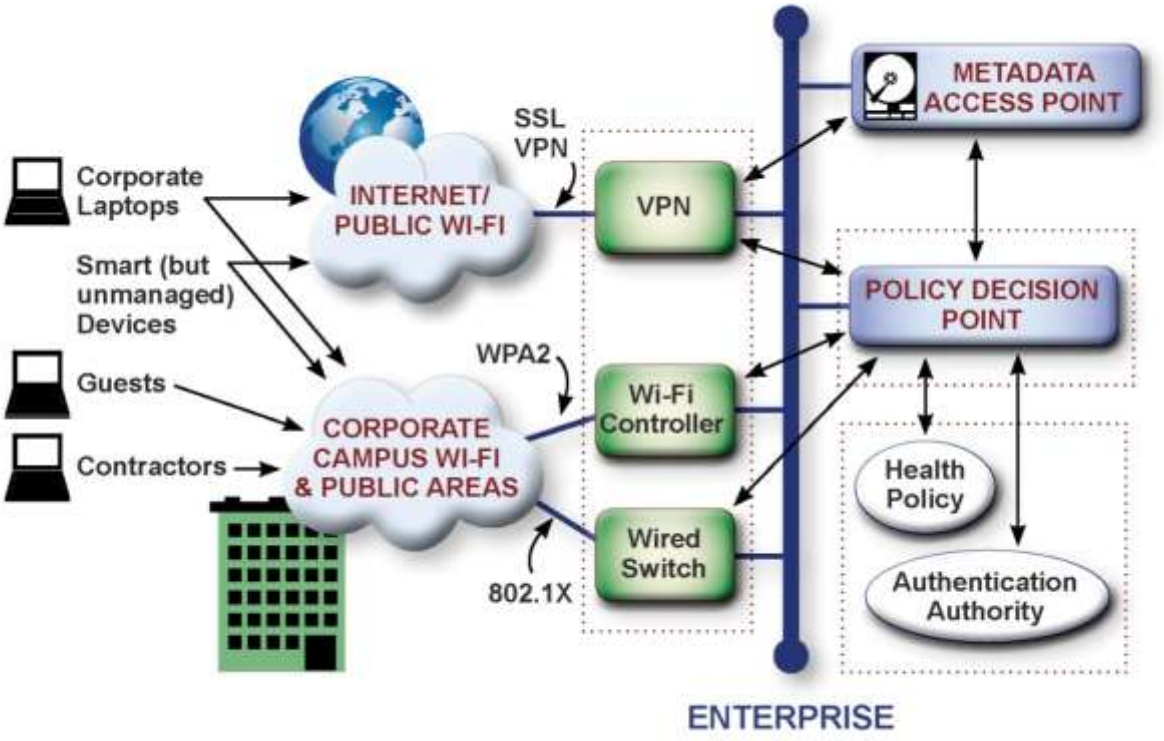


Figure 1 – Enterprise Mobile Device Architecture

Figure 1 above illustrates various stakeholders involved in Enterprise Mobile Device use cases. This architecture diagram is taken from the TCG Architect's Guide to BYOD Security [2] and builds on the concept that escalating the trust in a Mobile Device should allow increased Enterprise access. However, dual-purpose Mobile Devices bring with them a

major caveat – the devices may not be Enterprise-owned but instead owned by the End User and provisioned by several external stakeholders, in addition to the Enterprise itself. This multiple-stakeholder context is inherent in dual-purpose Mobile Devices and adds complexity to the challenge of establishing trust.

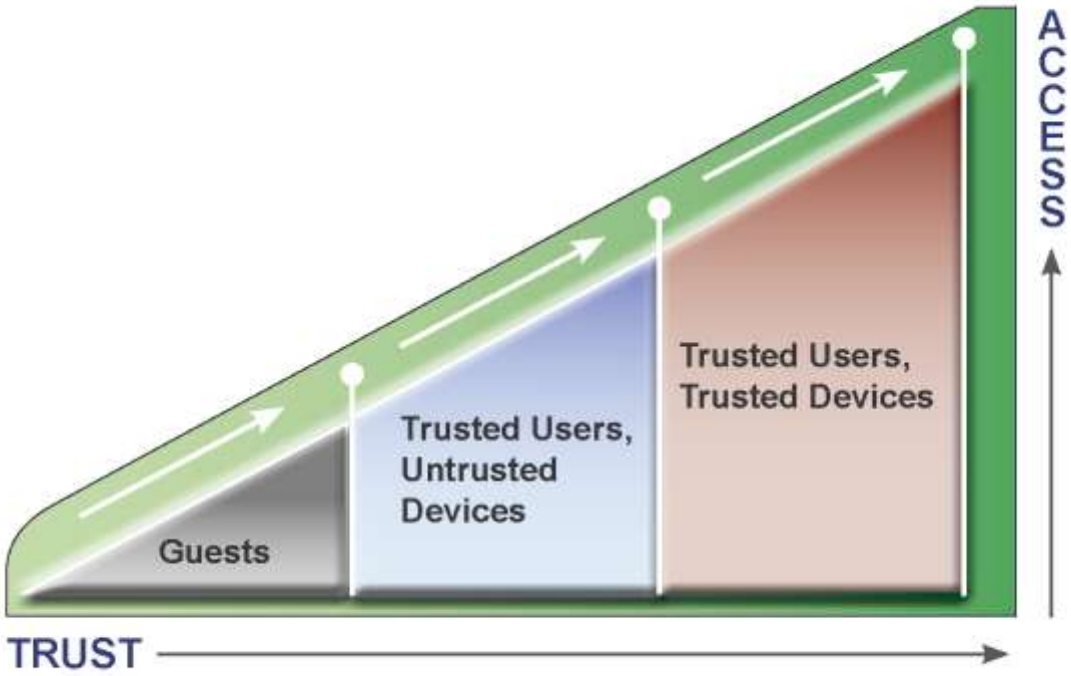


Figure 2 – Escalating Trust Brings Increased Access for Mobile Device Users

Figure 2 above is taken from the TCG Architect's Guide to BYOD Security [2] and illustrates how different End Users should be given different levels of access to corporate resources based on their trust level. Guests with a low level of trust should get little or no access. End Users with trusted devices (such as managed corporate-supplied tablets) should be given the greatest access. In between these two extremes are End Users at different levels of trust, such as staff members with unmanaged devices, or contractors with only "need to know" access.

An Enterprise may define a range of access categories, according to the requirements of the organization. For example, it is common to define a medium access category for contractors, who may have fully compliant devices but are granted a lower level of trust than Enterprise employees. However, the above division into three groups illustrates differentiation based on both authentication information and device trust information.

3.2.1 Mobile Device Enrollment

End Users first perform Enrollment of their Mobile Devices at Enterprise web portals before they can access any Enterprise services. Typically, End Users provide credentials that were previously distributed out-of-band (e.g., temporary passwords), based on physical

identification by Enterprise staff members. This Enrollment phase supplies long-term credentials (e.g., PKI certificates and keys) to the End Users.

3.2.2 Mobile Device Attachment

End Users first perform Attachment of their Mobile Devices to cellular base stations, Wi-Fi access points, cable interfaces, etc., before they can access public or private networks to connect to Enterprise networks. Typically, End Users provide long-term credentials that they acquired during the Enrollment phase above and establish VPN connections to Enterprise networks.

3.3 Benefits for Actors

See section 6 Benefits for Actors for a detailed benefits discussion.

3.4 Solution Assumptions

The solution assumptions for the Enterprise Mobile Device Use Cases are described below:

- The solution components follow best practices for security (confidentiality, integrity, authentication, non-repudiation and availability).
- The solution components are designed to resist both passive and active attacks.
- The solution components are designed to leverage TCG technologies such as TPM Mobile.

3.5 Post-conditions

The post-conditions for the Enterprise Mobile Device Use Case result in either Success or Failure.

3.5.1 Success End Condition

A successful implementation that leverages standards-based security technologies can enable key actors to realize the benefits listed in Section 6.

3.5.2 Failure End Condition

An implementation failure prevents key actors from realizing one or more of the benefits listed in Section 6.

Possible Enterprise Mobile Device Use Case failure end conditions may be:

- End User experiences data loss or theft
- End User cannot connect to Enterprise
- End User experiences decreased functionality of device
- Information Owner experiences data loss or theft
- Information Owner experiences loss of access control to its data
- Enterprise experiences increased IT support costs without productivity/security gains

3.6 Lifecycle Scenarios

See section 7 Lifecycle Scenarios for a discussion of lifecycles for the key actors in the TMS use cases defined in this document.

3.7 Trust Assertions

See section 8 Trust Assertions for a discussion of trust assertions describing trust relationships between key actors in the TMS use cases defined in this document.

This section introduces a set of trust assertions which are used in establishing trust relationships between each of the actors involved in the Enterprise Mobile Device use cases.

3.7.1 Trust Assertions for Enterprise Mobile Devices

The Enterprise Mobile Device use cases are only feasible and useful to the Enterprise if the basic Enterprise security policies can be reliably maintained for Enterprise data and applications upon deployment of Mobile Devices. This imperative implies one of the following conditions:

- The Mobile Device is Enterprise-owned (COPE) and principally managed by the Enterprise, and the End User's personal use does not compromise the Enterprise security posture of the Mobile Device. This condition increases Enterprise confidence in the integrity of the system while it is being used. Even for Enterprise-owned Mobile Devices, the trustworthiness of the device should be periodically assessed, since the Mobile Device is susceptible to attacks whenever it operates inside or outside Enterprise security domain – e.g., when the End User employs the Mobile Device for personal use.
- The Mobile Device is owned by the End User (BYOD or CYOD) but it has an installed security domain which is configured to operate under comparable security constraints for which Enterprise-owned (COPE) Mobile Devices are provisioned. Some Device Owners may regard this level of control as intrusive. A resident Policy Agent on the Enterprise Mobile Device should resolve conflicts between Policies in multiple security domains (e.g., turn off Bluetooth or NFC radios).
- The Mobile Device is owned by the End User (BYOD or CYOD) but fine-grained controls are enforced by Enterprise security policies and an installed Enterprise security agent on the ability of the Mobile Device and End User to access Enterprise resources.

In any case, the level of trust assigned by an Enterprise to a Mobile Device, a mobile application, or an End User should be policy-driven and based on:

1) One or more assessments by the Enterprise of the integrity state of the connecting or requesting Mobile Device;

2) The strength of the authentication mechanisms used to establish the identity of the Mobile Device and the End User;

3) Other operational environment factors that are included in Enterprise policies, e.g., physical or network location.

The Enterprise is concerned about protecting against attacks or loss of data. The End User of a Mobile Device is concerned about protecting their personal information from compromise or inadvertent loss as a side effect of some action taken by the Enterprise. For example, an Enterprise may install a VPN client to establish secure channels between the Mobile Device and the Enterprise and to monitor the download of data from the Enterprise as a means to implement Data Loss Prevention (DLP). The device owner wants assurance that this Enterprise DLP mechanism is not used to monitor personal internet usage or to compromise their own privacy. Additionally, the End User wants assurance that a remote lock or wipe of Enterprise data contained on the Enterprise Mobile Device will not lock or wipe their own personal access and data on the device (could be enforced by an MDM Client).

3.8 Security Policies

See section 10 Security Considerations below.

3.9 Threats and Mitigations

See section 10 Security Considerations below.

3.10 Solution Approaches

See section 9 Solution Approaches below.

4. Financial Use Cases

4.1 Objective and Scope

The objective is to enable the End User to use mobile financial services (e.g. mobile banking and mobile payment) using a hardware-secured Mobile Device such as a mobile phone. The End User should be able to perform point-of-sale (POS) payment transactions with a high degree of confidence.

As the cashless society becomes more pervasive, the likelihood that End Users carry Mobile Devices rather than cash is increasing. Banking also tends to be a more frequent activity, with growing demand for anytime and anywhere convenience.

4.2 Description

4.2.1 Mobile Banking Use Case

Security and usability are fundamental considerations for any mobile banking solution. Any mobile banking solution requires an End User interface (web browser or stand-alone mobile application), an advanced Mobile Device, and strong attestation of device integrity status.

On the other hand, the banking sector has a very fragmented Internet presence. Nevertheless, there are some commonalities.

- Many financial institutions use TLS with authentication to secure the channel between the banking server and the End User's Mobile Device
- Most accesses to banking services are browser based, therefore the concern over phishing attacks is quite common
- Many financial institutions use one-time-passwords [14] [15] [16] that are mailed to the user or can be deduced from a list of passwords that is sent to the user

In addition, some financial institutions consider using user identities provided by governmental organizations. Also, sometimes banking credentials can be used directly at some service providers for strong user authentication (via redirect).

A standardized solution for the provisioning protocol would be preferable, so that all banks would provision in the same way (whereby cross-sector consistency would be achieved) e.g. using OMA Device Management Services as part of their solution.

4.2.2 Mobile Payment Use Case

Security and usability are fundamental considerations for any mobile payment solution. A payment could be made from an account associated with a credit card, debit card, or pre-paid cash portal. The payment protocol could be executed by an application stored at a point-of-sale (POS), although this implementation option introduces additional vulnerabilities as demonstrated by POS attacks in recent years. Other forms of mobile payment include online subscriptions, online payments, person-to-person value transfer, and vending machines.

A payment with an exact amount is authorized by the account owner and potentially also by the financial institution (e.g., enforcing transaction limits, requesting End User PIN values, etc). The transaction authorization could be given either implicitly or explicitly.

For explicit authorization, the account owner could enter a PIN or use biometric authentication to authorize use of the owner's private key to generate a digital signature as a part of the payment transaction.

4.3 Benefits for Actors

See section 6 Benefits for Actors for a detailed benefits discussion.

4.4 Solution Assumptions

The solution assumptions for the Financial Use Cases are described below:

- The solution components follow best practices for security (confidentiality, integrity, authentication, non-repudiation and availability).
- The solution components are designed to resist both passive and active attacks.
- The solution components are designed to leverage TCG technologies such as TPM Mobile.

4.5 Post-conditions

4.5.1 Success End Condition

A successful Financial Use Case implementation leveraging standards-based security technologies can enable actors to realize the benefits listed in Section 4.3.

4.5.2 Failure End Condition

A Financial Use Case implementation without appropriate provisioning and risk mitigation from standards-based security technologies prevents actors from realizing one or more of the benefits listed in Section 4.3.

Possible Financial Use Case failure end conditions may cause:

- End User experiences data loss or theft
- Compliant End User cannot connect to Financial service provider
- End User experience decreased functionality of device
- Information Owner (such as Financial institution) experiences data loss or theft
- Information Owner experiences loss of access control to its data
- Financial service provider experiences increased IT support costs without productivity/security gain

4.6 Lifecycle Scenarios

See section 7 Lifecycle Scenarios for a discussion of lifecycles for the key actors in the TMS use cases defined in this document.

4.7 Trust Assertions

See section 8 Trust Assertions for a discussion of trust assertions describing trust relationships between key actors in the TMS use cases defined in this document.

4.7.1 Trust Assertions for Financial Use Cases

The Financial use cases are only feasible and useful for the Financial institution if the basic Financial institution security policies can be reliably maintained for Financial institution data and applications upon deployment of Mobile Devices.

In any case, the level of trust assigned by a Financial institution to a Mobile Device, a mobile application, or an End User should be policy-driven and based on:

1) One or more assessments by the Financial institution of the integrity state of the connecting or requesting Mobile Device;

2) The strength of the authentication mechanisms used to establish the identity of the Mobile Device and the End User;

3) Other operational environment factors that are included in Financial institution policies, e.g., physical or network location.

The Financial institution is concerned about protecting against attacks or loss of data. The End User of a Mobile Device is concerned about protecting their personal information from compromise or inadvertent loss as a side effect of some action taken by the Financial institution.

4.8 Security Policies

See section 10 Security Considerations below.

4.9 Threats and Mitigations

See section 10 Security Considerations below.

4.10 Solution Approaches

See section 9 Solution Approaches below.

5. NFV Use Cases

ETSI Network Functions Virtualization (NFV) Use Cases [19] describes a set of use cases in considerable detail, e.g., NFV Infrastructure as a Service and Virtualization of Mobile Core Network and IMS, and describes the context for ETSI NFV development activities.

5.1 Objective and Scope

The objective is to enable the Mobile Network Operator (MNO) to create, provision, manage, and verify Virtual Network Functions (VNFs) in service chains and distributed hybrid Cloud/SDN/Native network environments to perform normal core network functions (e.g., HSS, etc.). The presence of these VNF service chains should be transparent to the End Users of supported Mobile Devices. These VNF service chains should achieve a high level of reliability, accountability, and failover redundancy.

5.2 Description

In NFV use case scenarios, the central theme is that confidential and private information related to a transaction is circulated between several parties for consumption, frequently through intermediaries. The goal of proposed solutions is to minimize the replication of information and replace such replication by secure sharing of VNF processing functions with the logically central holding entity. Proposed solutions allow this processing and the generation of appropriate authorization assertions to be carried out such that the information required for processing never leaves one logically central holding entity. Exposure of the information is minimized by avoiding unnecessary distribution and replication and making the information available to selected authorized processes, only remotely instantiated and hosted in the logically central holding entity.

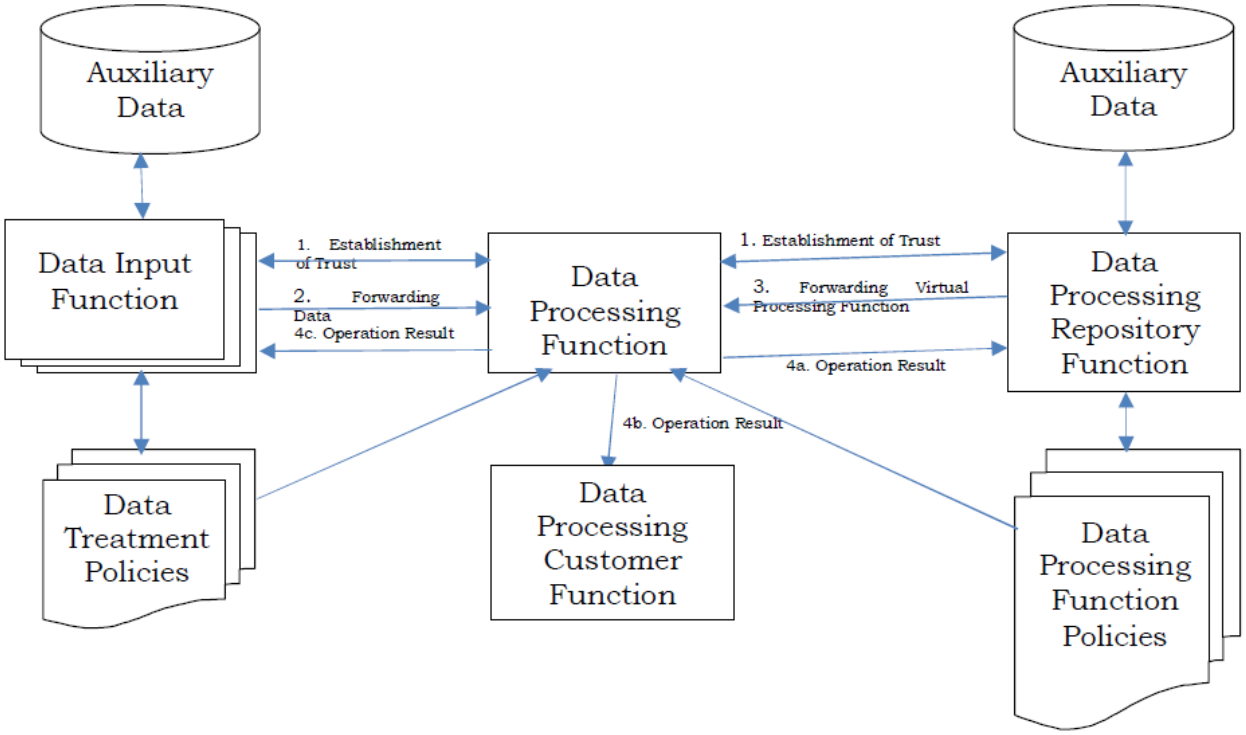


Figure 3 – NFV Use Case Simplified Functional Diagram

Figure 3 shows the NFV functional entities performing the following process flow steps:

1. The Data Input Function(s) establishes trust with the Data Processing Function. The Data Processing Repository Function establishes trust with the Data Processing Function. Appropriate Data Treatment Policies and Data Processing Function Policies are determined.
2. Using the Data Treatment Policies, the Data Input Function securely forwards its data to the Data Processing Function, which is a functional entity designated to perform all processing functions on transaction data.
3. Using the Data Processing Function Policies, the Data Processing Repository Function securely forwards Virtual Processing Functions to the Data Processing Function for the data from the Data Input Function. The Data Processing Function Policies and Data Processing Repository Function policies determine the physical placement of the Data Processing Function as a safe and optimal network location for processing of the transaction data.
4. The data processing results are generated by the Data Processing Function and forwarded to either one or all of the Data Input Function, Data Processing Repository Function, and/or Data Processing Customer Function.

To ensure the secure storage and secure processing of transaction data, virtualization and policy driven methods should be used to restrict access to private information.

Within the transaction scope of this procedure, the NFV functional components above should be formally evaluated and certified to assure that private information is not compromised and only legitimate functions are performed. Transaction private data can

also be confidentiality protected via encryption In the case of personal user data, each individual owner's stored data should be encrypted to reduce the attack surface of data held in storage locations. The owner's authorization credentials should be obtained during transaction processing and securely disposed of after processing has completed.

The first two use cases below show improved data protection mechanisms combined with virtualization and platform integrity techniques to help alleviate the loss of privacy/confidentiality during various secure and trustworthy operations conducted by a third party consuming the data.

5.2.1 Retailer Credit Check with Consumer Privacy Use Case

This use case enables a retailer to perform a check of creditworthiness of a consumer with a credit rating agency. The specific retailer in this example is a Mobile Network Operator (MNO) who wishes to check creditworthiness of a consumer prior to establishment of a postpaid mobile subscription. In this use case the End User's (applicant for the postpaid subscription) private information is being collected at the endpoint computing device (e.g., mobile phone, PC, MNO kiosk, etc.) and forwarded to either a 2nd Party processor (i.e., MNO) or 3rd Party processor (e.g., Credit Reporting Agency) for processing and generating the Authorization Assertion or Weighted Authorization Score (e.g., credit report). The nature of the private information requires its removal/deletion following consumption and upon production of the credit worthiness assertions as described above. However, such a policy is practically unenforceable from the End Users' point of view. Accumulation of End Users' private information at either the MNO (second party) or 3rd Party processors creates an attraction for unlawful access to such information from either inside or outside adversaries either during the time of consumption or when the personal data is stored at these entities.

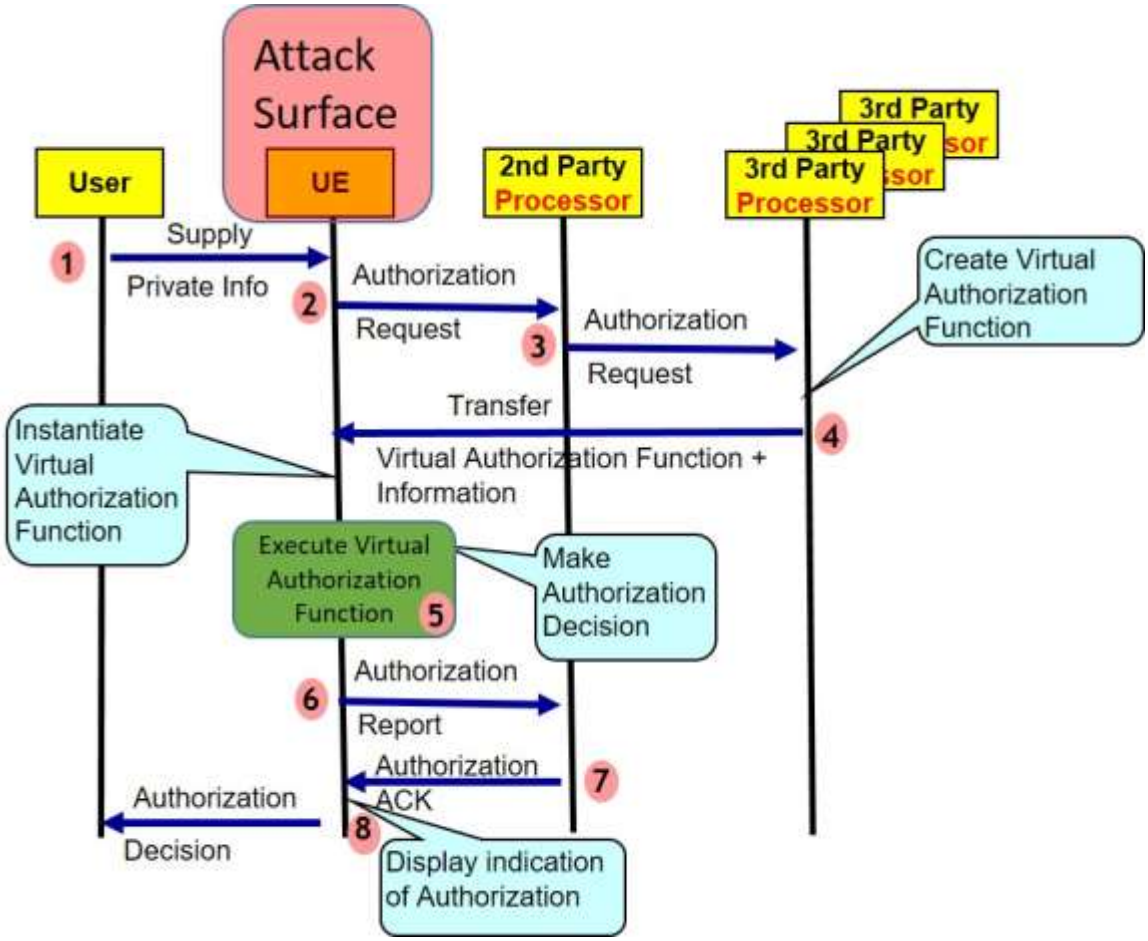


Figure 4 – Retailer Credit Check with Consumer Privacy

Information Flow:

1) User inputs his/her private/confidential information into his/her terminal equipment (denoted UE (User Equipment, the actual End User's Mobile Device) on the diagram)
2) The UE stores private/confidential information locally in protected memory and forwards Authorization Request to the 2nd Party data Processor (e.g., MNO)
3) The 2nd Party Processor (e.g., MNO) forwards Authorization Request to the 3rd Party data Processor (e.g., Credit Rating Agency)
4) The 3rd Party Processor (e.g., Credit Rating Agency) creates Virtual Authorization Function and transfers it to the UE for instantiation. Note that this transfer may be achieved either directly to the UE or through the 2nd Party Processor (e.g., MNO)
5) The UE verifies the integrity and authenticity of the received Virtual Authorization Function received in Step 4, instantiates and executes (e.g., computes Credit Score or assertion of Authorization) Virtual Authorization Function in its protected execution environment using the End User's private/confidential information from Step 2 and computes the Authorization Decision in the process. Note that it is

possible that any of the 3rd parties may have previously interacted with the End User and stored some of the End User's personal information or processed information at the End User's UE for later consumption (for example, personal End User credit history data collected over a period of time). The integrity and authenticity of the received Virtual Authorization Function can be verified by implementing one or more of industry standard methods (e.g., signed hash of the code, pre-provisioned vendor certificate, etc).

6) The UE transfers the computational result (i.e., credit score or assertion of authorization) from Step 5 to the 2nd Party Processor (e.g., MNO). End User is either authorized or not authorized.
7) The 2nd Party Processor acknowledges to the UE the receipt of the computational result (i.e.., credit score or assertion of authorization)
8) The Authorization decision is communicated to the End User

5.2.2 Network Entity Authentication for Network Admission

This use case demonstrates authentication of a UE to a network resource. The proposed information flow depicted in Figure 5 demonstrates the reduction of the attack surface achieved by the proposed solution.

In the traditional information flow of Figure 5, the user's credentials are propagated all the way to the Authentication Server. However, in the proposed information flow, the user's credentials do not leave the trusted perimeter of the user's UE.

Note that this use case also illustrates a policy-driven selection of a virtual authentication function (e.g. based on heuristic algorithm or set of predefined parameters (time of day, location, etc.).

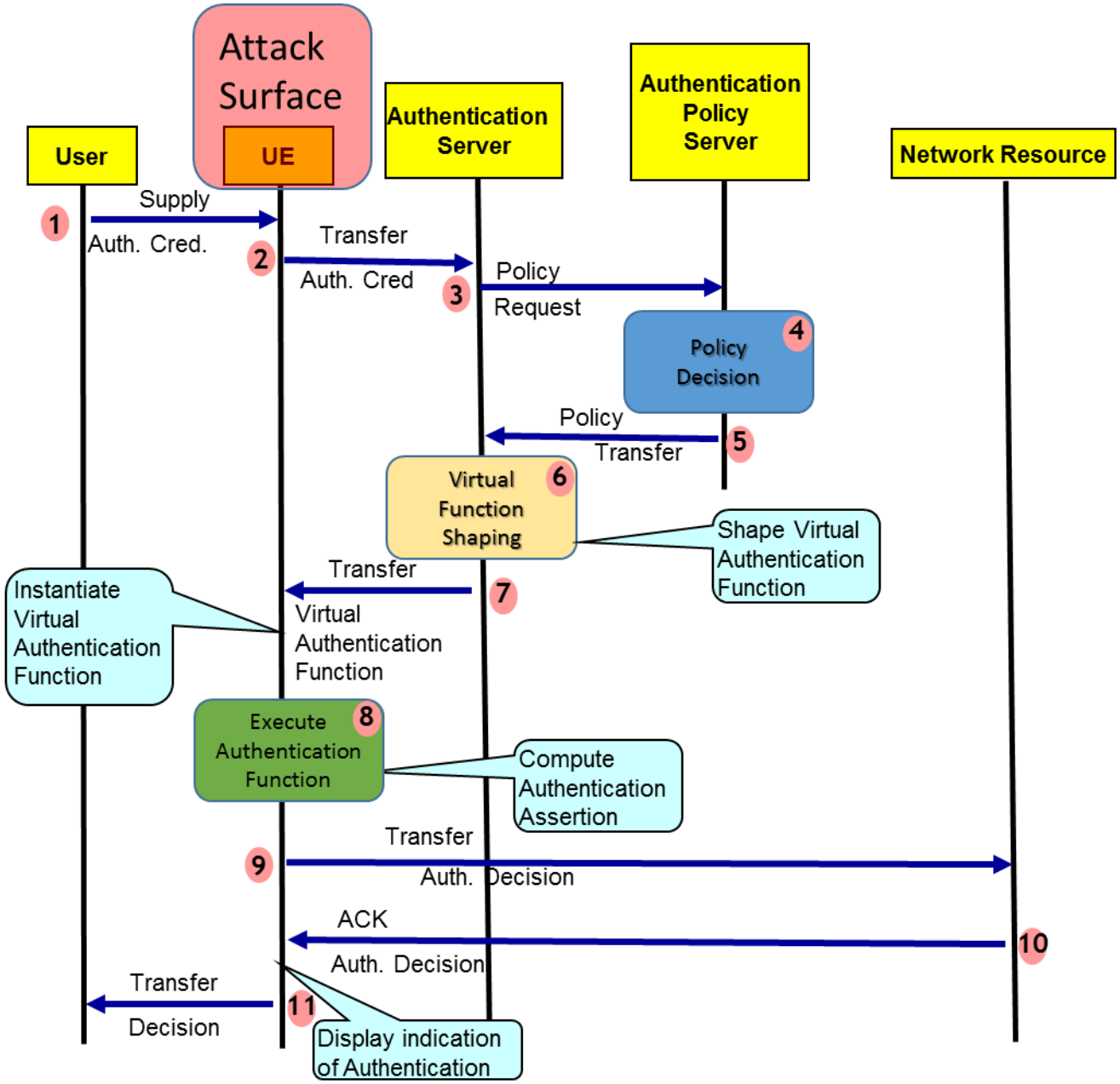


Figure 5 – Network Entity Authentication for Network Admission

Information Flow:

1) End Users input their identity and Authentication Credential(s) into their terminal equipment (denoted as UE (User Equipment, the actual End User's Mobile Device) in this diagram)
2) The UE forwards identity and Authentication Credential(s) or their hash to the Authentication Server

3) The Authentication Server creates the Policy Request (i.e., requesting a particular Authentication Policy for a particular End User Identity) and sends it to the Authentication Policy Server
4) The Authentication Policy Server computes the appropriate Authentication Policy executing Authentication Function (e.g., comparing the supplied set of credentials or its hash for the given identity to the set of credentials or its hash stored at the Authentication Server)
5) The Authentication Policy Server transfers Authentication Policy from Step 4 to the Authentication Server
6) The Authentication Server creates/selects Virtual Authentication Function based on the Authentication Policy received in Step 5. This is achieved by Virtual Function Shaping, i.e., selecting from available Virtual Authentication Functions or creating the Virtual Authentication Function that is shaped to satisfy the UE capabilities and the Authentication Policy. For example, the Virtual Authentication Function will not ask for the user fingerprint if the UE is not equipped with or cannot furnish a trusted fingerprint reader. Instead, the Virtual Authentication Function could ask for and process two authentication factors and UE location.
7) The Authentication Server forwards Virtual Authentication Function created/selected in Step 6 to the UE for execution on behalf of the Authentication Server.
8) The UE verifies the integrity and authenticity of the received Virtual Authentication Function received in Step 7, instantiates and executes it on behalf of the Authentication Server, and computes the Authentication Assertion, i.e., the Authentication Decision. The integrity and authenticity of the received Virtual Authentication Function can be verified by implementing one or more of industry standard methods, e.g., signed hash of the code, pre-provisioned vendor certificate, etc.
9) The UE forwards the Authentication Assertion, i.e., the Authentication Decision computed in Step 8 to the Network Resource
10) The Network Resource acknowledges to the UE the receipt of the Authentication Assertion from Step 9
11) The Authentication Decision is communicated to the End User

5.3 Benefits for Actors

See section 6 Benefits for Actors for a detailed discussion of benefits.

5.4 Solution Assumptions

The solution assumptions for the NFV Use Cases are described below:

- The solution components follow best practices for security (confidentiality, integrity, authentication, non-repudiation and availability).
- The solution components are designed to resist both passive and active attacks.
- The solution components are designed to leverage TCG technologies such as TPM Mobile.

5.5 Post-conditions

5.5.1 Success End Condition

A successful NFV Use Case implementation leveraging standards-based security technologies can enable actors to realize the benefits listed in Section 5.3.

5.5.2 Failure End Condition

An NFV Use Case implementation without appropriate provisioning and risk mitigation from standards-based security technologies prevents actors from realizing one or more of the benefits listed in Section 5.3.

Possible Financial Use Case failure end conditions may cause:

- End User experiences data loss or theft
- Compliant End User cannot connect to NFV service provider
- End User experiences decreased functionality of device
- Information Owner (such as NFV service provider) experiences data loss or theft
- Information Owner experiences loss of access control to its data
- NFV service provider experiences increased IT support costs without productivity/security gain

5.6 Lifecycle Scenarios

See section 7 Lifecycle Scenarios for a discussion of lifecycles for the key actors in the TMS use cases defined in this document.

5.7 Trust Assertions

See section 8 Trust Assertions for a discussion of trust assertions describing trust relationships between key actors in the TMS use cases defined in this document.

5.7.1 Trust Assertions for NFV Use Cases

The NFV use cases are only feasible and useful for the Communications Carrier if the basic Communications Carrier security policies can be reliably maintained for Communications Carrier data and applications upon deployment of Mobile Devices.

In any case, the level of trust assigned by a Communications Carrier to a Mobile Device is policy-driven and based on:

1) One or more assessments by the Communications Carrier of the integrity state of the connecting or requesting Mobile Device;

2) The strength of the authentication mechanisms used to establish the identity of the Mobile Device;

3) Other operational environment factors that are included in Communications Carrier policies, e.g., physical or network location.

The Communications Carrier is concerned about protecting against attacks or loss of data or services. The End User of a Mobile Device is concerned about protecting their personal

information from compromise or inadvertent loss as a side effect of some action taken by the Communications Carrier.

5.8 Security Policies

See section 10 Security Considerations below.

5.9 Threats and Mitigations

See section 10 Security Considerations below.

5.10 Solution Approaches

See section 9 Solution Approaches below.

6. Benefits for Actors

This section identifies the principal actors for the Mobile Device use cases as well as the associated benefits obtained from the implementation of a properly structured and managed deployment.

6.1 End User

End Users benefit from a secure Mobile Device implementation as follows:

1. Device protection – Enterprises and Communications Carriers deploy Mobile Device protection features, such as malware detection and anti-virus scanners, that enhance integrity protection for the End User.
2. Privacy of personal data – End Users are assured that their personal data won't be viewed, corrupted, or erased by other stakeholders on the Mobile Device.
3. Convenience for End User – By combining personal and work usage in one Mobile Device, an End User can reduce the number of devices they carry, thus increasing functional security and minimizing their learning curve, and choose and install applications.
4. Improved connectivity – Mobile Devices achieve improved access to Service Provider resources, which increases the End User productivity.

End Users benefit from choosing mobile banking services as follows:

1. Convenience – End User account queries are simplified.
2. Verification – End User Transactions can be verified (possibly using separate verification/confirmation channel for large transfers).
3. Notifications – Service Providers can send account balance and security alerts to End Users in real-time.
4. Renewal – Service Providers can send subscription reminders to End Users to avoid interruptions in service.
5. Agility – End Users can be offered payment method flexibility and be assured that their financial transactions are performed securely.

End Users can gain additional benefits from using mobile banking services augmented by Trusted Computing technologies:

1. The overall mobile End User experience can be enhanced by the anytime and anywhere convenience of trustworthy mobile banking.
2. Fraud risks can be reduced for both End User and Service Provider, as banking data and associated secrets can be strongly protected using Trusted Computing technologies. Reduced fraud for the Service Provider can help the End User too, through greater diversity of Service Providers supporting mobile banking.

3. Privacy and trust are enhanced. The Mobile Device can protect against interception and eavesdropping on banking transactions using Trusted Computing technologies.

6.2 Device Owner

An End User may be a Device Owner (BYOD/CYOD) and therefore responsible for purchase, management, and upkeep of the Mobile Device or an Enterprise may be the Device Owner (COPE). A Device Owner benefits from a secure Mobile Device implementation as follows:

1. End User actor – In the case of a personally-owned Mobile Device (BYOD/CYOD), the same benefits as an End User actor above.
2. Enterprise actor – In the case of an Enterprise-owned Mobile Device (COPE), the same benefits as an Enterprise actor below.

6.3 Device Manufacturer

A Device Manufacturer designs and manufactures a versatile Mobile Device that supports flexible deployment by Enterprises and Communications Carriers. A Device Manufacturer benefits from a secure Mobile Device implementation as follows:

1. Increased revenue – By satisfying the security goals of consumers and business partners, the Device Manufacturer can benefit from additional revenue from their flexible Mobile Devices as well as value-added application bundles.
2. Expanded markets – By enhancing the value chain to enable secure mobile banking, the Device Manufacturer can benefit from new market and revenue opportunities.

6.4 Information Owner

An Information Owner is the ultimate legal rights holder for a given set of data. There will typically be multiple Information Owners associated with any given Mobile Device. These Information Owners may include Enterprises, End Users, business clients and customers of Enterprises, and various intellectual property holders of licensed content and applications.

An Information Owner benefits from a secure Mobile Device implementation as follows:

1. Increased trust – The Information Owner can trust that the Mobile Device will access Information Owner services and data appropriately.
2. Improved confidentiality and availability – An Information Owner can trust that data stored on the Mobile Device will have enhanced confidentiality, integrity and availability.
3. Reliable service termination – An Information Owner can terminate every actors' access to the Information Owner's applications and data.

6.5 Enterprise

An Enterprise benefits from a secure Mobile Device implementation as follows:

1. Cost of acquisition – The End User may be responsible (BYOD/CYOD) for the purchase and maintenance of the Mobile Device, thus relieving the Enterprise of the associated acquisition costs, as well as some or all of the recurring monthly costs.
2. Improved productivity – The End User may already be familiar with the Mobile Device operation, so that there is a reduced learning curve. This can also reduce End User training costs for the Enterprise.
3. End User availability to the Enterprise – By use of an End User's personal Mobile Device there can be increased availability and reachability of the End User, when required for emergency work or other exceptional Enterprise tasks.

6.6 Service Providers

Service Providers furnish services and sometimes also furnish equipment. Service Providers may include Communications Carriers, Application Providers, Content Providers, Operating System Providers, and Device Manufacturers.

A Service Provider benefits from a secure Mobile Device implementation as follows:

1. Increased revenue – By satisfying the security goals of consumers and business partners, a Service Provider can benefit from additional revenue from their flexible mobile services as well as value-added application bundles.

Mobile Financial Service Providers (such as banks) and Retailers can benefit from mobile banking services (without losing control or adding additional expenses for special hardware) as follows:

1. Ease of use – End Users can avoid visits to the physical premises of Mobile Financial Service Providers to do most or all of their banking transactions. Mobile financial service providers and Retailers can benefit from offering payment method flexibility and transactional security.
2. Increased trust – By using standard TCG technologies, hardware-secured Mobile Devices can validate presented credentials, defend against phishing attacks, protect transactions and data-at-rest, across a wide range of Mobile Devices.
3. Simplified provisioning – There may be a reduced need for contracts and cooperation with a large range of local operators.
4. Infrastructure reuse – Existing front-end and back-end financial systems can also be used for mobile services.

6.7 Communication Carrier

In various Mobile Device use cases, a Communication Carrier provides network access (cellular, WiFi, etc.) and connectivity between a Mobile Device and an Enterprise network. Typically, the Communication Carrier is the vendor of the Mobile Device and is responsible for providing patches and updates to the Mobile Device.

A Communication Carrier benefits from a secure Mobile Device implementation as follows:

1. Increased revenue – A Communication Carrier can benefit from additional revenue from the purchase of their services, including new services such as Mobile Device usage enablement, integrated policy management, and increased security.

2. Reduced security compromises – a Communication Carrier can benefit from reduced operating costs due to fewer Mobile Devices being compromised on their network and/or compromising their network infrastructure servers.

6.8 Application Provider or Content Provider

An Application Provider supplies the applications for a Mobile Device, while a Content Provider supplies the data to be consumed on the Mobile Device (e.g., email, music, video, maps). This content may be commercially licensed intellectual property. Enterprises typically also act as Application Providers and Content Providers.

An Application Provider or Content Provider benefits from a secure Mobile Device implementation as follows:

1. Increased revenue – An independent Application Provider or Content Provider (not associated with a specific Enterprise) can benefit from additional revenue from their value-added application bundles.

6.9 Operating System Provider

An Operating System Provider (closed or open source) supplies an operating system that supports secure Mobile Device operations. An Operating System Provider creates and distributes patches and updates for this operating system.

An Operating System Provider benefits from a secure Mobile Device implementation as follows:

1. Increased revenue – An Operating System Provider can benefit from additional revenue from their Enterprise-enabled Operating Systems.

7. Lifecycle Scenarios

Lifecycles for the principal actors of the Mobile use cases are described and discussed.

7.1 Device Manufacturer Lifecycle

Assumptions:

1. Device Manufacturer installs a TPM , hypervisor, SIM/UICC, or other isolated Protected Environment - and other standards-based technology.
2. Device Manufacturer and/or separate remote authority provisions the Protected Environment and installs pre-loaded applications that use the Protected Environment.
3. Device Manufacturer verifies and audits (when possible) all Supply Chain activities.
4. Multiple Device part suppliers are involved in Device manufacturing.
    - OEM and Part Suppliers may not trust each other.
    - Individual parts of the Device may have untrusted "built-in" functionality

The following table summarizes the activities associated with each lifecycle stage for the Device Manufacturer.

Table 7-1 Device Manufacturer Lifecycle

Lifecycle stage	Activities undertaken during this stage
Manufacture / Initialization	• Provisioning by the Device Manufacturer, Communication Carrier, or separate remote authority of TPM, TNC, SED, and other standards-based technologies suitable for mobile systems • The Contract Manufacturer (or Device Manufacturer itself) assembles hardware and software from multiple suppliers and delivers device to the Device Manufacturer. The delivered device includes pre-provisioned TPM (or other standards-based technology) with the Device Manufacturer's keys • Keys may be delivered remotely, assuming pre-placed keys (or similar) were provisioned during TPM installation
Provisioning / Enrollment	• Device Provisioning may be performed by Contract Manufacturer prior to delivery to Device Manufacturer (see above) • Otherwise, Device Provisioning must be performed by another actor, such as Communication Carrier or Device Manufacturer • Device Manufacturer provides a strongly authenticated, trusted Device Identity for attestation and endpoint health

	assessment
Use / Customization	• Device Manufacturer, OS Provider(s) or Enterprise provide Application and associated Policy provisioning • Device Manufacturer or OS Provider(s) provides Application and associated Policy updates • Device Manufacturer or OS Provider verifies Application update integrity
Service Update	• Device Manufacturer may distribute OS or driver patches under the Platform Authority defined in TPM 2.0 Library
Service Termination	• Enterprise app/data wipe, Policy De-provisioning • If device returned to Device Manufacturer, de-provisioning of keys (Endorsement Keys, Storage Keys), End User/Enterprise data wipe from memory • Take ownership away from Communication Carrier, e.g., via Factory reset • Remanufacture/refurbish and resell Device
Device Retirement	• If Device is lost, damaged or exchanged with Communication Carrier, perform Service Termination steps above if possible • Provide proof of destruction to Communication Carrier or Device Manufacturer (e.g. to avoid per-device license fees)

7.2 Communication Carrier Lifecycle

Assumptions:

1. The Communication Carrier or separate remote authority provisions the TPM, hypervisor, SIM/UICC, or other isolated Protected Environment.
2. The Communication Carrier installs all standard applications.

The following table summarizes the activities associated with each lifecycle stage for the Communication Carrier.

Table 7-2 Communication Carrier Lifecycle

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialization	• N/A
Provisioning / Enrollment	• Communication Carrier provides and controls access credentials (e.g., SIM/USIM credentials residing on

	SIM/UICC) • Communication Carrier performs "Take Ownership" of the TPM (or other standards-based technology) based on delegation from the Device Manufacturer • Communication Carrier enrolls Device Owner for mobile service and completes provisioning of the device
Use / Customization	• Communication Carrier and/or Application Provider could provide new applications for download that use the TPM • Communication Carrier could verify App integrity
Service Update	• Communication Carrier may distribute OS or driver patches (e.g., under the Platform Authority defined in TPM 2.0 Library)
Service Termination	• Deprovision Device Owner account with Communication Carrier • Wipe Communication Carrier-specific apps/data/keys
Device Retirement	• If Device is lost, damaged or exchanged with Communication Carrier, perform Service Termination steps above if possible

7.3 Device Owner Lifecycle

Assumptions:

1. Device Owner purchases device and enrolls/subscribes in a service plan from a Communication Carrier or their distributor.

The following table summarizes the activities associated with each lifecycle stage for the Device Owner.

Table 7-3 Device Owner Lifecycle

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialization	• N/A
Provisioning / Enrollment	• Device Owner purchases device and enrolls/subscribes in a service plan from a Communication Carrier – Communication Carrier or stand-alone policy server provisions usage/security policies and cryptographic keys (e.g. Child Endorsement Keys) into the device • Device Owner downloads and installs security agents and other applications provided by an authenticated Communication Carrier, other Application Provider, or authenticated Enterprise

Use / Customization	• Device Owner, Communication Carrier, or OS/TPM/App Provider performs OS/application rollback if patch/application install fails • Device Owner imports PIM data (e.g. email, address book) • Device Owner makes/receives calls/messages that generate more personal data (e.g. phone logs, SMS) • Device Owner initiates secure Internet access for personal use (e.g. Wireless hotspot) • Device Owner initiates connections to commercial/public websites • Device Owner initiates/uses/terminates VPN tunnel connections to Enterprise networks and Cloud providers, and accesses Enterprise resources
Service Update	• Device Owner downloads/installs patches/updates for personal/Enterprise applications and OS • Device Owner renews service plan and Communication Carrier updates policies accordingly
Service Termination	• Enterprise performs Enterprise app/data wipe and de-provisioning • Device Owner performs End User app/data wipe and de-provisioning • Communication Carrier performs Communication Carrier app/data wipe and de-provisioning • Device Owner or Communication Carrier cancels service plan based on Device Owner request or plan expiration
Device Retirement	• If Device is lost, damaged or exchanged with Communication Carrier, perform Service Termination steps above if possible • Device Owner wipes any residual Enterprise, Communication Carrier, end user applications or data • Device Owner relinquishes ownership of device (e.g. return to Communication Carrier or Device Manufacturer, recycle)

7.4 Enterprise Lifecycle

Assumptions:

1. Enterprise provides a registration portal for Device enrollment and provisioning.

The following table summarizes the activities associated with each lifecycle stage for Enterprise Mobile Device.

Table 7-4 Enterprise Lifecycle

Lifecycle stage	Activities undertaken during this stage
Manufacture / Initialization	• Pre-condition of Device Manufacturer including capabilities such as TPM and hardware Root of Trust
Provisioning / Enrollment	• When a Device Owner, via a Device, authenticates the Device identity to an Enterprise authentication server (e.g. RADIUS), the Enterprise validates the authentication and, if it is acceptable, provides a VPN IP address to the device and authorization to access the Enterprise network and Cloud provider resources • Registration Portal provides Enterprise MDM Client, VPN client, browser or other policy-enabled software for download by the Device Owner • Registration Portal provisions device with certificates and enrolls Device in Enterprise directory services
Use / Customization	• Enterprise provides PIM data to Device (e.g. email, address book) • Enterprise security agent verifies Device compliance with Enterprise security policy (e.g. Health/Integrity check, App blacklist/whitelist, location awareness) • Enterprise VPN client allows access to Enterprise network and Cloud provider resources • Enterprise manages virtualized application state migration across multiple Devices • Enterprise and Device Owner select online and offline power management configurations (e.g., suspend, hibernate, resume)
Service Update	• Enterprise updates Access Control Policies and other Enterprise security configurations for Device and End User • Enterprise distributes updated Enterprise applications
Service Termination	• Enterprise performs Enterprise app/data wipe and de-provisioning (e.g. remove Device from directory services, RADIUS, etc.)
Device Retirement	• If Device is lost, damaged or exchanged with Communication Carrier, perform Service Termination steps above if possible • Device Owner wipes any residual Enterprise, Communication Carrier, end user applications or data • Device Owner relinquishes ownership of device (e.g. return to Communication Carrier or Device Manufacturer, recycle)

7.5 Service Provider Lifecycle

Assumptions:

1. The Service Provider provisions access policies and configuration for the Service on the mobile Device.
2. The Service Provider supplies applications and data for installation on the mobile Device.

The following table summarizes the activities associated with each lifecycle stage for the Service Provider.

Table 7-5 Service Provider Lifecycle

Lifecycle stage	Activities undertaken during this stage
Manufacture / Initialization	Pre-condition of Device Manufacturer including capabilities such as TPM and hardware Root of Trust
Provisioning / Enrollment	• When a Device Owner wants a specific Service (Financial, Medical, Email, etc.), the Device Owner can discover and contact a Registration Portal (typically via a web browser) • Registration Portal provides Service App software (browser scripts, Java, etc.) for download by the Device Owner • Service Provider provides and controls access credentials for the End User of the Service, which could be stored in the TPM (or other standards-based technology) • Service Provider enrolls Device for requested Service and completes provisioning of the Service
Use / Customization	• Service Provider could provide new applications for download that use the mobile Device • Service Provider could verify App integrity
Service Update	• Service Provider may distribute application patches (e.g., under the Endorsement Authority defined in TPM 2.0 Library)
Service Termination	• Deprovision Device Owner account with Service Provider. • Wipe Service Provider-specific apps/data/keys
Device Retirement	• If Device is lost, damaged, or changes ownership, perform Service Termination steps above if possible

7.6 VNF Software Lifecycle

Assumptions:

1. The VNF Software Manufacturer provisions access policies and configuration for use of the VNF software in the Cloud.
2. The VNF Software Manufacturer supplies VNF software for download and installation on an NFV Infrastructure Provider server with an associated license.

The following table summarizes the activities associated with each lifecycle stage for the VNF Software.

Table 7-6 VNF Software Lifecycle

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialization	• VNF Software Manufacturer creates VNF software including capabilities such as TPM and hardware Root of Trust and creates digital software license
Provisioning / Instantiation	• When an NFV Infrastructure Provider wants to deploy VNF software, it first validates the license terms • VNF Software Manufacturer provides VNF software for download by the NFV Infrastructure Provider • VNF Software Manufacturer provides and controls access credentials for the instantiation of the VNF instance, which could be stored in an NFV Infrastructure Provider server TPM (or other standards-based technology) • VNF Software Manufacturer enrolls NFV Infrastructure Provider for use of requested VNF software • NFV Infrastructure Provider instantiates VNF instance on demand in a Service Chain
Use / Customization	• VNF Software Manufacturer could provide new versions of VNF software for download and use by the NFV Infrastructure Provider • VNF Software Manufacturer could verify VNF software integrity
Software Update	• VNF Software Manufacturer may distribute VNF software patches (e.g., under the Endorsement Authority defined in TPM 2.0 Library)
Software Termination	• Deprovision NFV Infrastructure Provider account with VNF Software Manufacturer • Wipe NFV Infrastructure Provider-specific data/keys

7.7 Lifecycle Solution Requirements

The above lifecycles imply the following solution requirements for Mobile Device deployments.

1. Interoperable, standards-based Policy statements that support vendor and/or site-specific extensions.
2. Logical and secure separation of personal and Enterprise data/apps for storage (e.g., TCG SEDs), execution (e.g., GP TEE), and verification of device integrity (e.g., TPM)
3. Authentication infra-structure to verify Device identity.
4. Interoperable standards-based Mobile Device Management (MDM) solutions
5. Means for resolution/reconciliation of multiple (possibly conflicting) MDM policies on a particular Mobile Device.
6. Correlation of End User Identities across multiple Mobile Devices, as well as End User Roles, Certificates, Keys. There may be a hierarchy of Users and Devices that need to be managed.
7. Secure data synchronization across multiple Mobile Devices between different Device Owners (e.g. colleagues) or across multiple Mobile Devices with the same Device Owner.
8. Presence detection and reporting (publish/subscribe) for End Users and Mobile Devices.
9. Policy-based mitigation of Mobile Device loss/theft (e.g., remote wipe or SED key reset)
10. Cryptographic algorithm agility in security software and hardware.
11. Cryptographic support for host-based security mechanisms (e.g., data-at-rest via TPM or data-in-use via homomorphic encryption) or network security protocols (e.g., data-in-transit via IPSec or TLS).
12. Mechanisms to deal with multiple Enterprise data sensitivity levels/domains (e.g., classification levels) on a single Mobile Device.

8. Trust Assertions

This section discusses trust assertions describing trust relationships between key actors in the TMS use cases defined in this document. Any trust assertion can be made without underlying hardware support, but hardware-based trust assertions can increase confidence in the correctness of implementation and integrity of actors and cooperating systems. See TCG TMI WG Trust Assessment Framework [18] for detailed discussion and guidance.

8.1 Overview of Trust Assertions

In this document, a trust assertion is defined as:

- A recommended method for constructing the assertion
- A set of attributes (claims) regarding the state of an actor or system that may include provenance (time of collection, identity of collector, etc.) to assist in verification
- An optional set of attributes (evidence) that can be used in verification of the accuracy of a given trust assertion

A trust assertion can be used by a Relying Party to make access control decisions. When the set of attribute values are verified independently and/or through a chain of trust, the trust assertion can be safely used in a policy decision process.

Mobile Devices can use trust assertions to describe the attributes of a subject, for example firmware state, OS state, file encryption status, microphone status, etc. A Relying Party can receive trust assertions from a Mobile Device and decide if the Mobile Device is in compliance with a particular set of integrity, confidentiality, availability, or other policies.

8.2 Building Blocks for Trust Assertions

The following capabilities are prerequisites for establishing the validity of trust assertions.

- Roots of Trust: Each Root of Trust (RoT) possesses a certain level of immutability so that the Device Owner or Service Provider can be confident that no matter what state the Mobile Device is in, a RoT has not been affected.
- Transitive Trust Chain: Assertions start from RoTs and work their way up the software stack and across various Mobile Device use case execution contexts based on a transitive trust chain. A context is the operating environment for the End User's or Service Provider's data and applications.
- Continuous Monitoring of Device or Execution Context: There ought to be a way to periodically re-affirm that the device's (and specific execution context) state has not been compromised - the device must be able to make certain non-repudiable trust assertions about itself to the End User, Communication Carrier, or other applicable Actors.
- Policy Flexibility: In some scenarios, the End User or Service Provider may want explicit assertions to be made about specific execution contexts. Each assertion may need to have enough granularity and/or be composed hierarchically to form new assertions. Gradations of the trustworthiness of assertions may need to be supported.

- Local and Remote Trust Assertion Reporting: Devices should possess the ability to make trust assertions both locally (such as between the End User and Service Provider execution contexts) and remotely (such as to Network Infrastructure elements or Service Providers).
- Life Cycle Trust Assertions: The Mobile Device depends on trust assertions established and maintained over its life cycle; and it is essential for the device to be initially examined, configured, provisioned and affirmed as trusted by the Device Manufacturer and other stakeholders of the device.

For mobile platforms, there may be several Roots of Trust involved in creating, maintaining, verifying, and reporting assertions. These Roots of Trust are enumerated and defined in Draft NIST Special Publication 800-164 and described in more detail in the TPM 2.0 Mobile Reference Architecture [17]. Roots of Trust can be implemented as a combination of hardware and software to provide the best balance of cost of hardware against the security provided

The following sections describe in more detail how these building blocks are applied for Mobile Device use case trust assertions.

8.3 End User or Device to Service Provider

Trust assertions should be made by the End User and/or Mobile Device to the Service Provider or Communications Carrier to ensure that the Mobile Device identity and Mobile Device integrity state provide a reasonable basis for network access control decisions. The appropriate content of the trust assertions depends on the type of access requested. An email application may require only a user name and password; whereas, an Enterprise login may require a second End User authentication factor as well as Mobile Device authentication.

Trust assertions from the End User and Mobile Device to a Service Provider or Communications Carrier can include:

- Device Identity – An assertion regarding the Mobile Device identity can be useful for a Mobile Device policy decision by the Service Provider. This assertion could use PKI mechanisms such as possession of a Mobile Device private key to prove authenticity of the Mobile Device identity.
- Device State – An assertion of Mobile Device state (or the state of a subset of components of the Mobile Device) can be useful for an access control decision by the Service Provider. For example, an assertion may indicate that the Mobile Device has current OS patches and malware protection. For Mobile Devices with isolated execution environments, an additional Mobile Device state trust assertion may be used to verify the integrity of that isolated execution environment.
- Secure Storage – The Mobile Device may assert its ability to protect data owned by the Service Provider while it is stored on the Mobile Device in a protected location (e.g., by using a TCG SED). This protection could involve cryptographic keys generated by the Mobile Device itself or keys provisioned by the Device Manufacturer, Service Provider, or other remote entity. A Service Provider agent could be installed on the Mobile Device to monitor integrity state and operations on the Service Provider data.

- End User Identity – The Mobile Device may assert the End User identity and it may include multiple factors such as:
    - A password and/or PIN
    - One or more biometric credentials or tokens
    - Evidence of possession of a physical identification mechanism such as a UICC in the Mobile Device

8.4 Service Provider to Device or End User

Trust assertions should be made by the Service Provider or Communications Carrier to the Mobile Device, End User, or Service Provider-installed agents to ensure that the device is connecting to the correct Service Provider network, and to prevent man in the middle or other remote attacks.

Trust assertions from a Service Provider to a Mobile Device or End User can include:

- Network Identity and Authenticity – The Service Provider network should authenticate itself to the connecting device, for example, using a PKI certificate.
- State of Installed Service Provider Software – Any software installed by the Service Provider to facilitate Mobile Device deployment, for example VPN or MDM software, should verify its state to the device.
- Monitoring Software and End User Privacy – Any software installed by the Service Provider to monitor Service Provider data and application download activity should verify its integrity to the End User.

8.5 Security Infrastructure to Service Provider

Trust assertions that verify the integrity and trustworthiness of security infrastructure elements should be made by the Service Provider to the Mobile Device to provide a secure network execution context for the mobile applications. TCG technologies, other open standard security technologies, and vendor proprietary technologies can be used to attest to the integrity of security infrastructure elements. These trust assertions from security infrastructure elements include:

- Name Services – Trust assertions should be made to the Service Provider by the Name Services (e.g., DNS) to verify their identity and run-time integrity.
- Discovery Services – Trust assertions should be made to the Service Provider by the Discovery Services (e.g., DNS-SD) to verify their identity and run-time integrity.
- Directory Services – Trust assertions should be made to the Service Provider by the Directory Services (e.g., LDAPv3) to verify their identity and run-time integrity.
- Log Services – Trust assertions should be made to the Service Provider by the Log Services (e.g., Syslog over TLS) to verify their identity and run-time integrity.

8.6 Network Access Point to Device or Service Provider

A Network Access Point (NAP) is a device, such as a wireless router, that allows wired or wireless devices to connect to a network.. Depending on the configuration of the NAP the network can be directly owned and managed by the Service Provider or can serve as a gateway to access the Service Provider network externally.

Trust Assertions from an NAP to a Mobile Device can include:

- NAP and Network Identity and Authenticity – The NAP should provide identification information about the NAP itself and the associated network to the Mobile Device. This could be simply a string identifying a NAP in a coffee shop that is providing network access or could be a PKI-based credential for use by an Enterprise Service Provider.
- Mobile Device Access Privileges – The NAP can evaluate the posture (health and configuration) of the Mobile Device and send the resulting access permissions to the Mobile Device at the time of network attachment.

Trust Assertions from an NAP to a Service Provider can include:

- NAP Identity and Authenticity – The NAP should provide identification information about the AP itself to the Service Provider. This could be simply a string identifying the NAP in a coffee shop that is providing network access or could be a PKI-based credential for use by an Enterprise Service Provider.
- NAP Geographic Location – The NAP should provide geographic location information to the Service Provider, which can influence access control decisions by the Service Provider.

9. Solution Approaches

Any Mobile Device security solution for Enterprise, Financial, NFV, or other domain-specific use cases depends on the following critical elements:

1. A comprehensive understanding of the threats that need to be mitigated over the life cycle of components, objects, and interactions involved or addressed by the solution, and an approach designed to tackle these threats,
2. A trust framework that defines the relationship, governance, protocols, and checks between interacting entities on a platform, or across a network, as part of a transaction where confidentiality, integrity and availability of resources must be maintained,
3. Policy evaluation regarding the context of the interaction or access requested,
4. User / device authentication and device compliance checks,
5. Access control enforcement,
6. Protection of data at rest, in use, and in transit,
7. Continuous monitoring or audit of behaviour, vulnerabilities, compliance, and context once the user / device is connected; and, corresponding remedial security actions, and
8. User-friendly security management and administration over the life cycle of components, users, and data involved in the security solution.

In an integrated solution, these elements can be assembled using off-the-shelf components, providing interoperability, scalability, and reusability. The composed solution must also maintain consistent and continuous enforcement of confidentiality, integrity, and availability properties over the life cycle of the transaction, the device, the software, and data used by the associated entities involved.

10. Security Considerations

Mobile Device security considerations are discussed in this section.

10.1 Security Policies

Service Providers all need to establish a security policy for Mobile Device connection to Service Provider networks and Cloud providers, although Service Providers may differ in the details of such policies. Often the user is identified as the greatest threat in Mobile Device access, and the countermeasure of choice is for management to issue policies stating what users must and must not do when connecting to the Service Provider with the user's own device. But regardless of the expected level of compliance of users with Enterprise Mobile Device policies, unless effective technological countermeasures are in place there will likely be policy violations.

NIST Guidelines on Hardware-Rooted Security in Mobile Devices, SP800-164 draft [13], presents a technological view of security policies, threats, and solutions. It acknowledges the interests of Users as well as those of the Service Provider, and advocates security solutions that address the interests of both.

In general, Enterprise Mobile Device policy objectives can be summarized as follows:

- Reduce cost to the Service Provider
- Allow only authenticated user devices to connect to the Service Provider network
- Protect the confidentiality and integrity of the Service Provider's sensitive data
- Reduce cost to the End User
- Minimize the End User's effort to remain in compliance with Mobile Device policies
- Maximize the user's flexibility in using the device for non-Service Provider activities
- Protect the confidentiality and integrity of the user's private data
- Protect the intellectual property of all Actors

10.2 Threats and Mitigations

Because of the variety of communication mechanisms available and increasing use of business applications on Mobile Devices, the security threats to Mobile Devices have evolved to include all the threats applicable to desktops or laptops, plus new threats that are truly unique to Mobile Devices. Therefore, Mobile Devices need to be protected with an even broader set of security techniques than those employed for traditional desktop or laptop operating environments. The latest smartphones are designed to provide broad Internet and network connectivity through varying channels, such as 3G or 4G, Wi-Fi, Bluetooth or a wired connection to a PC. Security threats may occur in different places along these communication channels. A device connected via a wireless connection is at greater risk than a device connected via a wired connection because radio communication significantly simplifies eavesdropping, and the ease of spontaneous connection raises the risk of a "man-in-the-middle" attack (when a hacker configures a laptop, server or Mobile Device to listen in on or modify legitimate communications).

Within this document we use the definition of "threat" and several related terms that appear in the United States NIST Guide for Conducting Risk Assessments, SP800-30r1 [11] (see Glossary).

So, drawing on these definitions, a *threat* is a potential exploitation of a *vulnerability* by which a *threat source* could cause a *security policy* to be violated. And since it is generally infeasible to entirely remove threats, a security enhancement effort instead focuses on either reducing vulnerabilities to threats or reducing the negative effect of threats via the introduction of appropriate countermeasures. This section will consider technical countermeasures, primarily those involving TCG security mechanisms, as opposed to procedural countermeasures such as policy statements, legal action or insurance.

But before countermeasures can be discussed, an appropriate threat model must be selected. There are many ways in which threats in the Mobile Device use case can be categorized. A very good list of information security threats appears in IETF Guidelines for Writing RFC Text on Security Considerations, RFC 3552 [5]. As might be expected, this list focuses on threats to network communications, the forté of the IETF:

Passive Attacks

IETF A	Confidentiality Violations
IETF B	Password Sniffing
IETF C	Offline Cryptographic Attacks

Active Attacks

IETF D	Replay Attacks
IETF E	Message Insertion
IETF F	Message Deletion
IETF G	Message Modification
IETF H	Man-In-The-Middle

Although IETF C, Offline Cryptographic Attacks, is an important issue, we will omit IETF C from our threat model and leave this issue for the consideration of the cryptographic research community. Communications security is highly relevant to the Mobile Device scenario and will be considered in this use case, but the IETF typically does not address threats within the communication endpoint devices themselves. Because we do intend to address threats within the communication endpoints, we have altered this list somewhat by making IETF A more specific, and IETF B, IETF E, IETF F and IETF G more general:

IETF A.1	Eavesdropping on transmitted data
IETF A.2	Unauthorized read access to stored data
IETF B	Unauthorized use of sensitive authentication data
IETF D	Replay Attacks
IETF E	Data Insertion
IETF F	Data Deletion
IETF G	Data Modification

IETF A was split into two threat categories so that we can consider protection mechanisms for transmitted data separately from protection mechanisms for stored data. IETF B was

broadened to include all manner of confidential authentication data (e.g. private keys) and all manner of unauthorized use of that authentication data (e.g. malware posing as the legitimate owner of TPM-protected cryptographic keys). IETF E, IETF F, and IETF G were broadened to include stored data as well as transmitted data.

The Mobile Device use cases consider certain actors, such as the Device Manufacturer, that do not figure prominently in the IETF threat model. In recognition of the concerns of the Device Manufacturer we wish to add the additional threat of device cloning. We include in the concept of "device cloning" both "over-production" of authentic devices by a fabrication facility contracted by a Device Manufacturer, and counterfeit devices that masquerade as an authentic device from the purported Device Manufacturer. In both cases the Device Manufacturer may experience loss of sales revenue. In the latter case the Device Manufacturer may experience loss of reputation because defects in an inferior product may be attributed to the Device Manufacturer.

For a list of vulnerabilities pertinent to the Mobile Device use cases we reference NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise, SP800-124r1 [12]

NIST A	Lack of Physical Security Controls
NIST B	Use of Untrusted Mobile Devices
NIST C	Use of Untrusted Networks
NIST D	Use of Applications Created by Unknown Parties
NIST E	Interaction with Other Systems
NIST F	Use of Untrusted Content
NIST G	Use of Location Services

Of the categories listed above, vulnerability NIST G, while relevant to the user's privacy concerns, is not within the primary scope of this document. To the list of vulnerabilities identified by NIST SP800-124r1 [12], we add "Faulty implementation of authorized hardware and software", in acknowledgment of the important distinction between "trusted mechanisms" and "trustworthy mechanisms". It is all too common to place trust in mechanisms that are inherently flawed in some manner, and hence omit the important consideration of whether trust in these mechanisms is warranted.

So the threat model for the Mobile Device use cases consists of the security policies in Table 10-1, the security vulnerabilities in Table 10-2, and the threat types in Table 10-3.

Table 10-1 Service Provider Security Policies

Security Policy ID	Security Policy Description
P1	Allow only authenticated user devices to connect to the Service Provider network
P2	Protect the confidentiality and integrity of the Enterprise Service Provider's sensitive data

P3	Protect the confidentiality and integrity of the user's private data
P4	Protect the intellectual property of all Actors

Table 10-2 Service Provider Security Vulnerabilities

Vulnerability ID	**Vulnerability Description**
V1	NIST A - Lack of Physical Security Controls
V2	NIST E - Interaction with Other Systems
V3	NIST D - Use of Applications Created by Unknown Parties
V4	NIST F - Use of Untrusted Content
V5	Faulty implementation of authorized hardware and software

Table 10-3 Service Provider Security Threats

Threat ID	**Threat Description**
T1	IETF A.1 - Eavesdropping on transmitted data
T2	IETF A.2 - Unauthorized read access to stored data
T3	IETF B - Unauthorized use of confidential authentication data
T4	IETF D - Replay Attacks
T5	IETF E - Data Insertion
T6	IETF F - Data Deletion
T7	IETF G - Data Modification
T8	TCG - Cloning of the Mobile Device

Table 10-4 lists the security issues that will be considered in these use cases. Note that this list only includes security issues in which a stated security policy might be violated. It does not consider issues such as loss of property value due to theft or damage of the Mobile Device, or loss of utility of the device due to hardware or software malfunction.

Table 10-4 Security Issues Derived from the Service Provider Threat Model

Security Issue	Security Policy	Vulnerability	Threat Source	Threat Types
I1	• P1: Only authenticated devices connect to Service Provider	V1,V2	Attacker attempts to connect using unauthorized device	T1,T3,T4,T5,T6,T7
I2	• P1: Only authenticated devices connect to Service Provider	V1	Attacker attempts to connect using lost or stolen authorized device	T1,T2,T3,T4,T5,T6,T7
I3	• P1: Only authenticated devices connect to Service Provider • P2: Confidentiality and integrity of Service Provider data	V1,V2	Man in the middle attack	T1,T3,T4,T5,T6,T7
I4	• P2: Confidentiality of Service Provider data	V1,V2	Eavesdropping on RF transmission	T1,T3
I5	• P2: Confidentiality and integrity of Service Provider data • P3: Confidentiality and integrity of user data	V3	User installs app that contains malware	T1,T2,T3,T4,T5,T6,T7
I6	• P2: Confidentiality and integrity of Service Provider data • P3: Confidentiality and integrity of user data	V4 & V5	User downloads data that exploits flaw in trusted app	T1,T2,T3,T4,T5,T6,T7
I7	• P4: Intellectual property of the Device Manufacturer	V1, V2 & V5	User, knowingly or unknowingly, attempts to connect to the Service Provider network with a cloned Mobile Device	T8

There are a variety of threat mitigation techniques that can be employed to reduce the security risks occasioned by the security issues listed in Table 10-4.

Threat mitigation techniques are listed in Table 10-5 below.

Table 10-5 Service Provider Threat Mitigation Techniques

Mitigation	Mitigation Techniques
M1	Access Controls
M2	Public Key Signature Code – appropriate public key cryptographic algorithms and proper key management techniques can be employed to protect the integrity and authenticity of sensitive data both during transmission and during storage
M3	Public Key Exchange / Public Key Agreement – appropriate public key cryptographic algorithms and proper key management techniques can be employed to securely establish symmetric encryption keys at the endpoints of an encrypted communications session
M4	Secure Boot – an appropriate secure boot process can be used to ensure the integrity and authenticity of the Mobile Device's initial boot image
M5	Secure Storage – an appropriate secure storage mechanism can be used to protect the confidentiality and integrity of stored data
M6	Secure Transport Protocols
M7	Shared Data Tagging
M8	Attestation – TCG-compliant attestation mechanisms can be used to generate authenticated evidence of the software loaded by the Mobile Device
M9	Password/PIN – appropriately selected and protected password, PINs, or pass phrases can be used to authenticate the user of the Mobile Device
M10	Biometrics – appropriately selected, collected, and managed biometric data can be used to authenticate the user of the Mobile Device
M11	Runtime Integrity Checking – runtime integrity checking mechanisms can be used to ensure that critical portions of the Mobile Device's software and configuration data have not become corrupted since they were loaded
M12	Security Domain Isolation – the state of security-relevant hardware, software and data is protected against corruption or copying by means of hardware or software isolation mechanisms
M13	Provisioning – throughout the device lifecycle the device is provisioned with physical hardware, software, and configuration data of verified provenance
M14	Auditing – security-related events in the lifecycle of individual devices are recorded along with the identities of the actors and the individually accountable hardware associated with the devices

Mitigation	Mitigation Techniques
M15	Secure Data Processing – protection of data-in-use from attack by other processes, operating systems, or hypervisors (e.g., by Homomorphic Encryption)

Table 10-6 indicates which of the mitigation techniques listed above in Table 10-5 are applicable to the various security issues.

Table 10-6 Threat Mitigation Techniques & Applicability to Security Issues

Mitigation Technique #	Threat Mitigation Technique	Applicable to security issues
M1	Access Controls (Mandatory, Discretionary)	I1, I2
M2	Public Key Signature (Integrity, Non-repudiation)	I3, I5, I6
M3	Public Key Exchange / Public Key Agreement (Key Establishment)	I3
M4	Secure Boot (Device State Integrity)	I5
M5	Secure Storage (e.g., Encrypted/Authenticated data-at-rest)	I5, I6
M6	Secure Transport Protocols (e.g., Encrypted/Authenticated data-in-transit: TLS, IPSec)	I3, I5, I6
M7	Shared Data Tagging (e.g., Contact info, PIM)	I4, I5, I6
M8	Attestation (Device Integrity)	I1, I2
M9	Password/PIN (User Authentication)	I1, I2
M10	Biometrics (User Authentication)	I1, I2
M11	Runtime Integrity Checking (Device State Monitoring)	I5, I6
M12	Security Domain Isolation (e.g. virtualization, TEE)	I5, I6
M13	Provisioning	I1, I7
M14	Auditing	I1, I2, I7
M15	Secure Data Processing (e.g., Encrypted data-in-use: Homomorphic Encryption)	I5, I6