Enterprise Mobility Security Standard (EMSS) 
by AT&T Chief Security Office, ESPCP

The steady double digit growth of threats to smartphones makes security awareness and action imperative. Recognizing the seriousness of these threats and the ubiquitous, business-critical nature of mobile applications used by enterprises today, the AT&T Chief Security Office (CSO) has prepared this comprehensive document containing a lengthy set of controls for ensuring security of mobile applications and platforms. Enterprises may choose to use these security controls as a step by step method for auditing and strengthening the security of their mobile applications and providers. Alternatively, enterprises may engage AT&T Consulting to perform a mobility security audit using the standards in this document.

The aim of the Enterprise Mobility Security Standard (EMSS) is to provide a compelling suite of mobile security controls that tackle the growing security challenges associated with the revolution in mobile data utility around smartphones. Within the context of an overall information security program, organizations need to implement mobile security controls to provide adequate data and information protection and to ensure that the many applicable regulatory or compliance concerns are sufficiently addressed in smartphones and associated ecosystems.

EMSS provides a basis for testing smartphone security controls, as well as any technical security controls in the environment, that are relied on to protect against threats to smartphones such as malware payloads. This standard can be used to establish a level of confidence in smartphone and associated ecosystem security.

The EMSS security controls were aggregated with the following objectives in mind:

- **Use as a metric** - Provide application developers, application purveyors, and those acquiring applications with a yardstick with which to assess the degree of trust that can be placed on smartphone applications,
- **Use as guidance** - For the mobile application market that is growing at a breakneck pace, provide guidance to security solution developers as to what to build into their products slated for mobile platforms, and
- **Use during procurement** - Provide a basis for specifying application security verification requirements for mobile platforms in contracts.
EMSS uses a subset of the Control Areas from the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) as an overarching framework with focus on following key assessment categories:

- **Mobile Device Security and Management Controls**
- **Application Controls**
- **Data Controls**
- **Network level Controls and Protections**
- **Machine to Machine (M2M) Security**

Use of the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM), offers the added benefit of the mobile security controls being aligned with applicable standards (i.e. COBIT, HIPAA, ISO, NIST and PCI).

The Security Control Specifications contained in this document are attributed to the Cloud Security Alliance (CSA) Cloud Controls Matrix Version (CCM) 1.1, and are represented with approval from CSA. Please visit [http://www.cloudsecurityalliance.org/cm.html](http://www.cloudsecurityalliance.org/cm.html) for more information.

### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| Data Governance - Ownership / Stewardship DG-01 | All data shall be designated with stewardship with assigned responsibilities defined, documented and communicated. | **Data Controls**
1. The designated proprietary information, for which company employees and authorized contracted workers have custodian responsibility, must be protected by them when reading, transferring and/or storing this information on wireless handheld mobile devices [smartphones].
2. Smartphone users must complete awareness training about protecting the company, its data and information against theft, loss, and/or malicious use and must executed an acceptable use agreement. |
| Facility Security - User Access FS-02 | Physical access to information assets and functions by users and support personnel shall be restricted. | **Network Level Controls and Protections**
1. Wireless hardware (e.g. APs) connected to the company’s networks must be company authorized and located in company controlled space. This does not include wireless network cards.
2. All Supplier contracts for support services including access to mobile infrastructure equipment must include appropriate requirements for security controls. |
<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| **Facility Security - Asset Management** | **FS-08** A complete inventory of critical assets shall be maintained with ownership defined and documented. | **Mobile Device Security and Management Controls**  
1. Smartphone Asset Management should include:  
a. Centralized registration designating Company Official Use (COU) or Personal Owned  
b. Asset reporting  
c. Compliance reporting  
d. **Self-service** [re: registration, lock, wipe, password change, locate, etc.]  
3. A Personal owned smartphone must implement two separately contained processing environments, one for company business information processing and storage and one for personal information. This configuration must ensure separation of business and personal information on the smartphone.  
4. Smartphone software used to process and store company information **must** be obtained from company approved software inventory and/or app store(s) and the smartphone **must** be scanned for malware and unauthorized applications.  
5. Jailbroken smartphones must not access company data.  

**Network Level Controls and Protections**  
6. Personal owned smartphones should be scanned for compliance with company security standards and configurations before they access the company network. |
| **Information Security - User Access Restriction / Authorization** | **IS-08** Normal and privileged user access to applications, systems, databases, network configurations, and sensitive data and functions shall be restricted and approved by management prior to access granted. | **Mobile Device Security and Management Controls**  
1. The company should authorize use of wireless handheld devices based on what equipment and services employees are eligible to receive predicated on their job role.  
2. Access should only be granted to necessary services based on job role, i.e. EAS [Exchange ActiveSync], PIM [Personal Information Manager] sync, e.g. Calendar Contacts, Tasks, Memo..., VPN, etc. |
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Information Security – Encryption</strong> IS-18</td>
<td>Policies and procedures shall be established and mechanisms implemented for encrypting sensitive data in storage (e.g., file servers, databases, and end-user workstations and mobile devices) and data in transmission (e.g., system interfaces, over public networks, and electronic messaging).</td>
<td><strong>Data Controls</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. The Encryption used for protection of data at rest and in transit shall be Industry standard encryption.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Key lengths: <strong>Symmetric</strong> encryption key lengths must be at least 112 bits long. 256 bit key length is preferred, unless it impacts the responsiveness of the application. <strong>Asymmetric</strong> key lengths must be at least 1024 bits.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. 1-way hashes of PINs or passwords should include a random 64-bit salt.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Content stored on the smartphone should be encrypted.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. PIM [Personal Information Manager] sync, and all data transfer should be encrypted.</td>
</tr>
<tr>
<td><strong>Information Security - Encryption Key Management</strong> IS-19</td>
<td>Policies and procedures shall be established and mechanisms implemented for effective key management to support encryption of data in storage and in transmission.</td>
<td>1. A documented operational model must exist for each application that manages keys. The operational model must include defined roles and responsibilities for each key management function and a description of how key management standards for each function are met.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. Encryption keys [classified as proprietary information] must not be stored, cached or “remembered” in plain text, and must not be hard coded in the application. [Consider using Key stores provided by the operating system.] If stored on removable media, such as a USB drive or memory card the user must take precautions to physically secure the media.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. The decryption key should be stored on the system and the messaging server residing at the Company’s facilities.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4. Encryption keys should be unique for each handset instance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5. Encryption keys, and salt and nonce values, should be generated securely, as random numbers. [e.g. use of SecureRandom or Microsoft CryptoAPI.]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6. Encryption keys should be coded into mutable primitive arrays, not immutable objects. The arrays should be zeroed out before freeing for garbage collection.</td>
</tr>
</tbody>
</table>
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security - Anti-Virus / Malicious Software IS-21</td>
<td>Ensure that all antivirus programs are capable of detecting, removing, and protecting against all known types of malicious or unauthorized software with antivirus signature updates at least every 12 hours.</td>
<td><strong>Mobile Device Security and Management Controls</strong>&lt;br&gt;1. The Mobile ecosystem [Device, Network and Cloud] must include the capability [e.g. a gateway] to detect malware, and prevent it from installing itself in the end-to-end Mobile Service that includes cloud computing networked to endpoints or smartphones.&lt;br&gt;2. In house and 3rd party developed applications should be digitally signed. When these applications are downloaded, this code signing mechanism should be used to confirm the integrity of the application, and its mobile code as well as prevent malware from installing itself on a smartphone. This control is focused on user applications not preloaded factory software provided by the smartphone manufacturer.&lt;br&gt;3. Monitoring or scanning software should be capable of identifying and quarantining an infected smartphone, or wiping the company managed smartphone returning it to factory build state, or wiping it with poison pill encryption where the “poison pill” is reversible, i.e. when returned the IT department can restart the device and decrypt its storage with a special password.</td>
</tr>
</tbody>
</table>
| Information Security - Portable / Mobile Devices IS-32 | Policies and procedures shall be established and measures implemented to **strictly limit access to sensitive data from portable and mobile devices**, such as laptops, cell phones, and personal digital assistants (PDAs), which are generally higher-risk than non-portable devices (e.g., desktop computers at the organization’s facilities). | **Mobile Device Security and Management Controls**<br>1. **Mobile Computing: Access Control for Wireless Handheld Computing Systems or smartphones**<br>a. An appropriate account management team must provision the wireless handheld computing device or smartphone account on the push wireless email/wireless mobile message server, e.g. BlackBerry Enterprise Server (BES), Good Mobile Messaging (GMM) or Microsoft Exchange ActiveSync (MS EAS). [Where the wireless mobile message server acts as a proxy to the user’s email box via the permission granted through a service account on the wireless mobile message server.]
   2. **The Wireless handheld computing system or smartphone**<br>a. Must enforce passwords on all the devices that are part of Wireless Messaging Architecture.<br>b. Must not allow Users the ability to disable the password on the device or smartphone.<br>c. Must implement a password of at least 6 characters in length. Password complexity is recommended. |
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>d.</td>
<td>Should have a timeout interval [e.g. max of 15 minutes] for the smartphone to lock.</td>
<td></td>
</tr>
<tr>
<td>e.</td>
<td>Should have a setting interval [e.g. ‘no higher than 180’ for the number of days] after which the user will be prompted to change the smartphone password.</td>
<td></td>
</tr>
<tr>
<td>f.</td>
<td>Must provide System Administrators with over-the-air capability to delete the user, apply additional policies, and wipe data with verification of wipe, as necessary.</td>
<td></td>
</tr>
</tbody>
</table>

3. **Wireless handheld computing system or smartphone management ecosystem:**
   - a. Must include applying the password policies over-the-air to the devices.

4. **Wireless handheld computing system or smartphone data:**
   - a. Must be automatically wiped after a specified number of attempts [e.g. no higher than 7 attempts, as maximum number of attempts] and must confirm the over-the-air wipe.
   - b. Must be wiped when the smartphone is going out of service or being reassigned.
   - c. Smartphones should be integrated with backup and recovery services, [e.g. some smartphone platforms include ‘cloud’ backup storage].

5. In conjunction with the Company’s Compliance Program, internal ‘push wireless email’ infrastructure servers must be hardened according to standard security practices including maintaining current patches, removal of default passwords, periodic scanning and remediation of security vulnerabilities, along with periodic review of access privileges.

6. External ‘push wireless email’ servers must be hardened according to standard security practices including sustaining current patches, removal of default passwords, periodic scanning and remediation of security vulnerabilities, along with periodic review of access privileges consistent with the security requirements contained in the contract between the company and the 3rd party supplier.

7. Company Restricted and Sensitive Personal proprietary information must not be copied from
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| Resiliency - Business Continuity Planning | A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing and maintenance and information security requirements. Requirements for | primary sources and stored on smartphone removable or portable media (such as USB flash drives, memory sticks, or card) unless there is a business need and written approval is obtained (and retained) from a Company Executive with appropriate delegation of authority and, it is stored and/or transmitted encrypted, except where:  
(a) the media remains in a Company’s controlled space as part of a documented business process,  
(b) individual customer information is shipped to a customer on electronic media,  
(c) there is a business need to transfer data between Company locations or storage of backups from official company data centers,  
(d) the approved Smartphone removable or portable media [e.g. memory card] containing proprietary information:  
- Must either be kept in the direct supervision of the custodian or physically secured from unauthorized access (e.g. in a locked office, desk, or filing cabinet), and  
- Must not leave the direct supervision of the custodian when traveling on public transport (e.g. must not be placed in taxi trunk/boot, bus hold/baggage storage, checked-in on an airplane). |

1. Business Continuity planning to sustain or recover end-to-end Mobile service from Cell Tower radio access network (RAN) to Data Center or Cloud Computing should include:  
(a) a managed process established throughout the organization that addresses the information security requirements needed for the organization’s business continuity.  
(b) identification, along with the probability and impact of events that can cause interruptions to business and their consequences for information security.  
(c) Development and implementation of plans to maintain or restore operations and ensure availability of |
<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| business continuity plans include the following:  
  • Defined purpose and scope, aligned with relevant dependencies  
  • Accessible to and understood by those who will use them  
  • Owned by a named person(s) who is responsible for their review, update and approval  
  • Defined lines of communication, roles and responsibilities  
  • Detailed recovery procedures, manual work-around and reference information  
  • Method for plan invocation | information, applications and equipment at the required level and in the required time scales following interruption to, or failure of, critical business processes.  
(d) a single framework for business continuity plans to ensure that all plans are consistent, re: addressing information security requirements, and establishing priorities for testing and maintenance. | |

**Resiliency - Business Continuity Testing**

**RS-04**

Business continuity plans shall be subject to test at planned intervals or upon significant organizational or environmental changes to ensure continuing

1. Business continuity plans should be tested and updated regularly to ensure that they are current and effective.

**Security Architecture - Data Security / Integrity**

**SA-03**

Policies and procedures shall be established and mechanisms implemented to ensure security (e.g., encryption, access controls, and leakage prevention) and

**Data Controls**

1. Application Data Integrity for Wireless Handheld Mobile System or Smartphone

a. Based on data sensitivity, application data on a smartphone must be stored in local protected and/or encrypted storage, local key store, local file system, local nonvolatile memory, and/or local database et al and must be encrypted using industry standard encryption algorithms.
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| integrity of data exchanged between one or more system interfaces, jurisdictions, or with a third party shared services provider to prevent improper disclosure, alteration or destruction complying with legislative, regulatory, and contractual requirements. | b. A mobile application’s private data must be protected against unauthorized access.  
c. Passwords, private keys, and other confidential information must be stored in protected storage on the smartphone and encrypted. The password used to gain access to the protected information must not be stored on the smartphone.  
d. Application settings and provisioning data must only be accessible to the application and smartphone management components.  
e. Access, including read, write and update, of a smartphone PIM [Personal Information Manager] local address book, inbox, calendar, memo pad and other "storage" oriented applications should be subject to user control.  
f. Access to smartphone run time information, including but not limited to smartphone location information, subscriber MSISDN [Mobile Subscriber Integrated Services Digital Network Number], subscriber IMSI [International Mobile Subscriber Identity], device IMEI [International Mobile Equipment Identity], GPS [Global Positioning System] or location based data, etc, are subject to user control.  
g. Over-the-air wipe of smartphone or application data [i.e. returning it to factory build state] on a lost or stolen smartphone based on application level identification, subscriber MSISDN, and/or device IMEI must be supported and must be executed “silently” and be made uninterruptible by user interaction.  
h. Sandboxing: Application settings and provisioning data must only be accessible to the application and its corresponding smartphone management components. The data must be protected against access by other mobile applications. When shared with other applications, the data must continue to be inaccessible to unauthorized applications. Data that is private to a specific user or user session must only be accessible to that specific user or session. |
<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Architecture - Application Security</td>
<td>Applications shall be designed in accordance with industry accepted security standards (i.e., OWASP for web applications) and complies with applicable regulatory and business requirements.</td>
<td><strong>Application Controls</strong>&lt;br&gt;1. Applications must not contain “back-door” code that allows privileged access that bypasses the identification and authentication processes.&lt;br&gt;2. Encryption keys and passwords should be coded into mutable primitive arrays, not immutable objects. The arrays should be zeroed out before freeing for garbage collection e.g., Java coders should use character arrays, not String objects to store sensitive data. And those arrays should be zeroed out in finally clauses, prior to garbage collection. [This will reduce the chance of an attack on the memory of the device revealing sensitive information].&lt;br&gt;3. Authorization logic must be carefully designed to prevent escalation of privilege attacks. All architecture patterns (especially web solutions) should apply access-control filters to provide fail-safe access controls.&lt;br&gt;4. Application Packaging Security&lt;br&gt;a. Only the company authorized release version of the mobile software should be used in production.&lt;br&gt;b. The release version of the smartphone software should be code signed by the company, or company approved provisioning entity, such as Apple iTunes, where applicable.&lt;br&gt;c. Mobile software developed using interpreter based languages, e.g. J2ME, .NET, should be obfuscated to prevent hackers from leveraging the implementation logic and finding ways to attack through reverse engineering.&lt;br&gt;d. Privilege manifest, i.e. privileges and resources that a mobile executable requires for normal execution should be clearly specified in the release package.&lt;br&gt;e. A mobile application should be able to be hidden, be minimized, be paused, and be stopped and resumed to save smartphone power and for the courtesy of other applications on the smartphone.&lt;br&gt;5. Company should test all enterprise use mobile applications, especially if they access company data.</td>
</tr>
</tbody>
</table>
Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| **Security Architecture - Data Integrity** | Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data. | **Data Controls**

1. Data input must be validated from non approved sources (client applications, interfaces, databases, configuration, data and property files), for size, type, quantity, and permitted range of values, before the data values are used for computations. |

| **Security Architecture - Wireless Security** | Policies and procedures shall be established and mechanisms implemented to protect wireless network environments, including the following:

- Perimeter firewalls implemented and configured to restrict unauthorized traffic
- Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, SNMP community strings, etc.).
- Logical and physical user access to wireless network devices restricted to authorized personnel | **Network Level Controls and Protections**

**1. Mobile Computing: Connectivity**

a. The connection(s) between company systems/smartphones and any vendor systems must go through a company firewall/security gateway and must use a secure connection Secure Socket Layer [SSL].

b. End-to-end VPN access through a Virtual Private Gateway (VPG) should be used for data protection when connecting a VPN enabled smartphone to a cloud based application.

c. HTTPS should be used between mobile applications and web servers to protect the data stream, regardless of whether the data flows over the 3G network, transits the Internet, or utilizes WiFi connectivity where warranted by data sensitivity. |

**Application Control**

**1. Application Transport Security**

The available ‘network’ transport type can be WLAN, GSM/GPRS/EDGE/UMTS, Wi-Fi, WiMax, Bluetooth, Infrared, USB, etc. Each transport may be capable of voice, data and/or signaling transmission. Further each transport may implement one or more transport-level [protocol] stacks, e.g. TCP/IP, SMS, IMS, WAP, etc.

**The requirements for transport security in the context of mobile applications are:**

a. Explicit user confirmation is required before binding and connecting to mobile system network transport to exchange data with external peer applications. |
<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
</table>
| • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network. | b. The application must use only those transports authorized for the application to bind and connect to external applications, devices or systems.  

c. The connecting peer must be authenticated at the transport level before accepting connections. Methods may include Bluetooth authentication, WiFi authentication, verifying SSL server certificates, verifying IP address range, or using IPSec.  

d. A mobile application must not act as a “relay” to inter-connect the Company Intranet with the public cellular network, local area network, or personal area network, unless that functionality is specifically identified as a requirement.  

e. To reduce risk of Denial of Service (DOS) attacks the following should be implemented: setting timeout values on receive and idle states, validating packet size and contents, validating transport parameters and content, limiting the number of concurrent connections from a peer, and limiting total concurrent connections.  

f. Secure transport, using TLS for example, must use industry standard encryption algorithms.  
g. Applications that use broadcast transports (SMS, MMS, IMS) must implement a harassment detection and prevention mechanism. |

2. Application Protocol Security  
A protocol is defined when a mobile application needs to communicate with other applications to exchange application specific information. The application(s) that a mobile application interacts with can be local on-smart device applications, or remote applications with connectivity to the mobile application.  

a. The integrity of the protocol must be protected against man-in-the-middle and denial of service attacks.  

b. Packet level integrity must be provided using industry standard encryption algorithms.  

c. The confidentiality of any proprietary information must be protected against eavesdropping during transmission.  

d. Since Interaction with on-platform mobile applications (email, SMS, mobile browser, etc.) can cause privacy concerns and even fraud, this interaction
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>must be subject to explicit confirmation control based on the sensitivity of data. Interaction includes startup, shutdown, invocation, enable, disable, and exchange of information with other applications on the mobile systems.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e. Applicable, mutual authentication of peer applications must be conducted before actual exchange of data begins.</td>
</tr>
</tbody>
</table>

### 3. Application Identification

a. Each user or smart device must be identified uniquely and an identifier can belong to one and only one user or device in a mobile application name space.

### 4. Application Authentication

a. Authentication credentials (Passwords, PINS, passphrases, password hints) must be encrypted in storage and in transit, and be masked when displayed.
b. Authentication logic should never need to read a plaintext credential from storage; logic should always hash a credential entered by the user, and compare that value to the hashed stored value.
c. For Digital Certificates:
   - There must be a revocation process for certificates that have been compromised.
   - Expired or invalid certificates should not be used.
   - Owners of certificates must keep their certificates up to date, and not use out of date certificates.
   - All public key infrastructures must be authorized by the Company.

### 5. Application Accountability

a. Mobile applications should include audit log functionality.

### Network Level Controls and Protections

1. Bluetooth Security

   a. Bluetooth security must protect against the following:
      - Sniffing communication to capture authentication and encryption keys.
      - Device pairing initiated by an unauthorized source.
      - Unauthorized access or use of a shared service.
      - Use of weak authentication credentials.
      - Loss of the integrity and confidentiality of data being transmitted and stored.
      - Loss or theft of a Bluetooth device.
<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Wireless LAN Security</td>
<td>Mobile code shall be authorized before its installation and use, and the configuration shall ensure that the authorized mobile code operates according to a clearly defined security policy. All unauthorized mobile code shall be prevented from executing.</td>
<td>1. Application Controls</td>
</tr>
</tbody>
</table>

**SA-15**

- 2. Wireless LAN Security
  - a. Wireless Access Points (WAP) must be company authorized and WAP infrastructure [e.g. Access Points (APs), and Dynamic Host Configuration Protocol (DHCP)] must be hardened according to standard security practices including maintaining of current patches, removal of default passwords, periodic scanning and remediation of security vulnerabilities, along with periodic review of access privileges.

**Application Controls**

1. Common forms of mobile code are JavaScript, Java applets, ActiveX, and Flash. Each form of mobile code has a different security model and configuration management process. Web interactions rely on mobile code, either running on a Web server or Web browser. Web applications and mobile code are susceptible to four classes of attacks: browser-oriented, server-oriented, network-oriented, and user-oriented. Technical Controls that should be selected, deployed, and maintained as safeguards against these classes of attacks include but are not limited to:

   a. **Filters** that examine code at points of entry and block or disable it if deemed harmful.
   b. **Cages** that constrain the code’s behavior (e.g. privilege or function) during execution.
   c. **Signatures** that prevent code execution unless digitally signed by an approved source.
   d. **Proofs** that define properties of code and are conveyed with it, which must be successfully verified before the code is executed.

2. **Application Inventory and Revocation**
   - a. All software: OSs, applications, and tools on company registered smartphones must be company approved and 3rd party software must be properly licensed.
   - b. A company approved inventory of software must reside in a company managed software ‘store’ that includes software distribution or download to company registered smartphones, only.
   - c. Download of application software to company registered smartphones using sideload where a USB cable is tethered between a personal computer (PC) and the smartphone.
### Enterprise Mobility Security Standard (EMSS), Mobile Security Controls with Assessment Categories mapped to a subset of Control Areas from Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

<table>
<thead>
<tr>
<th>CSA-CCM Control Area &amp; Control ID</th>
<th>CSA-CCM Security Control Specification</th>
<th>Mapped Mobile Security Controls with Assessment Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>and a smartphone is allowed, e.g., Apple iOS applications via iTunes.</td>
</tr>
<tr>
<td>d.</td>
<td></td>
<td>Software configuration on the company registered smartphones must be monitored or scanned regularly. Any software identified as <strong>not approved</strong> must trigger one or more of the following actions depending on the vulnerability level created by the not approved application or tool:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Smartphone user notification,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Selective wipe of the offending application or tool,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Wipe with poison pill encryption where the &quot;poison pill&quot; is reversible, i.e., when returned the IT department can restart the device and decrypt its storage with a special password.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Administrator remote wipe of the smartphone returning it to factory build state.</td>
</tr>
</tbody>
</table>

### Machine to Machine (M2M) Security

a. M2m Wireless Device:
   Wireless should include
   - UMTS Encryption (UEA1)
   SIM Security should include
   - IMSI – IMEI tracking and change notification [where IMSI = International Mobile subscriber ID/network routing # and IMEI = International mobile Equip ID/mobile device ID]
   - SIM PIN locking
   - Solderable SIMs

b. Application Security should include
   - End to end VPN

c. Business Continuity should include
   - Redundant devices and connection paths.