REFERENCE

TCG Trusted Mobility Solutions Work Group

Use Cases – Bring Your Own Device (BYOD)

Version 1.0
Revision 1
October 21, 2013

Contact: admin@trustedcomputinggroup.org

TCG Published

TCG

Disclaimer

Acknowledgements

The TCG wishes to thank all those who contributed to this reference document. This document builds on work done in several other working groups in the TCG.

Special thanks to the active and previously active members of the TMS WG who contributed to this document:

John Padgette (TMS co-chair, lead editor)	Accenture
Emily Ratliff	AMD
John Mersh	ARM Ltd
Padma Krishnaswamy	Battelle Memorial Institute
Rafael Montalvo	Cisco Systems
Nicolai Kuntze	Fraunhofer Institute for Secure Information Technology
Carlin Covey (co-editor)	Freescale Semiconductor
Seigo Kotani	Fujitsu Limited
Virginie Galindo	Gemalto NV
Rene Bourquin	General Dynamics C4 Systems
Brooke Burson	General Dynamics C4 Systems
Michael Donovan	Hewlett-Packard
Ira McDonald (TMS co-chair, co-editor)	High North Inc
Florian Schreiner	Infineon
Martin Nicholes	Insyde Software Corp
Sung Lee	Intel Corporation
Alec Brusilovsky (co-editor)	InterDigital Communications, LLC
Kathleen McGill	Johns Hopkins University, Applied Physics Lab
Chris Daly (TMS co-chair, co-editor)	Juniper Networks, Inc
Steve Hanna	Juniper Networks, Inc
Atul Shah	Microsoft
Niall O'Donoghue	Nokia
Janne Uusilehto	Nokia
Hadi Nahari	NVIDIA Corp
Cedric Colnot	NXP Semiconductors
Ken Nicolson	Panasonic
Dick Wilkins	Phoenix Technologies Ltd
Anders Rundgren	PrimeKey Solutions AB
Esteban Yepez	Sandia National Laboratories
Yoni Shternhell	SanDisk Corporation

Ed Adams	Security Innovation
Hervé Sibert	STMicroelectronics
Mohamed Tabet	STMicroelectronics
Anne-Rose Gratadour	Thales Communications & Security
Steven Venema	The Boeing Company
Beth Abramowitz	The MITRE Corporation
Carlton Northern (co-editor)	The MITRE Corporation
Nicolas Ponsini	Trustonic Ltd
Capt. Joshua Dixon	United States Government
Jessica Fitzgerald-McKay	United States Government
Stanley Potter	United States Government

Table of Contents

1. INTRODUCTION

Use cases are narratives that define user needs and contexts of use that meet those needs. Use cases are intended to be sufficiently general in that they are not likely to change in their broad scope over time, can serve as generalizations having potential for a variety of more specific usage scenarios associated with them, and hint at the usefulness and value derived from meeting user needs.

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 the mobile embedded devices' context and ecosystem.

This document has been written to guide subsequent solutions framework development work within the TCG TMS Working Group (TMSWG). It has been written to provide parties within and outside of TCG with a description of the work being carried out by the TMSWG. The usage scenarios outlined herein also provide illustrations for solution developers regarding the types of capabilities that rely on TCG security technology in mobile platforms.

2. TERMINOLOGY AND REFERENCES

2.1 Terms & definitions

Accountability[1]	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[1]	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	The procedure of permitting a remote entity to verify the configuration of the proving device (i.e. what software exactly is running on the proving device).
Availability[1]	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.
BYOD Portal	Supports Device enrollment including End User signature of Enterprise Policy Agreement.
CA	Certificate Authority
CE	Consumer Electronics
Confidentiality[1]	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.
CRM	Customer Relationship Management
Denial of Service[1]	The prevention of authorized access to resources or the delaying of time-critical operations.
DM	Device Manufacturer
HU	Head Unit: the dash-mounted component in a vehicle which provides a unified information interface for the various components of an electronic media system

[1] NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, July 2002

IdP	Identity Provider (in conjunction with OpenID)
IETF	Internet Engineering Task Force
Integrity[1]	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) .
MFS	Mobile Financial Services
MITM	Man In The Middle [an attack vector]
MNO	Mobile Network Operator
NAC	Network Admission Control
NAP	Network Access Point
NFC	Near Field Communication
OpenID	An Open Source technology that enables End Users to use an existing account to sign in to multiple websites without needing to create new passwords.
OTA	Over the air
PKCS#11	One of the family of standards called Public-Key Cryptography Standards (PKCS). PKCS#11 defines a platform-independent API to cryptographic tokens.
POS	Point of sale
Risk[1]	The net mission 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 mission 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. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information
Secure Storage	Persistent data storage location where the confidentiality and integrity of data stored therein can be assured
Security Goals[1]	The five security goals are integrity, availability, confidentiality, accountability, and assurance.
SOC	System on a chip
SSL	Secure Socket Layer

SSO	Single Sign On
Threat[1]	The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
TNC	Trusted Network Connect
Trusted Execution Environment (TEE)	A trusted hardware/software execution space where software can be executed with a high level of trust, separately from other execution spaces where there is less trust. Typically a TEE is a secure execution space that resides in the main processor or a separate processor of the device and guarantees that sensitive data and code within that space is securely stored, processed and protected, with the ability to work independently or complementary to a secure element and the standard device applications.
Vulnerability[1]	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.

Refer to the TCG Glossary of Technical Terms for additional trusted computing terms and definitions http://www.trustedcomputinggroup.org/developers/glossary

2.2 Actors

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

Actor	Description
Application Provider (AP)	An entity generating and/or selling user applications to be executed on the platform (e.g. web browser, plug-ins)
Attacker	A person or organisation trying to circumvent some security policy of one or more of the other Actors (e.g. Device, the Service Provider, the Application Provider, the Network Provider)
Content Provider (CP)	The distributor of intellectual property that requires protection
Device	An entity comprising a mobile platform with a mobile TPM for which attestation data may be provided
Device Manufacturer (DM)	The manufacturer or brand of a Device, typically an Original Equipment Manufacturer (OEM). Also commonly referred to as a Vendor
Device Owner (DO)	The legal owner of the Device. The owner may be an End User (consumer), an IT Administrator for an Enterprise, or some other entity.
End User (EU)	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 data and networks. Besides the End User, the Enterprise is the most common Information Owner with respect to BYOD.
Information Owner (IO)	An entity whose information is stored and/or processed on a device. The Information Owner may be the Device Owner, the End User, an Enterprise, Application Provider, Communication Carrier, or Content Provider.
Communication Carrier (CC)	An entity that provides wireless communications (e.g. Wi-Fi, Cellular) functionality to the Device.
Operating System Provider	The entity that provides and maintains (e.g. patches) an OS on a mobile device. This includes Hypervisor VMM, hence it is possible that multiple OS run on a single device and multiple OS providers associated with a single device. Further, there may be multiple repositories used to maintain a particular OS' components including applications, drivers and libraries.
Service	A network-accessible entity that can provide Devices and/or services to a

Provider (SP)	Device

3. BYOD USE CASE

3.1 Objective and Scope

The concept of bring your own device (BYOD) in the work place refers to an Enterprise policy that allows employees or other individuals; such as partners, contractors and more, to access an Enterprise network through their personal mobile devices. The advantages to both the Enterprise and End Users are obvious:

- The Enterprise does not have the cost of purchasing a device since the End User already has done that.
- The End User has the convenience of carrying only one personalized device that they chose and optimized based on their criteria.

However, BYOD policies may also introduce serious business consequences if the mobile devices are not properly secured. Examples of such issues include:

- A non-compliant BYOD device is introduced to the Enterprise infrastructure and allowed access. Unauthorized or non-business oriented applications that are common on non-compliant devices have the potential to spread malware that affects the integrity of the device and the business data residing upon it. Additionally, the non-compliant BYOD device may not contain any monitoring agents which can detect and/or prevent malware from spreading on the corporate network.
- Data leakage of sensitive corporate IP could occur if content and applications are not protected on the BYOD.
- Corporate information could be lost if the BYOD is stolen or lost.

With BYOD, business and personal data now coexist on the same device. Finding a balance between strict security control and privacy of personal data can be challenging. Overly restrictive or non-selective Enterprise BYOD policies may jeopardize the convenience to End Users or place personal data at risk of being wiped out by an Enterprise security agent running on the mobile device.

The scope of this use case is Enterprise BYOD which focuses on a personal device that may have zero or more existing security policies connecting to an Enterprise network that has its own security policy. Note that there are other related use cases which are outside the scope of this document, including:

- Bring Enterprise-Owned Device (BEOD): Enterprise-owned and issued device being used at the Home/SOHO or elsewhere outside the Enterprise. This is effectively the reverse case of Enterprise BYOD, since the Home network may not have a security policy (e.g. no user authentication to the Home network). Key concern is that Enterprise data is still protected in the Home environment.

- Choose Your Own Device (CYOD): Enterprise offers user a specific set of devices from which to choose. Device Owner could be the End User or Enterprise. For CYOD the lifecycles are different than BYOD, even if Device Owner is the End User.

The objective of this use case is to highlight how technology developed by the TCG and other standards-based technologies can be combined to mitigate some of the security concerns associated with BYOD. The use case presents a holistic view of the BYOD concept including policies, processes, an overall trust framework, and relevant actors' roles throughout the life cycle security management of BYOD devices. Solution frameworks will be provided that are designed to highlight how technology (including TCG building blocks) can be applied to secure end-to-end mobility architectures. This use case is intended to assist Enterprise managers, mobile solution developers, and technology providers in understanding the important role that TCG and other standards-based technology can offer in the BYOD landscape.

3.2 Description

Device makers feature updates and improvements almost weekly to mobile platforms, such as smartphones, tablets, and laptops, resulting in an increasing level of sophistication in their capabilities. In addition, extant mobile devices are enhanced through new applications downloaded by their users. Mobile platform owners would like to leverage this significant, ever-increasing supply of new functionality by using their mobile devices as a single portal for all their computing needs – both personal and work-related. Because of this user interest in "multi-personality" devices, an increasing number of companies support a BYOD program today. In fact, eleven percent of information workers are using tablets to do their jobs, with 26 percent of workers using Android smartphones, and 22 percent using iPhones. While many mobile products are purchased by End Users for BYOD purposes, many are also provided by their employers for the convenience they afford, alongside the instant connectivity it allows the End User to have with the corporate IT data center.

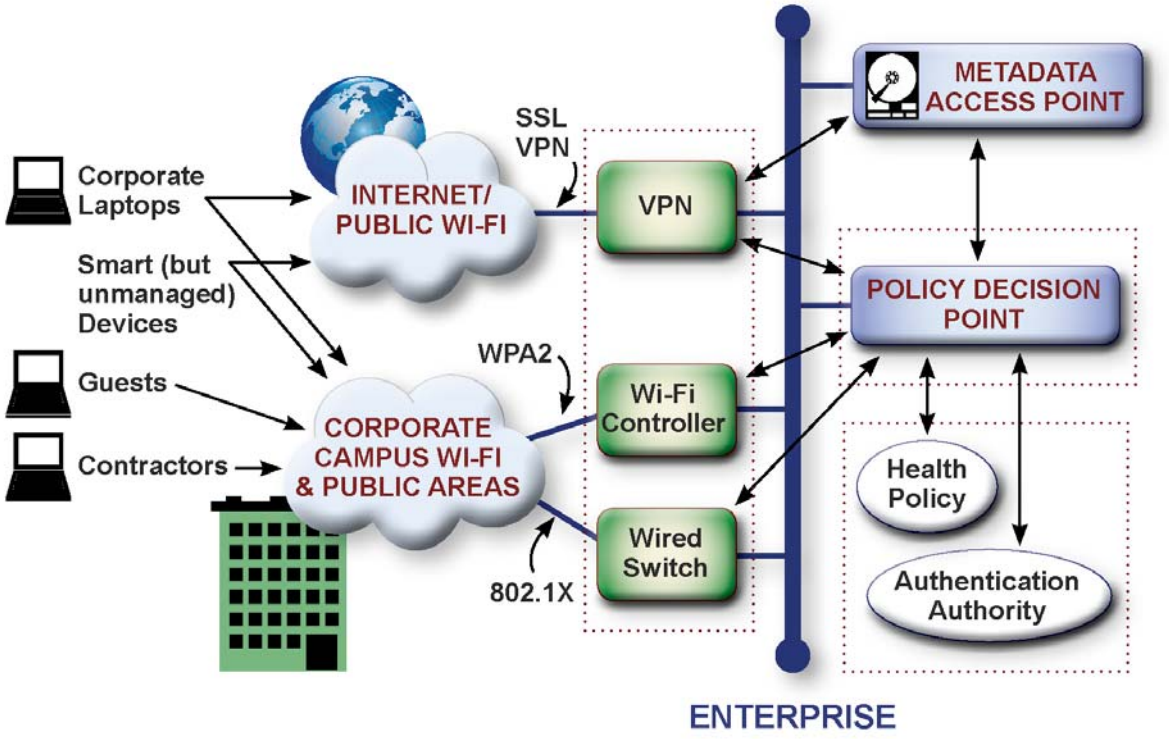

Figure 3.1 BYOD Architecture

Figure 3.1 BYOD Architecture, illustrates the different stakeholders involved in a BYOD approach. This notional solution builds on the premise captured in the TCG Architect's Guide for BYOD Security that escalating the trust in a mobile platform may bring increased Enterprise access. However, BYOD brings with it a major caveat - the device is not Enterprise-owned but is owned by the user and provisioned by several external stakeholders, possibly including the Enterprise itself. This multi-stakeholder approach inherent in BYOD usage adds a degree of difficulty to the challenge of establishing trust.

Figure 3.2 below illustrates how different users are given different levels of access to corporate resources based on their trust level. Guests, with a low level of trust, get virtually no access. Trusted users with trusted devices (such as managed corporate tablets) are given the most access. In between are users at different levels of trust, such as staff with unmanaged devices, or contractors who should have only "need to know" access. The process of transitioning these unmanaged devices to provisioned BYODs is the goal of the BYOD architectural guide.

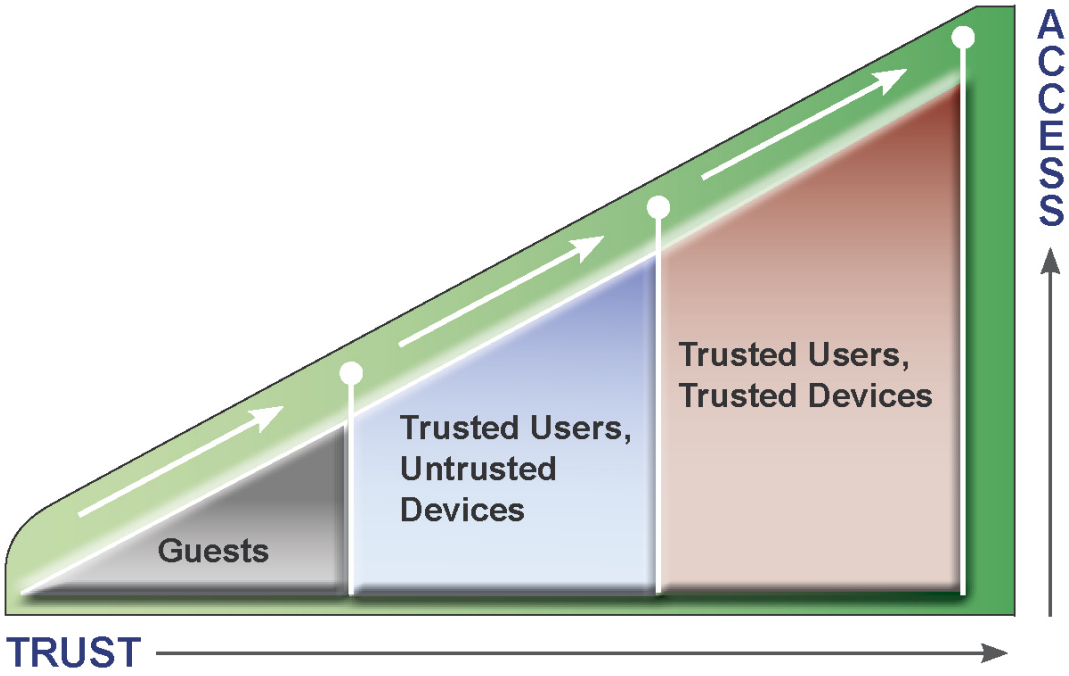

Figure 3.2 Escalating trust brings increased access for BYOD users.

An Enterprise could have fewer or more access types, and different types of access, as fits the needs of the organization. For example, it would be very common to have a moderate access category for contractors, who might have fully compliant devices but who are given a lower level of trust than other trusted Enterprise users. However, this division into three "buckets" is a very good starting point because it shows how to differentiate based on both authentication information and device trust information.

3.3 Benefits for Actors

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

3.3.1 End User

An End User benefits from a securely deployed BYOD implementation as follows:

1. Convenience of use. By combining personal and work devices, an End User can reduce the number of devices they must manage and carry. Additionally, an End User is already familiar with the device operation and there is minimal learning curve associated with it. Further, an End User can execute software and applications of their choice on the device.

2. High availability and productivity of corporate connectivity. The mobility of the device enables a high availability to the corporate data store (email, alerts, applications etc.) which will increase End User productivity.
3. Device protection. It is highly probable that an Enterprise will deploy device protection mechanisms such as malware detection applications etc. which provide a greater level of protection than an End User might otherwise employ.
4. Privacy/integrity of personal data. An End User will have confidence that their personal data will not be viewed, erased, or corrupted by other Information Owners on a Device. For example, an End User can detach from an Enterprise at any time without losing personal data.

3.3.2 Device Owner

In this BYOD Use Case an End User is a Device Owner, and is responsible for purchase, management and upkeep of the device and has the same benefits as an End User (above.)

3.3.3 Device Manufacturer

A Device Manufacturer provides a BYOD capable mobile Device. A Device Manufacturer benefits from a securely deployed BYOD implementation as follows:

1. By satisfying the security needs demanded by consumers/partners, a Device Manufacturer can capitalize on the growing revenue potential of the purchase/use of their mobile devices as well as value-added application bundles.

3.3.4 Information Owner

An Information Owner is the ultimate legal right holder to a piece of data. There will typically be multiple Information Owners for any given platform. These will include an Enterprise, an End User, clients or customers of an Enterprise, and intellectual property holders of licensed content and applications.

An Information Owner benefits from a securely deployed BYOD implementation as follows:

1. An Information Owner can trust the Device to access its services and process data.
2. An Information Owner can trust the data on the Device in terms of confidentiality, integrity and availability.
3. An Information Owner may terminate access to their information through specific controls.

3.3.5 Enterprise

In addition to Information Owner benefits, an Enterprise benefits from a securely deployed BYOD (vs. Enterprise-issued device) implementation as follows:

1. Cost of acquisition. An End User is responsible for the purchase and maintenance of the mobile device relieving an Enterprise of the associated up front acquisition costs, as well as recurring monthly costs.

2. Improved productivity. An End User may be already familiar with the device operation and there is minimal learning curve associated with it. This may also reduce training costs.
3. End User availability to the Enterprise. By utilizing an End User's personal device, which is also used outside the work environment and work hours, there will be an increased availability of an End User when required for emergency work or other reasons.

3.3.6 Service Providers

Service Providers furnish the services and equipment that enable the BYOD use case. Service Providers include Communications Carriers, Application and Content Providers, Operating System Providers and Device Manufacturers.

A Service Provider benefits from a securely deployed BYOD implementation as follows:

1. By satisfying the security needs demanded by consumers/partners, a Service Provider can capitalize on the growing revenue potential of the purchase/use of their services.

3.3.7 Communication Carrier

A Communication Carrier provides network access (cellular or other) and connectivity between a mobile device and an Enterprise network. Typically, the Communication Carrier is the vendor of the mobile device, and will be responsible for providing patches and updates to the device.

A Communication Carrier benefits from a securely deployed BYOD implementation as follows:

1. A Communication Carrier can capitalize on the growing revenue potential of the purchase/use of their services, including new services such as BYOD service enablement, integrated policy management, and increased security.

3.3.8 Application/Content Provider

An Application Provider furnishes the applications to be run on the mobile device. A Content Provider serves the data to be consumed on the device (e.g., email, music, video). This data may be commercially provided intellectual property. In some instances, an Enterprise may be an Application or Content Provider.

An Application/Content Provider benefits from a securely deployed BYOD implementation as follows:

1. An Application/Content Provider can capitalize on the growing revenue potential of value-added application bundles.

3.3.9 Operating System Provider

An Operating System Provider furnishes the operating system(s) to support secure BYOD operations. An Operating System Provider is responsible for creating patches and updates to the operating system.

An Operating System Provider benefits from a securely deployed BYOD implementation as follows:

1. An Operating System Provider can capitalize on the growing revenue potential of value-added application bundles and BYOD-capable Operating Systems.

3.4 Pre-conditions

The pre-conditions for the BYOD Use Case are described below.

- The designed solution follows best practices for security (confidentiality, integrity, authentication, non-repudiation and availability).
- The designed solution can resist both passive and active attacks.
- The mobile application is easy to use (good usability).
- The solution components are designed to leverage TCG technologies such as mobile TPM and other standards-based technologies.

3.5 Post-conditions

The post-conditions for the BYOD Use Case result in either Success or Failure.

3.5.1 Success End Condition

A successful BYOD Use Case implementation leveraging current and future standards-based security technologies assists actors in realizing the benefits listed in Section 3.3.

3.5.2 Failure End Condition

A BYOD Use Case implementation without appropriate provisioning and risk mitigation from current and future standards-based security technologies prevents actors from realizing one or more of the benefits listed in Section 3.3.

Possible BYOD Use Case failure end conditions may cause:

- End User data loss or theft
- Compliant End User cannot connect to Enterprise (false positive)
- End User decreased functionality of device
- Information Owner data loss or theft
- Information Owner cannot control access to its data
- Enterprise has increased IT support costs without productivity/security gain

3.6 Lifecycle Scenarios

Lifecycles for the principal actors of this Use Case are described and discussed.

3.6.1 Device Manufacturer Lifecycle

Assumptions:

1. Device Manufacturer installs a mobile TPM (hosted in a TEE), hypervisor, SIM/UICC or other isolated trusted environment - and other standards-based technology.
2. Device Manufacturer and/or separate remote authority provisions the mobile TPM and installs pre-loaded applications that use the mobile TPM.
3. Device Manufacturer verifies and audits 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 3-1 Device Manufacturer Lifecycle Activities

Lifecycle stage	Activities undertaken during this stage
Manufacture / Initialization	• Mobile TPM, TNC, SED and other standards-based technologies suitable for mobile systems provisioning by Device Manufacturer (DM), Communication Carrier (CC), or separate remote authority. • The Contract Manufacturer (or DM itself) assembles hardware and software from multiple suppliers and delivers device to DM. Delivered device includes provisioned mobile TPM (or other standards-based technology) with Device Manufacturer's keys. • Keys may be delivered remotely, assuming pre-placed keys (or similar) were provisioned during mobile TPM installation.
Provisioning / Enrollment	• Scope is Device (vs. Application) Provisioning in this DM lifecycle stage. • Device Provisioning may be performed by Contract Manufacturer prior to delivery to DM (see above).

	• Otherwise, Device Provisioning must be performed by another actor, such as Communication Carrier or DM. • DM provides a strongly authenticated, trusted Device Identity for attestation and endpoint health assessment.
Use / Customization	• DM, OS Provider(s) or Enterprise provide Application and associated Policy provisioning. • DM or OS Provider(s) provides Application and associated Policy updates. • DM or OS Provider verifies Application update integrity.
Service Update	• DM 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 DM, de-provisioning of keys (Endorsement Keys, Storage Keys), user/Enterprise data wipe from memory. • Take ownership away from Communication Carrier. E.g., 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 DM (e.g. to avoid per-device license fees).

3.6.2 Communication Carrier Lifecycle

Assumptions:

1. The Communication Carrier or separate remote authority provisions the mobile TPM.
2. The Communication Carrier installs all standard applications.

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

Table 3-2 Communication Carrier Lifecycle Activities

Lifecycle stage	**Activities undertaken during this stage**
Manufacture /	N/A

Initialization	
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 mobile TPM based on delegation from the Device Manufacturer (DM). • Communication Carrier enrolls Device Owner (DO) 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 mobile TPM. • Communication Carrier could verify App integrity • Power management issues (suspend/resume)
Service Update	• Communication Carrier may distribute OS or driver patches 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.

3.6.3 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 (DO).

Table 3-3 Device Owner Lifecycle Activities

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 TDM 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 DM, recycle)

3.6.4 Enterprise BYOD Lifecycle

Assumptions:

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

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

Table 3-4 Enterprise BYOD Lifecycle Activities

Lifecycle stage	**Activities undertaken during this stage**
Manufacture / Initialization	• N/A – precondition 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 • Enterprise BYOD Portal provides Enterprise MDM Client, VPN client, browser or other policy-enabled software for download by the Device Owner. • Enterprise BYOD 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 DM, recycle)

3.6.5 Lifecycle Solution Needs

The above lifecycles imply the following solution needs for BYOD deployments. Further solution needs are discussed in Section 3.7 below, ”Trust Assertions”.

1. Need for interoperable, standards-based Policy statements that support vendor and/or site-specific extensions.
2. Need for logical and secure separation of personal and Enterprise data/apps for storage (e.g., logical LBA ranges on SEDs), execution (e.g., TEE hypervisor, etc.), and verification of device integrity

3. Need for authentication infra-structure to verify Device identity. e.g., PKI infrastructure and public certificate servers, etc.
4. Need for interoperable standards-based Mobile Device Management (MDM) solutions
5. Need a means for resolution/reconciliation of multiple – possibly conflicting - MDM policies on a particular Device. (NIST SP 800-164 PEnE)
6. Need for correlation of User Identities across multiple Devices, as well as User Roles, Certificates, Keys. There may be a hierarchy of Users and Devices that need to be managed.
7. Need for secure data synchronization across multiple Devices between different Device Owners (e.g. colleagues) or across multiple Devices with the same Device Owner.
8. Need for presence detection and reporting (publish/subscribe) (e.g. IF-MAP servers)
9. Need for policy-based mitigation of Device loss/theft (e.g., remote wipe or SED key reset)
10. Need for cryptographic algorithm agility in security software/hardware (e.g. TSS, TNC, TPM, VPN).
11. Need for TPM cryptographic support for host-based security mechanisms (e.g., data-at-rest) or network security protocols (e.g. IPSec, 3GPP).
12. Need for mechanisms to deal with multiple Enterprise data sensitivity levels/domains (e.g., classification levels) on a Device.

NOTE: See NIST SP 800-164 for Issues and Integrity guidelines

3.7 Trust Assertions

This section outlines a set of trust assertions which are utilized in establishing trust between all of the actors involved in a BYOD deployment. All of these assertions are defined without the requirement for an underlying support in hardware but it will be highlighted how a hardware or firmware-based trust assertion allows for a greater confidence in the assertion itself.

3.7.1 Trust Assertion Overview.

For the purposes of this document, an assertion is defined as follows:

- Consists of a set of attributes or claims regarding the state properties of an object or actor
- Has a “binding” to the object or actor
- May describe or identify the method for constructing the assertion, including the quality of the method
- May define any authorities or other assertions used to back-up / verify the claims about the attributes.

An assertion is used by a policy decision point in making confidentiality, integrity, and availability assessments concerning the object or actor. These assessments can be used for policy decisions that determine the degree of access to an Enterprise's resources. An assertion itself does not guarantee trustworthiness. Only when the attribute is validated independently or its existence and properties can be provably established through a chain of trust can the assertion itself be considered trustworthy in the decision process – a trust assertion.

Mobile devices may use assertions to represent the state of an object, such as firmware, as either verified or unverified, the state of an OS as either validated or not, the state of file encryption as either on or off, the state of the microphone as either on or off, etc. A Policy Decision Point receives assertions of a mobile platform [or of a virtual container on a mobile platform] and determines whether or not the platform [or container] is in compliance with a particular integrity, confidentiality, or availability policy.

Trust assertions provide a reliable way for the Enterprise to detect if the Device Owner's activities have unknowingly altered the state of the device in such a way so as to put the Enterprise's data at risk; or, to evaluate the degree of access allowed to a user of a BYOD.

3.7.2 Trust Assertions for BYOD

The BYOD concept is only feasible and useful to the Enterprise if the basic Enterprise security policies can be maintained for Enterprise data and applications upon deployment of BYOD devices. This stipulation implies one of the following conditions:

- The BYOD device is Enterprise-owned and managed by the Enterprise, and the End User's personal use does not compromise the Enterprise security posture for the device. This condition provides the Enterprise with some guarantee of the integrity of the system while it is being used. Even for Enterprise-managed mobile devices, the trustworthiness of the device needs to be assessable at any time since the device is susceptible to attacks when it operates outside the corporate boundary – i.e., when the user employs the device for personal use.
- The BYOD device is owned by the End User but it has an installed security domain which is configured to operate under the same security constraints to which Enterprise-owned mobile devices are provisioned. In some cases, Device Owners may regard this level of control as intrusive. A resident Policy Agent on the BYOD Device should resolve conflicts between Policies in multiple security domains (e.g., Turn off Bluetooth or NFC radios).
- The BYOD device is owned by the End User but fine-grained controls are imposed on the ability of the BYOD device and user to access Enterprise resources.

In all cases, the level of trust assigned to a BYOD device by an Enterprise needs to be policy-driven and based on: 1) an assessment the Enterprise will make on the integrity state of the connecting device; 2) the strength of authentication mechanisms used to establish the identity of the device and the use; 3) other environmental context factors that are part of Enterprise policies, e.g., location. Note that in addition to the desire by the Enterprise to protect against attacks or loss of data, the End User of a BYOD also requires that their personal information is not compromised or lost inadvertently by some action taken by the Enterprise. For example, an Enterprise may install a VPN client to establish a secure channel between the 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

needs to feel assured that this DLP mechanism is not used to monitor personal internet usage or compromise their privacy. Additionally, the End User needs assurances that a remote lock or wipe of the Enterprise data contained on the BYOD will not lock or wipe personal usage and data on the device (typically enforced by the MDM Client).

3.7.3 Building Blocks for Trust Assertions

Assertions that are trustworthy leverage certain capabilities built into the BYOD or are provided remotely by the Enterprise. These capabilities may also have interdependencies or be constructed in a trust assertion hierarchy. The following capabilities are prerequisites for establishing trust assertions.

- Roots of Trust: Each Root of Trust (RoT) possesses a certain level of immutability so that the Device Owner or Enterprise 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 BYOD execution contexts based on a transitive trust chain. A context is the operating environment for the End User's or Enterprise's data and applications.
- Continuous Monitoring of Device or Execution Context: There needs 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 Enterprise, End User, Communication Carrier or other applicable Actors.
- Policy Flexibility: In some scenarios, the End User or Enterprise may want explicit assertions to be made about specific execution contexts. Assertions 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 Enterprise execution contexts) and remotely (such as to Network Infrastructure elements or Service Providers).
- Life Cycle Trust Assertions: The mobile device needs 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. 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 BYOD trust assertions.

3.7.4 Trust Assertions from End User and Device to Enterprise and Communication Carrier

A set of trust assertions that establish the End User and device identity, as well as the integrity state of the BYOD device, provides a reasonable baseline by which a policy decision point can evaluate the level of network access to be granted by the Enterprise. The robustness of the assertion required is dependent on the type of access requested. For example, a web-based email application may only require a user name and password to grant access; whereas, a domain login may require a secondary authentication factor, and potentially authentication of the device.

The top level trust assertions from the End User and BYOD device to an Enterprise include:

- Device Identity and Authenticity – A strong assertion regarding the identity of the device is instrumental in allowing a meaningful BYOD policy by the Enterprise. This assertion could involve the use of PKI mechanisms and the possession of a device-owned private key (potentially provisioned by the Enterprise) to prove authenticity of the device identity. The stronger that this key is protected by the device, the more trust which can be placed on the assertion itself.
- Device State – An assertion of a device state (or state of a subset of components of the device) allows the Enterprise to enforce an access policy based on trust that the asserted state of the device is true. For example, this assertion may indicate that the device is up-to-date with respect to OS patches and malware protection updates. For mobile devices with certified isolated execution environments, such a device state trust assertion may indicate that the integrity of an isolated Trusted Execution Environment (TEE) has been verified as true.
- Secure Storage – The BYOD device should assert its ability to protect Enterprise-owned data while it is stored on the device in a secure storage element (e.g., best practice is to use a TCG SED). This data could be cached emails or other sensitive information. This protection will involve cryptographic keys either unique to the device itself or provisioned to the device by the Enterprise. The stronger that this key is protected by the device, then the more trust which can be placed on the assertion itself. This assertion may also require that Enterprise software required to monitor the operations on the Enterprise data be installed and that the integrity state of the software can be measured and verified.
- User Identity and Authenticity[2] – This assertion is made about the End User identity and it may involve composed assertions – e.g., something I know, something I have, something I am. Generally, proof of identity requires proving the ownership of the identification credential. This credential could be either (or a combination of)
  - A password or pass-phrase
  - Biometric credential
  - Possession of a physical identification mechanism such as
    - Smart card, e.g., UICC in a mobile device

[2] See NIST Special Publication 800-63-1, *Electronic Authentication Guideline*

- OTP token

3.7.5 Trust Assertions from Enterprise to Device and End User

It is imperative that trust assertions are made from the Enterprise network to the BYOD device, End User, or Enterprise-installed agents to ensure that system is connecting to the correct Enterprise network, and to prevent man in the middle or other remote attacks. These assertions are defined as follows:

- Network Identity and Authenticity – The Enterprise network needs to identify itself to the connecting device. This will typically involve the use of PKI mechanisms and the possession of an Enterprise owned private key with an associated certificate. The stronger that this key is protected by the Enterprise then the more trust which can be implied from the assertion itself.
- State of Installed Enterprise Software – Any software installed by the Enterprise to facilitate the BYOD deployment, such as VPN and mobile device management (MDM) software, needs to assert its identity and authenticity to the device.
- Monitoring Software and End User Privacy – Any software installed by the Enterprise to monitor Enterprise data and application download activity in order to implement a data loss prevention (DLP) mechanism needs to assert its ability to prevent compromising the privacy of the End User during the execution of Enterprise applications.

3.7.6 Trust Assertions within the Enterprise

The Enterprise itself needs to put in place a set of assertions from which trust in the BYOD implementation can be derived. The PEP and PDP are elements of TCG technology that may be used within the Enterprise for enforcing access policy. They consolidate trust assertions from the BYOD device and End User to determine the network access privileges to grant. As such certain trust assertions are implied between these two network elements.

- Add MAP, Directory Services, Log Servers (e.g., Syslog)
    - E.g. MAP to PEP, MDM (introduce concept)
- PEP Identity and Authenticity – The PEP is the point of attachment of the BYOD to the Enterprise network. Although the PEP may not be directly connected to the BYOD device, it is responsible for granting or denying the device's access to the Enterprise network based on:
    - The Enterprise policy defined by the PDP
    - The validation of any trust assertions mandated by the access policy.

  The PEP itself needs to assert its identity to the Enterprise network to ensure it can be trusted to enforce the Enterprise policy determined by the PDP. This will typically involve the use of PKI mechanisms and the possession of a device owned private key (potentially provisioned by the Enterprise). The stronger the key is protected by the device then the more trust which can be implied from the assertion itself.
- PDP Identity and Authenticity – The Policy Decision Point implements the Enterprise network access control policy. It needs to be strongly identified and authenticated to the PEP.

3.7.7 Trust Assertions for Network Access Point

A Network Access Point (AP) is considered to be an edge network device providing direct connectivity to a network for the BYOD. Depending on the class of the AP this network can be directly owned and managed by the Enterprise or may just serve as a gateway from which to access the Enterprise network externally.

Trust Assertions by the AP to the BYOD Device:

- AP and associated Network identification – The AP needs to identify itself to the connecting device. This may be as weak as a string identifying the coffee store providing access or may involve the use of PKI mechanisms for Enterprise managed systems. The stronger that this ID is protected then the more trust which can be implied from the assertion itself.
- BYOD AP access privileges – This asserts the permission of the endpoint to access the network through the AP.

Trust Assertions by the AP to the Enterprise:

- AP identification – This assertion identifies the AP itself to an Enterprise. This may be as weak as a string identifying the coffee store providing access or may involve the use of PKI mechanisms for remotely managed units (such as a WiFi hotspot provided by an Enterprise managed cellular device). The stronger that this ID is protected then the more trust which can be implied from the assertion itself and subsequent assertions about the BYOD connection.
- AP Location. The location of the AP implicitly can be used to validate the location assertion of the Enterprise device.

3.8 Security Policies

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

NIST has recently solicited comments on a draft document titled Special Publication 800-164 "Guidelines on Hardware-Rooted Security in Mobile Devices". This document presents a technological view of security policies, threats, and solutions. It acknowledges the interests of the users as well as those of the Enterprise, and advocates security solutions that address the interests of both.

In general BYOD policy objectives can be summarized as follows:

- Reduce cost to the Enterprise
- Allow only authenticated user devices to connect to the Enterprise network
- Protect the confidentiality and integrity of the Enterprise's sensitive data

- Reduce cost to the End User
- Minimize the End User's effort to remain in compliance with BYOD policies
- Maximize the user's flexibility in using the device for non-Enterprise activities
- Protect the confidentiality and integrity of the user's private data
- Protect the intellectual property of all Actors

3.9 Identified Threats

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 will use the definition of "threat", and several related terms, that appear in the United States National Institute of Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*:

- "Threat - The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." [3]

- "Vulnerability - 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."

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[4] must be selected. There are many ways in which threats in the BYOD use case can be categorized.

[3] NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002

[4] IETF RFC 3552, *Guidelines for Writing RFC Text on Security Considerations*

A very good list of information security threats appears in IETF RFC 3552, *Guidelines for Writing RFC Text on Security Considerations*. 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 BYOD 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, E, F and 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, F and G] were broadened to include stored data as well as transmitted data.

This BYOD use case considers 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 that are pertinent to the BYOD use case we can turn to NIST *Guidelines for Managing and Securing Mobile Devices in the Enterprise*[5]*:*

[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 scope of the BYOD use case. To the list of vulnerabilites identified by NIST, we added "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.

We earlier made the observation that a *threat* is a potential exploitation of a *vulnerability* by which a *threat source* could cause a security policy to be violated. Having identified the threats that we consider in scope, we now consider how threat sources might interact with vulnerabilities to yield the different threats in our threat model. Of the BYOD policy objectives listed in section **Error! Reference source not found.**, we will consider the objectives that are security-related.

So the threat model for the BYOD use case consists of the security policies in Table 3-5, the vulnerabilities in Table 3-6, and the threat types in Table 3-7.

Table 3-5 BYOD Security Policies

Security Policy ID	Security Policy Description
P1-AUTHENUSERS	Allow only authenticated user devices to connect to the Enterprise network
P2-ENTDATA	Protect the confidentiality and integrity of the Enterprise's sensitive data
P3-PERSDATA	Protect the confidentiality and integrity of the user's private data
P4-INTELPROP	Protect the intellectual property of all Actors

Table 3-6 BYOD Security Vulnerabilities

[5] NIST Special Publication 800-124, Revision 1 (Draft), July 2012, *Guidelines for Managing and Securing Mobile Devices in the Enterprise*

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

Table 3-7 BYOD Security Threats

Threat ID	Threat Description
T1-EAVES	[IETF A.1] Eavesdropping on transmitted data
T2-UNAUTHREAD	[IETF A.2] Unauthorized read access to stored data
T3-UNAUTHUSE	[IETF B] Unauthorized use of confidential authentication data
T4-REPLAY	[IETF D] Replay Attacks
T5-INSERT	[IETF E] Data Insertion
T6-DELETE	[IETF F] Data Deletion
T7-MODIFY	[IETF G] Data Modification
T8-CLONE	Cloning of the mobile device

The following table lists the security issues that will be considered in this use case. Note that this list includes only 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 3-8 Security issues derived from the BYOD threat model

Security Issue	Security Policy	Vulnerability	Threat Source	Threat Types
I1	• P1: Only authenticated devices connect to Enterprise network	V1,V2	Attacker attempts to connect using unauthorized device	T1,T3,T4,T5,T6,T7

Security Issue	Security Policy	Vulnerability	Threat Source	Threat Types
I2	• P1: Only authenticated devices connect to Enterprise network	V1	Attacker attempts to connect using lost or stolen authorized[6] device	T1,T2,T3,T4,T5,T6,T7
I3	• P1: Only authenticated devices connect to Enterprise network • P2: Confidentiality and integrity of Enterprise data	V1,V2	Man in the middle attack	T1,T3,T4,T5,T6,T7
I4	• P2: Confidentiality of Enterprise data	V1,V2	Eavesdropping on RF transmission	T1,T3
I5	• P2: Confidentiality and integrity of Enterprise 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 Enterprise 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 Enterprise 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 3-8.

Threat mitigation techniques are listed in Table 3-9 below.

Table 3-9 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

[6] We will assume that an authenticated device is an authorized device in the hands of an authorized user.

Mitigation	Mitigation Techniques
	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 phrase 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 – appropriate 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

Table 3-10 indicates which of the mitigation techniques listed above are applicable to the various security issues.

Table 3-10 Threat mitigation techniques and their applicability to security issues

Mitigation Technique #	Threat Mitigation Technique	Applicable to security issues
M1-ACL	Access Controls (Mandatory, Discretionary)	I1, I2
M2-PUBKEYSIGN	Public Key Signature (Integrity, Non-repudiation)	I3, I5, I6
M3-PUBKEYXCH	Public Key Exchange / Public Key Agreement (Key Establishment)	I3
M4-SECBOOT	Secure Boot (Device State Integrity)	I5
M5-SECSTORE	Secure Storage (e.g., Encrypted/Authenticated Data-at-rest)	I5, I6
M6-SECTRAN	Secure Transport Protocols (e.g., Encrypted/Authenticated Data-in-transit: TLS, IPSec)	I3, I5, I6
M7-DATATAG	Shared Data Tagging (e.g., Contact info, PIM)	I4, I5, I6
M8-ATTEST	Attestation (Device Integrity)	I1, I2
M9-PASSPIN	Password/PIN (User Authentication)	I1, I2
M10-BIO	Biometrics (User Authentication)	I1, I2
M11-INTEGCHECK	Runtime Integrity Checking (Device State Monitoring)	I5, I6
M12-SDISO	Security Domain Isolation (e.g. virtualization, TEE)	I5, I6
M13_PROVIS	Provisioning	I1, I7
M14-AUDIT	Auditing	I1, I2, I7

3.10 Use Case Solution Approaches

Any Enterprise security solution 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 a unified 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.

Table 3-11 lists specific solution components and related security components to address the basic blocking and tackling for security controls on a BYOD; including: authentication, access control, continuous monitoring and remediation, data protection, and user-friendly administration.

Table 3-11 Applicable Security Components for BYOD Solution

BYOD Solution Component	Applicable Security Component(s)
Mobile Device	TPM (hardware/firmware)
	SED (e.g., cryptographic erase support)
	Secure Element (e.g. SIM, UICC, microSD)
	Policy Agent, Health Assessment Agent, Remediation Agent (e.g. MDM client)
	Separation Kernel and Hypervisor (Type 1, Type 2)
	Secure Container – OS-enforced software-based isolation of applications and data (e.g. Sandboxing)
	Security token (e.g. Smart Card CAC/PIV, RSA SecurID)
	Runtime Integrity Monitor
	VPN / TNC Client
	Host-based Security (e.g., AntiVirus, Firewall, IDS)
	Trusted Execution Environment (e.g., Global Platform TEE)
	PKI services client
Network Access Point	PKI services client
	Name Services (e.g. Secure DNS, Service Discovery)
	Directory Services (e.g. Secure LDAP services – Users, ACLs, Certificates)

BYOD Solution Component	Applicable Security Component(s)
	IDS, Firewall
	TNC Client / Proxy
	PEP
Public Network Infrastructure	PKI Certificate Authority
	Name Services (e.g. Secure DNS, Service Discovery)
	Directory Services (e.g. Secure LDAP services – Users, ACLs, Certificates)
	Hosted Security Services (e.g. Cloud-based MDM/MAM)
	TNC Servers (e.g., PEPs, PDPs, IF-MAP)
	Routers (e.g., Overlay/Virtual Networks)
	VPN Servers
	IDS / Firewall
Private Network Infrastructure	PKI Certificate Authority - Certificate Enrollment/Distribution - Key Management / Escrow / Archive - Certificate Revocation (e.g. OCSP, CRL)
	Name Services (Secure DNS, Service Discovery)
	Directory Services (e.g. Secure LDAP services – Users, ACLs, Certificates)
	TNC Servers (e.g. PEP, PDP, IF-MAP)
	Routers (e.g., Overlay/Virtual Networks)
	VPN Servers
	IDS / Firewall
	Authentication/Authorization Service (e.g. RADIUS)
	Mobile Device Management (MDM)
	Mobile Application Management (MAM)