

COTS SECURITY GUIDANCE

Summary of Security Requirements

CSEC Recommendation on the Management of Multi-Function Cellular Phones in the Government of Canada

CSG-12\S

August 2009

This page intentionally left blank.

Foreword

CSEC Recommendation on the Management of Multi-Function Cellular Phones in the Government of Canada is an unclassified publication, issued under the authority of the Chief, Communications Security Establishment Canada (CSEC).

Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSEC.

For further information, please contact CSEC's ITS Client Services area by e-mail at itsclientservices@cse-cst.gc.ca or call (613) 991-7654.

Effective Date

This publication takes effect on 08/28/2009.

*Carey Frey
Director, IT Security Industry Program*

© 2009 Government of Canada, Communications Security Establishment Canada
It is not permissible to make copies or extracts from this publication without the written consent of CSEC.

This page intentionally left blank.

1 Summary of Security Recommendations

This section summarizes recommendations for deploying and using smartphones in an Enterprise environment securely throughout their life cycle.

Planning, Design and Acquisition

The steps listed below should be part of planning, design and acquisition whether or not the enterprise or a service provider will own and operate the smartphone network:

- Select system:
 - Choose the operating system and platform that offer the best combination of security features that will comply with the enterprise security policy.
 - Whenever possible, select FIPS 140-2 validated implementations with CSEC-approved cryptography.
 - Based on manufacturer documentation and specifications of security features, verify that security features are functional.
 - Select third party add-ons to augment operating system and platform security;
 - Decide which applications will be provided and how they will be delivered: ensure that applications are trusted and signed.
 - Select detection and prevention controls.
 - Include a centralized asset management platform in the design for policy enforcement and management of users and costs.
- Consider system features and functions that include network security elements such as two-factor authentication, firewalls, secure VPN, anti-virus software, integrity checking, intrusion prevention and detection; and strong password enforcement;
- A comprehensive threat and risk assessment will provide visibility to potential vulnerabilities and architecture and security safeguards can be adjusted accordingly; and,
- Document user responsibilities for smartphone use and for safeguarding enterprise assets: include appropriate uses, enablement of security features, reporting malware infections, loss or stolen devices, and return of smartphone at minimum.

Deployment and Management

The actions listed below will support continued security for the smartphone network and other enterprise IT such as e-mail servers:

- Establish a baseline inventory of smartphone assets and services;
- Enable centralized security management for operating system, platform and device security features to support the network security policy;
- Establish protocols for device return including inventory update, data overwrite or device destruction;
- Establish incident management and back-up and recovery of data for smartphones, including actions on report of lost or stolen devices and use of statistics on security incidents;
- Establish routines for updating smartphone operating system and applications;
- Test, certify and accredit the system;
- Prepare and deliver user security awareness and smartphone training sessions;
- Periodically review the effectiveness of security safeguards and revise the threat and risk assessment as required, particularly when threat environment changes and when the enterprise deploys new technology or implements other change; and
- Conduct periodic user awareness sessions and IT operational staff security training.

User Awareness

Users can contribute to or undermine security. Smartphone managers can educate users regarding their responsibilities for safeguarding enterprise assets by including the following information in awareness sessions:

- Physically protect the smartphone:
 - Report lost or stolen smartphone immediately and trigger remote wipe if it is enabled;
 - Keep the smartphone hardware token separate from smartphone and store it safely;
 - Evaluate risk vs benefit of taking the enterprise smartphone on personal vacation..

- Use security features:
 - Where technologically possible, encrypt e-mail while in transit;
 - Ensure automatic device lock is enabled;
 - Encrypt data stored on smartphone;
 - Change passwords in accordance with enterprise security policy;
 - Store sensitive data on sanitized removable media when travelling and store separately;
 - Use secure data wiping software to clear sensitive data;
 - Back up data; and
 - Keep security patches for applications and the operating system up-to-date.

- Access e-mail, shared files and shared databases servers safely:
 - Use a secure VPN for connection to the enterprise network;
 - Protect password from eavesdropping on unsecured links or shoulder surfing;
 - Do not share the password or token;
 - Save sensitive data to removable media and physically protect removable media;
 - Enable WPA2 when using Wi-Fi;
 - Disable HotSync/Active Sync when not in use; and
 - Avoid using the smartphone in the Public Zone.

- Procurement
 - Participate in PWGSC-led GC procurements for common/shared services by specifying requirements including security.

This page intentionally left blank.

Annex A: Glossary

The Third Generation Partnership Project (3GPP): a consortium of national standards bodies that developed the 3G Mobile System. The 3G Mobile System evolved from GSM core networks and their supported radio access technologies. (Source: <http://www.3gpp.org/>)

Ad hoc Network: a network that connects remote devices such as cellular telephones, laptops, and personal data devices by relying on a master-slave system that uses wireless links for communication between devices. The shifting network topology is the reason for calling this type of network *ad hoc*: the network maintains random network configurations rather than the fixed infrastructure of a conventional network. As devices move about in an unpredictable fashion, the master in an *ad hoc* network should establish and maintain relationships among devices, constantly reconfiguring the network to address the dynamic topology. (Source: U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology Special Publication 800-48, “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, November 2002.)

Authentication Factors: Authentication may consist of one, two or three factors as described below:

Something you know: a factor of authentication based on what a user knows, such as a password;

Something you have: a factor of authentication based on what a user has in their possession, such as a smartcard or token; and

Something you are: a factor of authentication based on what a user is, such as a physical attribute. Biometric devices use a physical attribute to authenticate a user.

(Source: W. Burr, D. Dodson, and T. Polk, “Electronic Authentication Guideline”, *NIST Special Publication 800-63*, April 2006).

Type	Example	Advantage	Disadvantage
Something you know	Password or PIN	Easy and inexpensive	Easy to guess
Something you have	Smartcard, token	Hard to compromise	Easy to lose or steal
Something you are	Biometric devices	Portable	Expensive to deploy

Table 1 Authentication Factors

Bluejacking: the use of a Bluetooth-enabled device to send unsolicited messages or vCards to other Bluetooth owners by exploiting a weakness in Bluetooth messaging options. The sender or bluejacker can use a smartphone, personal data device or laptop; the range varies with the device. Bluejackers often operate in crowded areas such as shopping centers or airports where the potential number of targets is high and the limited range of a device is not a major factor.

Bluesnarfing: the use of a wireless device for unauthorized access to information on another wireless device using a Bluetooth connection. While Bluejacking is relatively harmless, Bluesnarfing is a technique for stealing private information such as contact lists, e-mails and even videos. For Bluesnarfing to work, smartphones should be paired.

Bluebugging: the use of a specially designed software program, called Bluebug, to allow an attacker to use a victim's Bluetooth-enabled device to call the attacker's device so that the attacker can listen to the victim's smartphone conversations. New, more sophisticated Bluebugging tools permit the attacker to take total control of the victim's device, which means the attacker can use any function on the device.

Claimant: the device attempting to prove its identity in a Bluetooth authentication procedure, which uses a "challenge-response" scheme. The challenge-response authenticates devices by verifying the knowledge of a Bluetooth link key. See also **Verifier**. ((Source: U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology Special Publication 800-48, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", November 2002.)

Data Caging: a platform security technique that protects files from unauthorized access by storing files such as executables or resources in predefined directories that a limited number of applications can access. Only processes with the original application secure identifier can access such a directory.

Flash Key, USB key, or USB flash drive: a flash memory data device integrated with a universal serial bus (USB) interface. It provides fast, compact, removable, re-writable data storage.

Golden Master Configuration: the default enterprise software configuration template deployed with the smartphone. The template contains the latest enterprise approved and tested device settings and access control policies that adhere to the enterprise security policy.

IEEE 802.11i Standard: the international standard that defines the capabilities required to implement IEEE 802.1X on 802.11 networks securely, including a requirement for use of an EAP method to support mutual authentication, key management, and dictionary attack resistance. In addition, 802.11i defines the hierarchy for use with the TKIP and AES ciphers and a "four way" key management handshake that ensures that the station is authenticated to the AP and a back-end authentication server, if present. (Source: U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology Special Publication 800-48, "Wireless Network Security 802.11, Bluetooth and Handheld Devices", November 2002.)

Infrared (IR): electromagnetic radiation with wavelengths between that of visible light and that of microwaves. IR is suitable for short-range communication among computer peripherals, personal digital assistants and smartphones. These devices usually conform to standards published by the Infrared Data Association.

Malware: a blend of two words, “malicious” and “software”, used to describe a variety of hostile, intrusive, or annoying software or program code that infiltrates or damages a computer system. Viruses, logic bombs, Trojan horses, worms and rootkits are malware.

Pairing: a form of two-factor authentication that pairs a user’s smart card with the user’s PIN; or the procedure used when two devices that share a secret link key communicate for the first time. See **Verifier** and **Claimant**. (Source: U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology Special Publication 800-48, “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, November 2002.)

Personal information: “information about an identifiable individual that is recorded in any form”. (Source: *The Privacy Act*)

Private information: “(1) identifiable information about an individual and (2) business confidential information from an organization.” (Source: Treasury Board of Canada Secretariat, “Government On-line Certificate Policies 5/13”)

Public Zone: in the physical world, the public zone is “where the public has unimpeded access and generally surrounds or forms part of a government facility”. Examples include the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings. (Source: Treasury Board of Canada Secretariat, “Operational Standard on Physical Security”)

In IT security, the public zone “is entirely open and includes public networks such as the public Internet, the public switched telephone network, and other public carrier backbone networks and services. Restrictions and requirements are difficult or impossible to place or enforce on this Zone because it is normally outside the control of the GC as a system owner. The Public Zone environment is assumed extremely hostile.” (Source: Communications Security Establishment, “Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)”, June 2007.)

Reimaging: the act of reinstalling everything on a device. The process wipes all data and is irreversible.

Sanitization: the removal or wiping of data from magnetic media in a manner that reduces or eliminates the likelihood of data recovery. Sanitization is superior to reformatting. Selection of sanitization method reflects the sensitivity of the data: in order of effectiveness, degaussing, overwriting, and physical destruction are methods of sanitization.

Spoofing: an attack that uses sophisticated techniques to make an attacking computer appear to be a trusted user or machine by masquerading as the trusted entity; in this way, the attacker gains unauthorized access to a computer or a network.

Tethering: how a non-mobile device, such as a desktop, is connected to a mobile device, such as a personal digital assistant or smartphone, to give the non-mobile device access to wireless networks.

Token: a physical or software-based object provided to a user through a cryptographic method to authenticate securely to a device or network. The token may replace a password or PIN, combine with a

password or PIN, or use more sophisticated identifiers such as digital signatures or biometric images. A security token is usually tamper resistant.

Unlicensed Mobile Access: a wireless standard that provides users with access to mobile services over unlicensed spectrum technologies, including Cellular, Bluetooth and Wi-Fi. UMA allows users to freely roam and handover between different wireless interfaces such as going from cellular and transparently transitioning over to a Wi-Fi network. Users need a multi-mode smartphone and UMA enabled to accomplish this roaming and handover.

Verifier: the Bluetooth device that validates the identity of another device in a Bluetooth authentication procedure, which is a “challenge-response” scheme. The challenge-response authenticates devices by verifying the knowledge of a Bluetooth link key. See also **Claimant**. (Source: U.S. Department of Commerce Technology Administration, National Institute of Standards and Technology Special Publication 800-48, “Wireless Network Security 802.11, Bluetooth and Handheld Devices”, November 2002.)

Wireless Fidelity (Wi-Fi): the trademark name that the Wi-Fi alliance uses for devices that it tests and certifies as correctly implementing IEEE 802.11 standards for wireless local area networks. Certified devices are compatible.

Zombie Computer: a computer that a hacker, virus or other malware has compromised so that it is remotely controlled to perform tasks without its owner’s knowledge.

Annex B: Cryptographic Algorithms

Smartphones may use a wide range of cryptographic algorithms. It is important to verify whether the algorithms are

- CSEC-approved as listed at <http://www.cse-cst.gc.ca/its-sti/services/crypto-services-crypto/ca-ac-eng.html>; and
- Implementation in the smartphone is FIPS 140-2 validated.

Using approved, FIPS 140-2 validated implementations of evaluated algorithms will ensure that the smartphone has strong cryptography to protect data and communications. Table 2 lists the cryptographic algorithms discussed in this document and their usage.

Algorithm	Functions	Usage
A3	Authentication	GSM
A5	Encryption	GSM
A8	Key generation	GSM
AES	Encryption	Applications over Bluetooth, Mail, Secure browsing, Wi-Fi
CAVE	Authentication and Key generation	CDMA
CMEA	Encryption	CDMA
COMP 128	Authentication and Key generation	GSM
E0	Encryption	Bluetooth
E1	Authentication	Bluetooth
E21	Key generation	Bluetooth
E22	Key generation	Bluetooth
E3	Key generation	Bluetooth
EAP	Authentication	Wi-Fi, Authentication into Enterprise domain
ORYX	Encryption	CDMA
TKIP	Encryption	Wi-Fi

Table 2 Summary of Cryptographic Algorithms

The following sections describe the cryptography used for Cellular, Wi-Fi, and Bluetooth communications.

Cellular

Researchers designed all of the CDMA and GSM cryptographic algorithms in a private environment, which did not permit public scrutiny. With time, however, the public discovered these algorithms and cryptographic analysts published weaknesses. The CDMA and GSM design community created newer versions of the algorithms to strengthen the security.

GSM: GSM uses the A3 algorithm for authentication and the A8 algorithm for key generation. Both algorithms reside in the SIM card. Most carriers use COMP128 as the implementation algorithm for both A3 and A8. The most recent version of COMP 128 is COMP 128-3, as earlier versions were weak. The latest COMP 128 algorithm has not undergone cryptanalysis, however.

The GSM network uses the A5 algorithm for encryption. European systems use A5/1 but North American systems use a weaker version, called A5/2. Hackers have broken both algorithms; neither is secure. A third revision, A5/3, is considered strong encryption but will only be deployed with the 3GPP networks, UMTS. Mobile devices have this algorithm embedded within the smartphone's firmware or hardware.

CDMA: A CDMA smartphone comes with a 64-bit authentication key (A-Key) and an Electronic Serial Number (ESN) programmed into the mobile. The mobile creates a "Shared Secret Data" (SSD) using the A-Key and other inputs into the Cellular Authentication and Voice Encryption (CAVE) algorithm. The SSD contains 128 bits that form a 64-bit SSD_A key that creates authentication signatures, and a 64-bit SSD_B key for generating encryption keys that provide voice and message confidentiality. Carriers share the SSD with other carriers when the user roams in another network but generate a new SSD once the mobile returns to the home network. The CAVE algorithm generates an 18-bit authentication signature using the SSD_A and a random broadcasted number.

For encryption, the CAVE algorithm and the SSD_B generate a key for encrypting signalling traffic using the Cellular Message Encryption Algorithm (CMEA). To encrypt data messages and traffic, SSD_B and CAVE create another key, which inputs into the ORYX algorithm, protecting the data.

Wi-Fi

Authentication in a Wi-Fi network uses the IEEE 802.1X, based on the Extensible Authentication Protocol (EAP). EAP has many different versions depending on what type of login credentials an enterprise uses: LEAP, PEAP, EAP-TLS, EAP-TTLS, EAP-FAST, or EAP-SIM. The choice depends on authentication credentials: these should consist of a user name combined with an authentication factor(s), i.e. something you know, something you have, and/or something you are.

Bluetooth

The pairing process allows two Bluetooth devices communicating with each other to associate themselves and generate a shared link key, which the devices use in further communications. The link key uses the initialization key, master key, unit key, or combination key depending on the implemented application on the devices trying to communicate. The E21 algorithm generates the unit and combination keys while the E22 algorithm generates the initialization and master keys. With a Bluetooth link key and the E1 algorithm, the verifier will challenge the claimant to ensure the claimant possesses the same-shared link key. If authentication fails, the verifier will wait before processing a new request to reduce exposure to a brute force attack. Once the paired devices establish the link key, the devices establish a session encryption key using the E3 algorithm to protect traffic. Encrypted traffic uses the E0 encryption algorithm.

The main weaknesses in legacy Bluetooth specifications stem from the pairing process, which uses a 4-digit PIN, from the sharable link key, and from passive eavesdropping on clear text information. Fifty per cent of the time, the PIN is simply '0000' and 4-digits do not create enough possible combinations. Since one device can share the same link key with many other devices, a previously paired device can calculate the encryption key between the owner of the link key and another device.

Bluetooth 2.1 designed a new pairing process called the Secure Simple Pairing (SSP) process, which fixes previous weaknesses and adds new security functionality. SSP simplifies user interaction and protects against passive eavesdropping by creating four association models. These association models use Elliptic Curve Cryptography to generate the link keys.