BUILDING BLOCK

MOBILE DEVICE SECURITY FOR ENTERPRISES

V.2 – Final Draft
September 12 2014
mobile-nccoe@nist.gov

This revision incorporates comments from the public.

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) works with industry, academic and government experts to find practical solutions for businesses' most pressing cybersecurity needs. The NCCoE collaborates to build open, standards-based, modular, end-to-end solutions that are broadly applicable, customizable to the needs of individual businesses, and help businesses more easily comply with applicable standards and regulations.

This document describes a problem that is relevant to many industry sectors. NCCoE cybersecurity experts will address this challenge through the creation of a "reference design" in collaboration with a community of interest including vendors of cybersecurity solutions. The reference design will become an NCCoE "Building Block": an approach that can be incorporated into multiple use cases. The reference design created by this effort will not be the only solution available in the fast-paced cybersecurity technology market. If you would like to propose an alternative architecture or know of products that might be applicable to this challenge, please contact us at mobile-nccoe@nist.gov.

1. TARGET AUDIENCE

The cybersecurity challenge described here requires a technical solution that provides capabilities driven by business needs as well as security characteristics that are consistent with standards and best practices. This document is intended for organizations that want to implement reference designs resulting from this project and the technology and security vendors who will collaborate with the NCCoE to address this challenge.

2. DESCRIPTION

Goal

Traditionally, enterprises established boundaries to separate their trusted internal IT network(s) from untrusted external networks. When employees consume and generate corporate information on mobile devices, this traditional boundary erodes. Due to the rapid changes in today's mobile platforms, corporations have the challenge of ensuring that mobile devices connected to their networks can be trusted to protect sensitive data as it is stored, accessed and processed, while still giving users the features they have come to expect from mobile devices.

This building block will demonstrate commercially available technologies that provide protection to both organization-issued and personally-owned mobile platforms. These technologies enable users to work inside and outside the corporate network with a securely configured mobile device, while allowing for granular control over the enterprise network boundary, and minimizing the impact on function. The architecture demonstrated by this building block will incorporate a modular technology stack that allows enterprises to tailor solutions to their business needs.

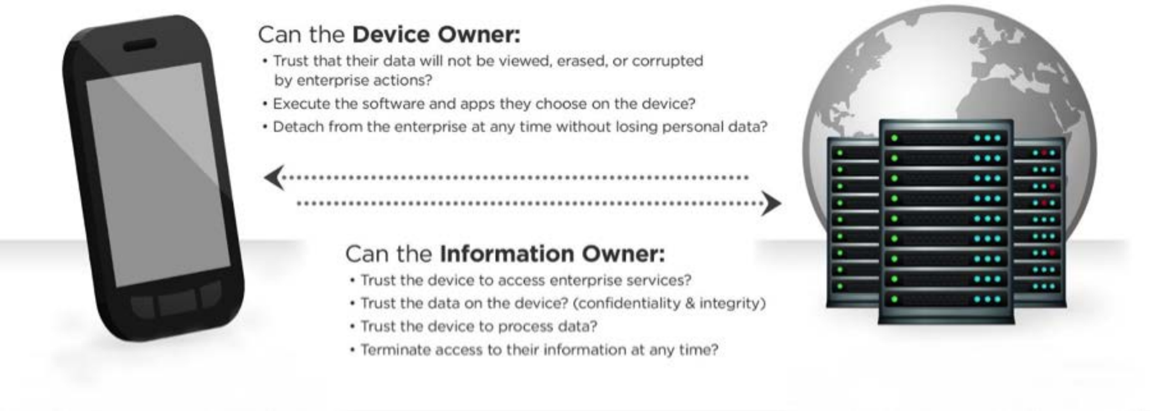
Background

In the past decade, mobile devices have allowed employees to access information resources wherever they are, whenever they need to. These capabilities present both an opportunity and a challenge. While their always-on, always-connected nature can make business practices more efficient and effective, mobile devices create new challenges to ensure the confidentiality, integrity and availability of the information they access.

As mobile technologies mature, employees increasingly want to use both organization-issued and personally-owned mobile devices to access corporate enterprise services, data and resources to perform work-related activities. Despite the security risks inherent in today's mobile devices, enterprises are under pressure to accept them due to several factors, including anticipated cost savings and employees' demand for more convenience.

3. Scenarios

This building block will demonstrate security capabilities that can provide greater assurance that a mobile device can be trusted to protect data stored, accessed or processed on the device. Understanding that every organization makes decisions regarding access to its resources based on an analysis of its enterprise risk posture, these capabilities provide tools that support an array of security controls. To ensure that these security controls are most effective, this building block will address security controls in a manner that does not negatively impact the experiences of the employee or the enterprise. The scenarios below are examples of those expectations.



Can the **Device Owner:**

- Trust that their data will not be viewed, erased, or corrupted by enterprise actions?
- Execute the software and apps they choose on the device?
- Detach from the enterprise at any time without losing personal data?

Can the **Information Owner:**

- Trust the device to access enterprise services?
- Trust the data on the device? (confidentiality & integrity)
- Trust the device to process data?
- Terminate access to their information at any time?

Figure 1. Mobile security expectations

Scenario: The User Perspective

A new employee would like to access corporate information resources, namely her e-mail, calendar, contacts and files, from a mobile device (e.g., a smart phone or tablet). The employee is informed that her company can either provision her personal device or provide her with a preconfigured device procured by the company. The inconvenience of carrying an additional mobile device does not appeal to her but she also knows that using a single device for both her personal life and work requires her company to implement certain device restrictions in order to protect the corporate data she will be accessing.

At the employee's prior company, mandatory policies severely diminished her ability to use a mobile device. Unlocking the device required a long password, which often took a long time to enter, was hard to remember, and was easy to mistype. Each time she accessed corporate files she had to set up a secure connection, requiring yet another password. Without warning, the company blacklisted a banking application she used to deposit her paychecks. If the company detected malware on her device she had to give it to the technology services staff, who would keep it for a week to remediate the incident.

Leery of repeating her prior experience, she talks with the IT staff about what restrictions the company might place on her personal device. The IT staff informs her that company security controls are designed to minimize the impact on the user. If she lets the IT staff enable her phone for work use, they will logically separate personal and corporate data and applications on the device, protecting them by password-based authentication. Remote access will require a protected tunnel back to the enterprise. Remote authentication will be handled via cryptographically secure mechanisms, such as the use of digital certificates.

After initial configuration, notifications will be sent directly to the device to inform her of any upcoming policy changes, such as restricted applications, before the policy is remotely pushed to her device. Her company will want to monitor the device for security incidents and malicious behavior, however, where possible, the monitoring will be limited to the logical areas storing corporate data and conducted with the employee's informed consent. In the event that her device is infected by malware, it will be quarantined from enterprise resources automatically, allowing her to maintain the device for personal use. She will then have the option to allow her company to perform remote remediation procedures on the device, prior to regaining access to enterprise resources.

If the employee needs to perform actions that are restricted by the corporate policy, she will be able to revoke her own access to the corporate services and information. To re-enroll, her device will need to undergo a health and integrity check to ensure that it is in a known good state and the security architecture is not compromised.

With a thorough understanding of the security and usability considerations, the employee can decide which approach best fits her needs.

Scenario: The Enterprise Perspective

Facing increasing demand from employees to access sensitive corporate data on mobile devices, an enterprise decides to implement a new mobile security strategy. In the past, the enterprise provisioned users with secured mobile devices; however, the restrictions placed on the devices encumbered users and system management required significant IT resources to keep up with device provisioning, maintenance and security incident remediation. Any new strategy needs to provide modern security and asset management capabilities while easily integrating with current production systems.

According to the new strategy, the corporate IT staff will perform a remote scan to determine the current health and integrity of the device prior to enrollment. Once the device is deemed acceptable, the enterprise will enroll the device by remotely pushing user- and device-specific security policies. Policy implementation will allow the enterprise to maintain a logical separation between corporate and user data. Cryptographic tokens for accessing enterprise email and other resources will be issued during provisioning, either in person or remotely, to ensure cryptographic mechanisms are in place and properly used once the employee receives the device.

Once users are allowed to access enterprise resources, it should be easy to maintain an asset database and push policy and system updates to all enrolled devices. Compliance checks should occur automatically at regular intervals, with policy violations immediately reported to the employee and the enterprise for remediation. For audit purposes, regular scanning and logging should occur automatically and be reported back to the enterprise. In support of security incident triaging and remediation, the security dashboard should easily display pertinent audit and logging information and enable the enterprise to cut off resources and/or remotely wipe corporate data from the malicious device.

With these expectations in mind, the enterprise can draft and implement their new mobile strategy.

4. Architecture Characteristics

Specific methods for meeting both user and enterprise expectations require the implementation of both functional and security characteristics.

The wide adoption of smart devices for personal use has expanded the feature set that employees expect from mobile devices used for business. When securing these devices, the impact of security controls on users must be taken into consideration, as an increase in security controls alone does not guarantee an increase in overall security. If a control inhibits an employee's ability to work or goes against their expectations of functionality, a user will often find a way around it, reducing realized security. Therefore, implemented security controls should promote secure behaviors while minimizing impact on a user's daily workflow.

The sets of characteristic found below help enterprises attain a secure solution. Each characteristic has one or more example of a capability that would meet the intent of the characteristic. These characteristics and corresponding capabilities are not exhaustive. Furthermore, capabilities are defined to provide context for the characteristics and are not meant to be prescriptive.

Security Characteristics

The following characteristics are founded in the principles identified in NIST SP 800-164. All of the characteristics should be implemented with verifiable integrity via continued assertions that the device has not been compromised (e.g., that key firmware or operating system files have not been tampered with, that the device has not been "rooted" or "jail broken," and that the device's security policies are verified as those being issued by the enterprise). Many of the terms used below are not standardized throughout industry. Therefore, the descriptions provided alongside the capabilities reflect our meaning in the context of this building block.

133

Security characteristics	Example security capabilities
data protection	• protected storage - device encryption: cryptographic protection of all or portions of a device's data storage locations - primarily NAND flash memory - secure containers: a combination of mechanisms, such as encryption, to protect a distinct data storage location that can be managed - trusted key storage: protected locations in software, firmware or hardware in which long-term cryptographic keys can be held - hardware security modules: tamper-resistant hardware used to perform cryptographic operations and secure storage that may be removable or physically part of the device - remote wipe: render access to corporate data stored on the device infeasible and may only wipe a portion of flash memory • protected communications - VPN, to include per-app VPN • data protection in process - encrypted memory - protected execution environments
data isolation	• virtualization: support for hardware-based virtualization • sandboxing: OS or application-level mechanisms utilizing multiple protection, isolation and integrity capabilities to achieve higher levels of overall isolation • memory isolation: processes should be unable to access or modify another process' memory • trusted execution: a process is created and runs in a trustworthy and isolated execution environment leveraging distinct memory spaces and controlled interfaces • device resource management: ability to enable/disable device peripherals • data flow control - data tagging: as data is accessed by a mobile application, policies relevant to that data are transmitted simultaneously and enforced on that data by the application • baseband isolation: ensure that the software/firmware on the application processor and the baseband communicate with one another over well-defined and constrained interfaces

Table continues, next page

Security characteristics	**Example security capabilities**
device integrity	• baseband integrity checks: ensure that the baseband firmware/operating system has not been maliciously or accidentally modified • application black/whitelisting: preventing or allowing applications to run based on a pre-specified list • device integrity checks: - boot validation: validation the that device is in a known working state and unmodified at boot; e.g. BIOS integrity checks - application verification: ensure corporate applications being installed come from a valid source - verified application and OS updates - trusted integrity reports: ensure that integrity reports pulled from the device are representative of the current and true state of the device - policy integrity verification: ensure that the policies received by the device come from a verified source
monitoring	• canned reports and ad hoc queries • auditing and logging: capture and store device and application information • anomalous behavior detection: observe activities of mobile users, devices and processes, and measure those activities against a baseline of known normal activity • compliance checks: provide information about whether a device has remained compliant with a mandated set of policies • asset management: identify and track devices, components, software and services residing on a network • root and jailbreak detection: ensure that the security architecture for a mobile device has not been compromised • geo-fencing: monitor a device's geolocation and enable/disable device and network resources based on that location
identity and authorization	• authentication of user - local authentication to applications - local authentication to device - remote authentication • authentication of device - remote authentication • implementation of user and device roles for authorization • credential, token storage and use • device provisioning and enrollment
privacy	• company should not be able to monitor and/or report personal activity or capture personal information such as non-corporate account authentication credentials, contacts, phone logs or text messages • notifications provided to users about the privacy implications of certain device and application functionality

Functional Characteristics

Turning theoretical security controls into real-world security requires system security designs that ensure ease of use for both the employee and the enterprise. The functional characteristics and capabilities listed below are examples of considerations that can greatly affect the security of an enterprise mobility management strategy. These functional characteristics enhance the user and administrative experience while supporting the above security characteristics.

Functional characteristics	Example functional capabilities	Benefactor
provisioning	• ability to provision the device remotely	user and enterprise
software update management	• remote application delivery and updates: push application and OS patches, as well as new applications, to the device • remote system updates: distribute the newest releases of corporate applications and security software	user and enterprise
policy management	• ability to easily specify granular security policies • remotely push new or updated policies to the device • notify users of any expected functionality changes prior to the update	user and enterprise
easily distinguishable corporate user interface	• visual cues within the user interface to help remind the user of when they are accessing corporate data and resources	user and enterprise
monitoring	• automatic, regular device integrity and compliance checks • automated alerts for policy violations	enterprise
auditing	• automatically generate reports/dashboard for auditing • easy to access and interpret logging	enterprise
unobtrusive remediation procedures	• should a device compromise occur, security incident remediation can be performed with little to no loss of personal functionality on the device	user
unobtrusive protected connection establishment	• ability for the user to quickly and easily establish a protected connection between the device and the corporate resources	user
unobtrusive authentication methods	• authentication to applications and services done in the background without the need for user interaction • authentication that does not require complex passwords requirements to unlock the device	user
simple key management	• the ability to easily obtain keys for encrypted e-mail	user
simple corporate file sharing	• ability to transfer enterprise data (e.g., drag-and-drop, SMS, upload to cloud) via the mobile interface	user

5. Approach

This building block demonstrates a commercially available set of technologies that address the security challenges mobile devices present to an enterprise. The capabilities demonstrated in this build should allow enterprises to implement security controls that best fit their enterprise security needs regardless of device or information ownership. This project will take a “device up” approach, starting with the implementation of security characteristics and capabilities that involve the mobile device and its management. Figure 3 demonstrates example capabilities that fit into the device technology stack.

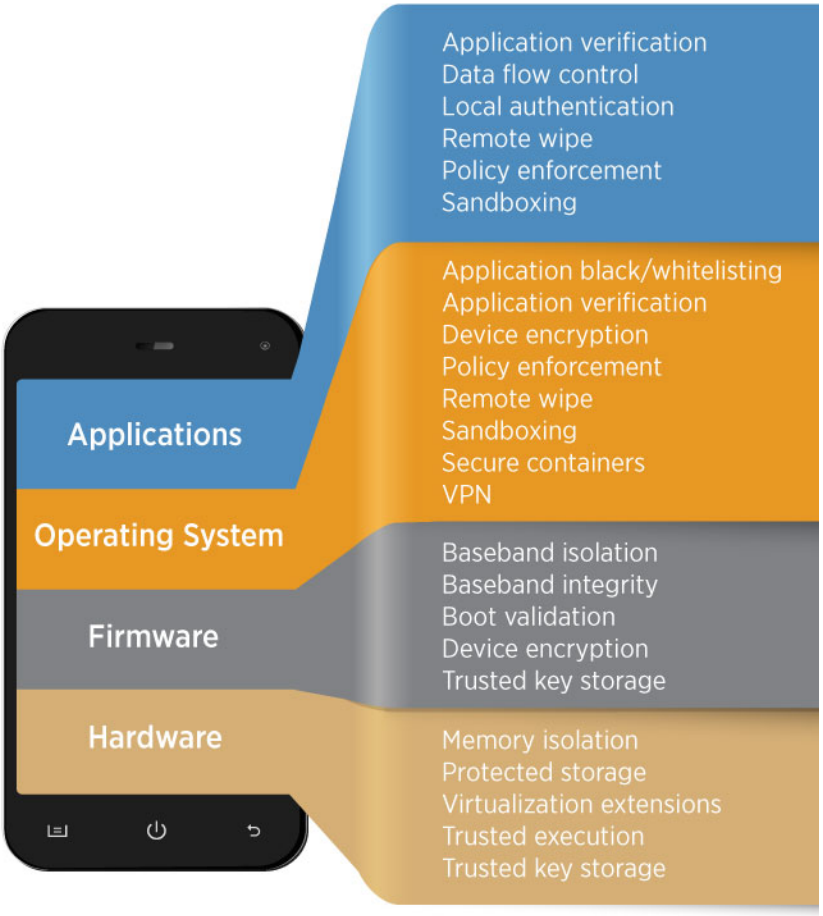


Figure 3. High-level device architecture

In order to address a full array of mobile platforms and technologies, several initial builds may occur as part of this building block. Note that this is an initial approach and that the building block process is intended to be iterative. As mobile technologies and capabilities evolve, the initial technology set of this building block may be augmented with additional functionality such as application vetting. Finally, throughout the build process, the implementation of all security characteristics shall be mapped to their applicable security controls found in the standards in Section 7 of this document.

The initial build architecture will focus on securing common workplace applications: email, contacts and calendar. Additionally, the architecture will demonstrate that the hardened mobile device can securely access corporate data for which the user and device are authorized and that accessed data stays within corporately defined boundaries and terms of use. The implementation of the above device security capabilities will leverage an enterprise mobility management suite (EMM), necessitating that the build includes an enterprise mobility security architecture that incorporates common network components and management practices.

6. Business Value

- provides enterprise-class protection to users who need to access untrustworthy cellular and Wi-Fi networks, peripherals, apps and web sites
- enables users to work inside and outside the corporate network with a hardened mobile device that is unlikely to adversely affect an enterprise if the device is compromised
- reduces total outlays in redundant enterprise network security systems by improving security of mobile devices
- helps companies embrace the BYOD and other mobile management models and reduce corresponding capital investment by increasing security on users' mobile devices
- broadens visibility of users' behavior in accessing and working on corporate networks in order to bolster identity and access management capabilities

7. Relevant Standards

- NIST SP 800-124 Rev 1, Guidelines for Managing the Security of Mobile Devices in the Enterprise
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
- NIST SP 800-163 (Draft), Technical Considerations for Vetting 3rd Party Mobile Applications
  http://csrc.nist.gov/publications/drafts/800-163/sp800_163_draft.pdf
- NIST SP 800-164 (Draft), Guidelines on Hardware-Rooted Security for Mobile Device
  http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf
- Global Platform Specifications for Secure Element (http://www.globalplatform.org/mediaguideSE.asp) and Trusted Execution Environment (http://www.globalplatform.org/mediaguidetee.asp)
- Trusted Computing Group specifications for Trusted Platform Module (http://www.trustedcomputinggroup.org/resources/tpm_main_specification) and Trusted Network Connect (http://www.trustedcomputinggroup.org/developers/trusted_network_connect)
- NIST SP 800-147: BIOS Protection
  http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf
- NIST SP 800-155: BIOS Integrity Measurements
  http://csrc.nist.gov/publications/drafts/800-155/draft-SP800-155_Dec2011.pdf
- NSA Mobility Capability Package 2.3
  http://www.nsa.gov/ia/_files/Mobility_Capability_Pkg_Vers_2_3.pdf

- Department of Defense Commercial Mobile Device Implementation Plan http://www.defense.gov/news/dodcMdimplementationplan.pdf
- National Information Assurance Partnership Protection Profile for Mobile Device Management Version 1.1 https://www.niap-ccevs.org/pp/pp_mdm_v1.1/
- National Information Assurance Partnership Protection Profile for Mobile Devices Version 1.1 https://www.niap-ccevs.org/pp/pp_md_v1.1/
- Digital Government Strategy Government Mobile and Wireless Security Baseline https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf
- GSA Managed Mobility Program Request for Technical Capabilities https://www.fbo.gov/notices/3ce61f2675d67e705337738e58f2ec57

8. Security Control Map

This table maps the preliminary list of desired characteristics of the commercial products that the NCCoE will apply to this cybersecurity challenge to the applicable standards and best practices described in the Framework for Improving Critical Infrastructure Cybersecurity (CSF) and other NIST activities. This is meant to demonstrate the real-world applicability of standards and best practices, but does not imply that products with these characteristics will meet your industry's requirements for regulatory approval or accreditation.

Example Characteristic		Cybersecurity Standards & Best Practices					
Security Characteristic	**Example Capability**	**CSF Function**	**CSF Category**	**CSF Subcategory**	**NIST 800-53 rev 4**	**IEC/ISO - 27002**	**SANS CAG20**
data protection	protected storage: device encryption, secure containers, trusted key storage, hardware security modules, remote wipe; protected communications: VPN, to include per-app VPN; data protection in process: encrypted memory, protected execution environments	Protect	Data Security, Protective Technologies	PR.DS-1, PR.DS-2 , PR.DS-5, PR.PT-4	AC-20, AU-9, IA-6, IA-7, MP-6, SA-13, SC-8, SC-11, SC-12, SC-13, SC-17, SI-12	6.2.1, 9.4.3, 9.4.4, 9.4.5, 10.1.2, 12.4.2, 12.4.3, 13.1.1 , 13.2.1, 13.2.3, 14.1.3	CSC-15
data isolation	virtualization, sandboxing, memory isolation, trusted execution, device resource management, data flow control, data tagging, baseband isolation	Protect	Data Security, Protective Technologies	PR.DS-1 , PR.DS-5, PR.PT-3	CM-11, SA-13, SC-3, SC-11, SC-35, SC-39, SC-40, SI-16	6.2.1, 6.2.2, 9.4.1, 9.4.4, 12.2.1	CSC-7, CSC-12, CSC-14
device integrity	baseband integrity checks, application black/whitelisting, device integrity checks: boot validation, application verification, verified application and OS updates, trusted integrity reports, policy integrity verification	Protect/Detect	Data Protection, Anomalies and Events, Security Continuous Monitoring	PR.DS-6, DC.CM-4, DE.CM-5, DE.CM-6	AC-20, CM-3, IA-3, IA-10, SA-12, SA-13, SA-19, SC-16, SI-3, SI-4, SI-7	6.2.1, 12.2.1, 14.2.4, 15.1.3	CSC-3, CSC-6, CSC-12
monitoring	canned reports and ad-hoc queries, auditing and logging, anomalous behavior detection, compliance checks, asset management, root and jailbreak detection, geo-fencing	Identify/Protect/Detect	Asset Management, Maintenance, Protective Technology, Anomalies and Events, Security Continuous Monitoring, Detection Processes	ID.AM-1, ID.AM-2, PR.DS-3PR.MA-2, PR.PT-1, DE.AE-1, DE.AE-2, DE.AE-3 , DE.AE-5, DE.CM-1, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8, DE.DP-2, DE.DP-4	AC-2, AC-3, AC-7, AC-21, AC-25, AU-3, AU-5, AU-5, AU-7, AU-8, AU-9, AU-10, AU-12, AU-13, AU-14, AU-15, AU-16, CA-7, CM-2, CM-3, CM-6, CM-8, CM-11, IA-4, IR-4, IR-5, IR-7, IR-9, MA-6, SA-13, SA-22, SC-4, SC-5, SC-7, SC-18, SC-42, SC-43, SI-3, SI-4, SI-5	6.1.4, 6.2.1, 6.2.2, 8.1.1, 8.1.2, 9.2.3, 9.2.5, 9.4.4, 9.4.5, 10.1.2, 12.2.1, 12.4.1, 12.4.2, 12.4.3, 12.5.1, 12.6.1, 12.7.1, 13.1.1, 15.1.3, 16.1.2, 16.1.4, 16.1.5, 18.2.3	CSC-1, CSC-2, CSC-5, CSC-6, CSC-10, CSC-11, CSC-12, CSC-13, CSC-14, CSC-18
identity and authorization	local user authentication to applications, local user authentication to device, remote user authentication, remote device authentication, implementation of user and device roles for authorization, credential and token storage and use, device provisioning and enrollment	Protect/Detect	Access Control, Protective Technologies, Asset Management	ID.AM-1, PR.AC-1, PR.AC-3, PR.AC-4, PR.PT-3, DE.CM-3, DE.CM-7	AC-2, AC-3, AC-4 ,AC-5, AC-6, AC-7, AC-16, AC-17, AC-18, AC-19, AC-20, AU-16, CM-5, CM-7, IA-2, IA-3, IA-5, IA-6, IA-7, IA-8, IA-9, IA-11, MP-2, SA-9, SA-13, SA-19, SC-4, SC-16, SC-40	6.2.1, 6.2.2, 9.1.1, 9.1.2, 9.2.1, 9.2.2, 9.2.3, 9.2.4, 9.3.1, 9.4.1, 9.4.2, 9.4.3, 13.1.1, 13.1.2, 13.2.2, 13.2.3, 14.1.2, 14.1.3	CSC-8, CSC-9
privacy protection	informed consent of user, data monitoring minimization, privacy notification provided to user	Identify/Protect	Governance, Training and Awareness	ID.GV-3, PR.AT-1	AR-4, AR-7, DM-1, IP-1, IP-2, SE-1, TR-1, UL-1	18.1.4	CSC-17

9. High-Level Architecture

The high-level architecture depicts an example mobility management solution implemented within an enterprise.

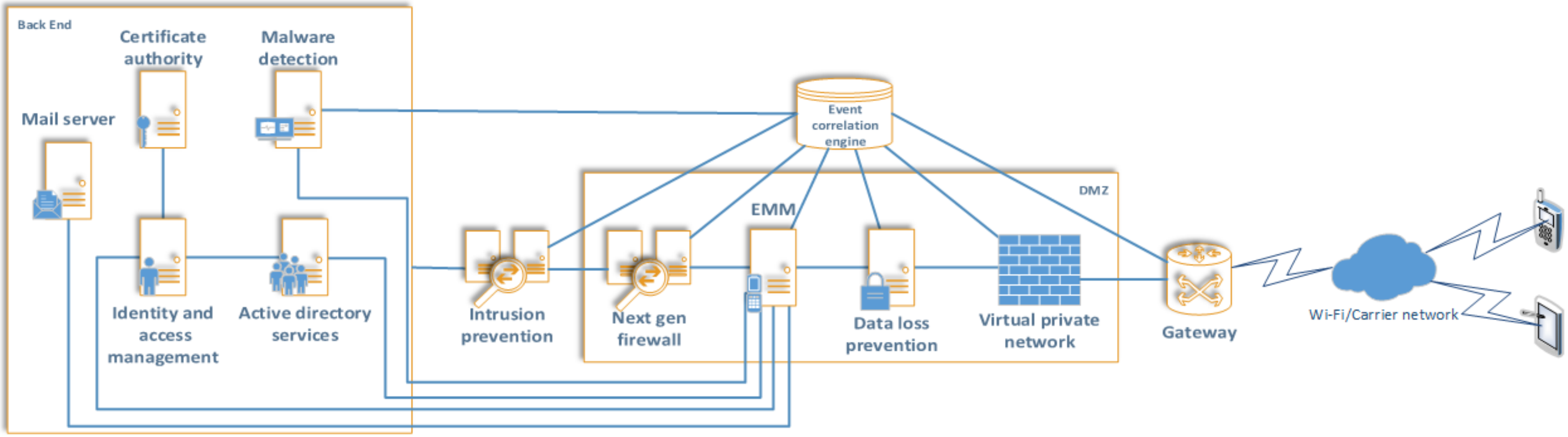


Figure 4. High-level enterprise mobility architecture

10. COMPONENT LIST

- an initial set of mobile devices including phones, tablets, and wearables, running modern mobile operating systems (i.e., Android, iOS, Windows Phone) from various hardware manufacturers
  - to the extent possible, mobile devices will support the security features outlined in NIST SP 800-164, DRAFT Guidelines on Hardware-Rooted Security in Mobile Devices
- enterprise mobility management suite
- mobile applications requiring security assurance
  - e.g.: applications that can be put in a secure container, allow for wrapping, etc.
- identity and access management system
- data loss prevention (DLP) solution
- event correlation engine
- enterprise infrastructure (e.g., directory server, VPN gateways, internal network, certification authority)

11. COMMENTS

We received 24 comments regarding the draft building block. We have provided a response to each comment and revised the document accordingly. Comments labeled as proprietary or confidential were taken into consideration but are not published here.

ID	Comments	Response
1	Specifically we would like to discuss Page 7, Mobile Application Security and suggest that it also includes MRM (Mobile Risk Management) as a method to assess the security characteristics for all applications installed on a device.	Within the builds we may reference the ability to assign a risk score to each application prior to installing it onto the device. We could possibly accomplish this via the NIST mobile application portal envisioned by NIST SP 800-163.
2	This document does not seem to break any new ground for most of us in IT. This is stuff that we've known for years. And really, a BYOD is not much different that managing other devices, with one clear difference. We cannot in any way infringe upon or damage the integrity and/or the privacy of the BYOD user/owner's information.	This is consistent with the feedback the NCCoE received from its National Cybersecurity Excellence Partners working in this area. In conjunction with this comment and others, the document was completely restructured to focus on securing data with the goal of unifying endpoint device management.
3	I actually think that a BYOD owner should not so easily give in to the corporate embrace of BYOD. The corporate embrace of BYOD is not in the favor of the employee. Why should an employer's purchase of their own device to do work for their employer be perceived as a good thing on the part of the employee? If the company wants that much work out of me, they can buy my device and most are actually choosing this approach, even now.	If we can achieve a high level of usability, we believe this becomes less of an issue. The flip side is obviously that the user now has to carry two devices which they may not want, either. We have added privacy as a security characteristic within the document, and elsewhere we mention informed consent of the user.
4	The document (especially Sections 1 and 2) does not address the role or impact that the cellular provider has on the configuration of the mobile device (secure or otherwise). For the scenarios in Section 2: a. In the BYOD scenarios described, the cellular provider will most likely be the primary source of configuration (not the user or the employer) b. In the COPE scenario, any corporate changes will most likely need to be made in coordination with one or more cellular provider	We recognize the role of the cellular provider in securing the device. However, the determination has been made that working with cellular providers is out of scope for the first instantiation of this building block. This is a possible future area of research.

ID	Comments	Response
5	The document refers to a technology solution “stack” but does not provide any discussion of how this building block actually uses any layering. One would expect that the document to describe how MDM/MAM layer policy onto the mobile device which in turn provides the basis to enforce policy in the applications.	The core concept of the technology solution stack has been removed to make the document more data driven and to focus on endpoint device management. Additionally, we grouped our security characteristics into new categories with the intent of aligning with policy and other security considerations in lieu of individual technologies (e.g., MDM). This also removes the duplicated characteristics and capabilities, in our opinion leading to a more readable document.
6	Secure Voice/VOIP did not appear to be addressed in the building block. While this functionality may not be as broadly desired as other capabilities, there are significant customer bases where this is important and seems it would be an area that should be included in the building block.	This is out of scope for our current project, but this could be addressed within a future effort. Excellent idea.
7	Lines 95-100: The term “high assurance” has specific meaning within the security assessment community, implying formal methods and design/implementation level analysis. The description in this paragraph focuses on continual monitoring and the integrity of the device, along with some trusted channel aspects. Suggest that part of the building block build-out and documentation address the assurance considerations (in the classic sense—that is, the confidence one has the mechanisms/capabilities implemented perform correctly and cannot be made to take actions that circumvent the device security policy/functionality), and that the continuous monitoring aspect be an additional, separately-discussed capability for this building block.	Astute comment. Perhaps the "High Assurance" pieces are only those that are built upon a root of trust, versus those that are checked on a very frequent basis for compliance/integrity. We removed the concept of "high assurance" from the document in part due to this comment as we did not want to cause confusion within the conformity assessment community. However, the concept of "assurance considerations" may be included within the future practice guide.
8	Table after line 106, “data protection” and “policy management”: It seems that “Trusted Communications” (e.g., a VPN) between the MDM and the device is an important example characteristic that should be included in this entry. The “encrypted communications” example in the policy management line seems to indicate a somewhat limited capability.	We specifically call out VPN capabilities in the document. From the comment alone, it was difficult to determine the intended difference in the semantics between "encrypted communications" and "trusted communications". The term "trusted communications" has been removed and changed to "protected communications" as "trusted" may imply

ID	Comments	Response
		something further than what we were intending.
9	Table after line 106, ‘monitoring and alerting’ entry, ‘anomalous behavior detection’: ‘observe’ implies real-time monitoring of the actions of mobile users, where it seems more likely that this is done through analysis of logs collected by the mobile device (as indicated on line 144). Suggest using ‘analyze logs of’ instead of ‘observe.’	We meant ‘*observe*’ in a real-time sense although we simply call for logging and not log analysis. Made change by specifying "automatically."
10	Line 109-111 – enforcement of policy at the application level is probably a bad example. This level is inherently vulnerable – for example it is not clear how a remote wipe policy could be realistically enforced at the application level.	We certainly agree that policy enforcement can occur with varying levels of security at the application level. For instance, a corporately owned and developed app could include more policy enforcement than an app taken from the Google play store. Remote wiping could include deleting the cryptographic keys used to encrypt information at the application level, leading to a remote wiping scenario. This is sometimes referred to as a cryptographic wipe or a cryptographic erase. Refer to forthcoming NIST publication on data sanitization for additional information.
11	Table after line 112, ‘data protection’: While the introduction makes clear that the examples are only representative and not exhaustive, suggest adding ‘certificate management’ and ‘device resource management’ (e.g., access to device resources such as GPS, network, baseband, etc.), as these are two distinguishers that will significantly enhance the security and granularity for specification and implementation of policy.	We completed a revamp of that section alongside explanations of each capability within the data protection characteristic. Although your specific recommendations may not have been included, they were definitely taken into consideration.

ID	Comments	Response
12	Table after line 112, ‘policy enforcement’: It seems that authentication of the user to the device is not included in this table (although per-app authentication is included in the next section), and has implications for the local implementation of policies. The capability for a device to enforce the distinction between local policy configuration and enterprise policy configuration (such that a local user may be able to configure some policies, but others may only be configurable by the enterprise) also seems like it would be an important characteristic to demonstrate.	We mentioned a PIN/password enforcement requirement but we are unsure if this is discussing the existence of a local identity and associated user profile stored on the device. We are unsure of how this would be implemented, so a change was made to include it as "local authentication."
13	Lines 139, 145: The ‘layered’ approach is clear for apps on a mobile device; the relationship between the MDM and the device is not as clear, however. If anything, it seems the device would form ‘layer 0,’ as it contains the features that the MDM will be managing, so establishing the feature set would aid in determining how those features would be controlled. ‘Layer 1’ (the MDM) would then show the management of those features. In practice, these would probably be done together so it’s likely more accurate that these are layer 1a and 1b.	The core concept of the technology solution stack has been removed to make the document more data driven. Additionally, we grouped our security characteristics into new buckets aligning with policy and other security considerations - and less on the individual technologies (e.g., MDM). This also removes the duplicated characteristics and capabilities, leading to a more readable document.
14	Line 168, Section 6: In addition to the MDM and MDF Protection Profiles, the VPN Client Protection Profile is also relevant. If Secure Voice is included, then the VOIP Client and SIP Server Protection Profiles also are relevant.	VPNs are specifically included within the document, but because there is no mobile specific VPN client protection profile, we've decided to omit this protection profile.

ID	Comments	Response
15	Best practice for information security is to develop a layered security strategy. As it relates to mobility, secure computing should be developed from the device 'up.' Specifically, start at the data level, move to the apps, and provide the ability to restrict access based on device type. Appropriate policies should also be put in place. II. Recommended changes to document Reorder the stack found on lines 87-89 as follows: • Mobile devices • Mobile applications • Mobile device and application management The reason for this suggestion is to "build the case" for secure mobile computing from the device up. By building from the ground up, organizations can mitigate many possible mobile risks. There are three supporting considerations, as follows: If the device hardware is not developed with a secure hardware and secure firmware foundation, future efforts to secure the device will always be built on an inadequate device hardware/firmware foundation.	Due to comments both internally and externally, the building block was significantly changed from its original incarnation. The concept of the technology solution stack was removed and the document was reformed around a data protection train of thought.
16	Mobile apps should go through a rigorous test/evaluation process to ensure the apps are properly coded and are relatively secure 'without' the introduction of MDM/MAM processes. In other words, if the mobile app software is in and of itself unsecure, buggy, or poorly coded, it should never reach the phase where it is placed on a mobile device.	We agree. We wanted to ensure that mobile application vetting was not 100% removed from the scope of the document. To accomplish this, we included the following paragraph: "In order to address a full array of mobile platforms and technologies, several initial builds may occur as part of this building block. Note that this is an initial approach and that the building block process is intended to be iterative. As mobile technologies and capabilities evolve, the initial technology set of this building block may be augmented with additional functionality such as application vetting."

ID	Comments	Response
17	Lastly, but certainly in no way the least critical consideration, the MDM/MAM functional system should be put in place.	Agreed.
18	The steps: The best way to mitigate security risk factors at the device level is to start at the data, move to the app, finally provide the ability to restrict access based on the device type and secure the device through policy. The recommended strategy is to make sure the data on the device is always in an encrypted state even when the device is unlocked. In other words, protect the data so it is never on the disk in the clear.	Agreed. The document was restructured in large part due to this comment and others received from our National Cybersecurity Excellence Partners.
19	Specifically below line 106, the phrase 'remote wipe' should, ideally, be more strongly worded in the explanation. Remotely rendering access to data as unfeasible implies that the data still resides on the mobile device. Instead, it is best of the data is deleted from the device without data remanence [sic] on the device once wiped.	We want to ensure that a cryptographic wipe is still possible, as it may be particularly useful in scenarios in which a user is using a personal device with enterprise data residing on it. Remotely wiping the device may not be an option, but cryptographically rendering the data unreadable is feasible. Additionally, this concept is outlaid in NIST SP 800-164 and forthcoming NIST data sanitization guidance.
20	With regard to create/manage secure containers, we recommend promoting very high encryption standards for those containers.	Agreed, although we will be unable to specify the standards within the building block itself as different containerization solutions may use different cryptographic standards. This will be discussed in detail within the forthcoming practice guides.
21	With regard to monitoring and alerting, specify not just that rooted/jail broken devices will be detected, but that policy can be set in place to immediately wipe corporate data from such devices upon initial rooted/jail broken detection.	Many policies can be implemented and instead of enumerating all of them within the building block, we can utilize those offered by the MDMs and OSs to ensure that they meet our security characteristics and capabilities.
22	With regard to data protection, the discussion on VPN would be useful to promote IPSEC versus legacy VPN methods that may be more vulnerable to MITM attacks.	We are unable to specify the specific standards within the building block itself as different VPN solution from various vendors may use different algorithms. This will be discussed in detail within the

ID	Comments	Response
		forthcoming practice guides.
23	For the entire section on Mobile Application Security, it may be useful to promote a process of ‘app validation’ prior to an organization approving mobile apps for their enterprise mobile device ecosystem. A perfect example of this is the DHS ‘Carwash’ program. Several commercial vendors are also developing such programs to validate the security functionality and overall coding quality of various mobile apps. By being selective in which mobile apps an organization approves for its users to process sensitive organizational data, the organization can have this as an additional security step (security in layers is the mantra of all good infosec practitioners).	We would agree with this comment, had the original version of this document not been significantly restructured. We wanted to ensure that mobile application vetting was not 100% removed from the scope of the document. To accomplish this, we included the following paragraph: "As mobile technologies and capabilities evolve, the initial technology set of this building block may be augmented with additional functionality such as application vetting."
24	III. Trends We suggest including a future development strategy section that encourages organizations to specifically pursue MDM/MAM vendors that will provide specialized Two Factor Authentication methods, efficient/effective cloud security management controls for the MDM/MAM admin server architecture, and integration with DLP solutions that will be able to identify in ‘real time’ whenever a mobile user is accessing sensitive data from the internal organizational network and attempting to download it to his or her mobile device. Also synchronous with this concept would be in the cases where policies allow mobile users to perform such downloads to stop (and notify management) whenever a mobile user attempts to move such sensitive data from the secure mobile container to an unsecure area of the mobile device or out through a non-approved method (Gmail, Dropbox, Evernote, off to a printer, etc.)	Many of these concepts were included within the final version of the document (e.g., DLP). As of now, we are not including "Future Development Strategy" sections in our building blocks, but we are taking this under consideration for the future.