Security Considerations for Operational Software for Software Defined Radio Devices in a Commercial Wireless Domain

DL-SIN
SDRF-04-P- 0010-V1.0.0

(Formerly SDRF-04-A-0010-V0.0)

27 October 2004

Executive Summary

Wireless communications security in general is a subject of high interest; more specifically, security issues related to reconfigurable wireless devices. Evidence of this is provided by the extensive list of references and the list of other sources of information contained in this document. This document attempts to clarify the security issues for operational software by providing a detailed description of the operational software security requirements and by introducing a security reference model.

The scope of the document includes relevant aspects of operational software security provisioning and configuration for software defined radio (SDR) devices, including software/firmware download, storage, installation, and instantiation (DSII). The scope of the document is end-to-end security for SDR devices and systems in the commercial wireless domain.[1]

Security issues for operational software (non-applications software) have many different perspectives, including:

- Type of software downloaded
- Involved organizational entities (e.g., manufacturer, operator/service provider, regulator, user)
- Type of device (e.g., security requirement differences between devices that operate in the licensed band and those that operate in the unlicensed band)
- Level of sophistication of the user
- Timeframe

The timeframe is a particularly important aspect — the SDR Forum defines the operational software download, storage, installation, and instantiation security issues in terms of near-term, mid-term, and long-term timescales.

Although numerous security technologies are relevant to operational software security, the SDR Forum believes that unresolved issues exist for both the near-term and mid-term.

Some of the near-term problems stem from the fact that some wireless devices are resource limited (e.g., processing power and memory limited). Clearly, for the near-term, the manufacturers will retain responsibility for the proper operation of their own wireless devices and the manufacturers are responsible for ensuring that their devices are in compliance with applicable regulations. Manufacturer, operator, regulator, and end user perspectives of requirements are provided in this document.

From a mid-term perspective, a number of security issues are related to the following concerns:

[1] Other domains for SDR devices are the military/defense marketplace and civil government marketplace (e.g., public safety). These domains may have similar or differing requirements with regard to security considerations for operational software download.

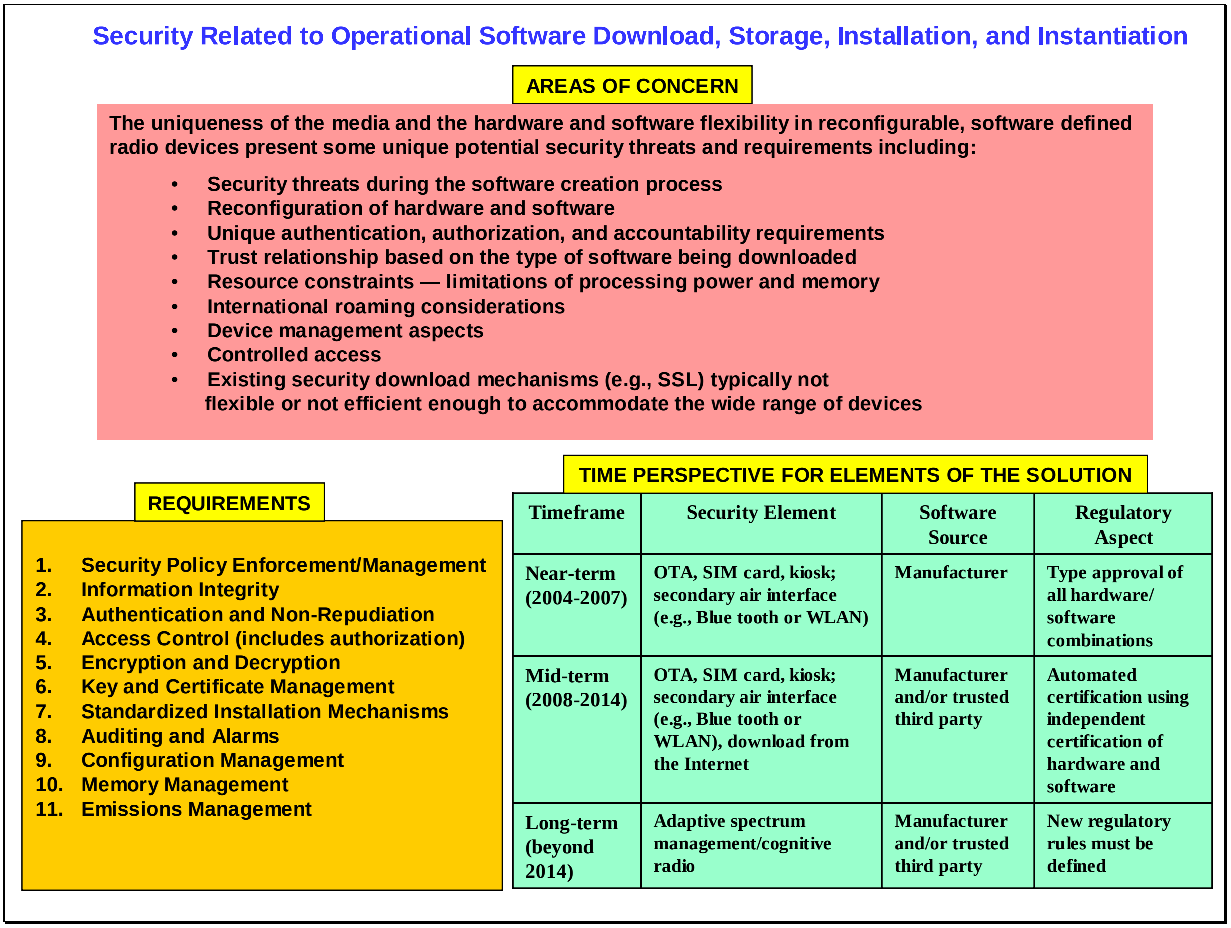
- Independent certification of hardware and software
- Validation and authorization of combinations of certified hardware and independently certified software
- Automatic calibration
- The availability of operational software from a trusted third-party vendor

This document also provides an introduction to some initial methodologies for solving the near-term and mid-term operational software download security issues. Particularly for the mid-term, some promising security methodologies currently are in the research and development (R&D) phase. Technologies being developed in various parts of the world hold promise for fulfillment of the mid-term requirements to the satisfaction of regulators as well as manufacturers and operators.

For the near- and mid-term, the SDR Forum asserts that both hardware and software are critical to the security solution, particularly for radio software security. The allocation of function between hardware and software as it applies to the security solution is based on the level of the protection required, which may range from solutions that must incorporate hardware to those for which a software mechanism alone is sufficient.

The long-term perspective is outside the scope of the present document.

The following figure summarizes key points in the document.



Security Related to Operational Software Download, Storage, Installation, and Instantiation

AREAS OF CONCERN

The uniqueness of the media and the hardware and software flexibility in reconfigurable, software defined radio devices present some unique potential security threats and requirements including:

- **Security threats during the software creation process**
- **Reconfiguration of hardware and software**
- **Unique authentication, authorization, and accountability requirements**
- **Trust relationship based on the type of software being downloaded**
- **Resource constraints — limitations of processing power and memory**
- **International roaming considerations**
- **Device management aspects**
- **Controlled access**
- **Existing security download mechanisms (e.g., SSL) typically not flexible or not efficient enough to accommodate the wide range of devices**

REQUIREMENTS

1. **Security Policy Enforcement/Management**
2. **Information Integrity**
3. **Authentication and Non-Repudiation**
4. **Access Control (includes authorization)**
5. **Encryption and Decryption**
6. **Key and Certificate Management**
7. **Standardized Installation Mechanisms**
8. **Auditing and Alarms**
9. **Configuration Management**
10. **Memory Management**
11. **Emissions Management**

TIME PERSPECTIVE FOR ELEMENTS OF THE SOLUTION

Timeframe	Security Element	Software Source	Regulatory Aspect
Near-term (2004-2007)	OTA, SIM card, kiosk; secondary air interface (e.g., Blue tooth or WLAN)	Manufacturer	Type approval of all hardware/ software combinations
Mid-term (2008-2014)	OTA, SIM card, kiosk; secondary air interface (e.g., Blue tooth or WLAN), download from the Internet	Manufacturer and/or trusted third party	Automated certification using independent certification of hardware and software
Long-term (beyond 2014)	Adaptive spectrum management/cognitive radio	Manufacturer and/or trusted third party	New regulatory rules must be defined

Table of Contents

List of Figures

List of Tables

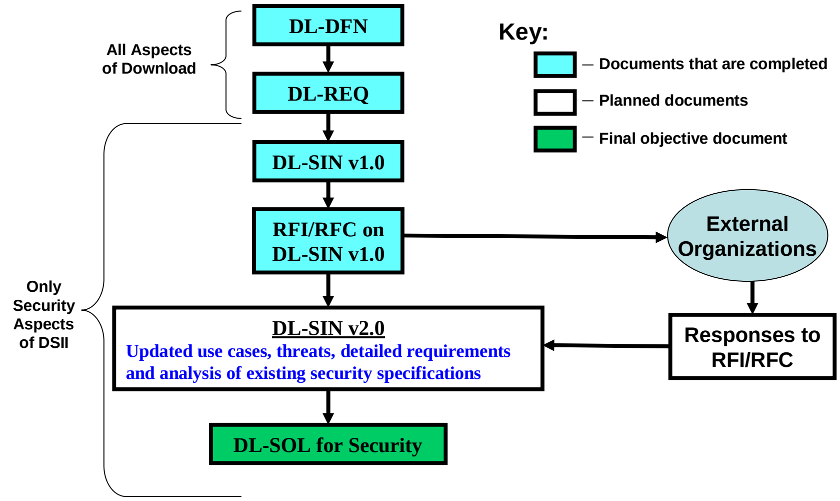
Preface

This document provides detailed security requirements for operational software provisioning and configuration including download, storage, installation, and instantiation (DSII). The document also provides an introduction to some promising technologies that have been proposed for meeting those requirements. The requirements and survey of existing security methodologies contained herein are differentiated by the unique perspectives of manufacturers, operators, regulators, and end users. Each of these views contributes to the end-to-end system (network) perspective used in this document to derive the requirements as well as some example methods for satisfying them. The document also includes a summary of work in the area of operational software security issues being performed by recognized Standards Development Organizations (SDOs), partnership projects (e.g., 3GPP and 3GPP2), technology proponents, and other commercial organizations (such as the Open Mobile Alliance) as well as from the research and development community.

This document is one in a series of SDR Forum documents on radio software download. Commercial wireless is the focus of the current deliverables in this software download series of documents. The other documents in this series are:

- DL-DFN: Overview and Definition of Radio Software Download for RF Reconfiguration in a Technical and Regulatory Context, SDR Forum Document SDRF-02-A-0002V0.0, August 2002.
- DL-REQ: Requirements for Software Download for RF Reconfiguration, SDR Forum Document SDRF-02-A-0007V0.0, November 2002.
- DL-SOL: Methods to Satisfy Security Requirements for Operational Software Download, Storage, Installation and Instantiation.

The relationships among these documents are seen in the figure below. DL-DFN, the overarching document, provides a foundation for the remaining documents and drives their development. DL-REQ provides a high-level functional description of radio software download requirements for RF reconfiguration. The present document is DL-SIN v1.0. Ultimately, DL-SOL will provide the set of solution methods to satisfy the security requirements stated in DL-SIN.



Relationships among SDR Forum DSII Documents

Definitions

Applications software: Software that instantiates service enablers deployed by service providers, manufacturers or users. Individual applications will often be enablers for a wide range of services.

Authentication: The ability to validate the source of a message (i.e., that it was transmitted by a properly identified sender and is not a replay of a previously transmitted message, such as. NIST SP 800-21 [NIST, 1999], which refers to NIST SP-800-2). The broadest definition of authentication encompasses identity verification, message origin authentication, and message content authentication (NIST SP 800-21 [NIST, 1999], which references FIPS Pub 190).

Authorization: Verification that the user is permitted to access the data or to utilize a communications capability [SDR Forum, 2002b].

Availability: A requirement intended to assure that systems work promptly and service is not denied to authorized users. (NIST SP 800-12, NIST Security Handbook [NIST, 1995]).

Certificate: A data structure that binds a public key to an entity in an authentic way [Mitchell, 2004, p. 13].

Certification Authority: A trusted entity that issues and revokes public key certificates and certificate revocation lists (NIST ITL Bulletin, Public Key Infrastructure Technology [NIST, 1997]).

Certificate Revocation List: A list of certificates that have been revoked. The list is usually signed by the same entity that issued the certificates. Certificates can be revoked for several reasons. For example, a certificate can be revoked if the owner’s private key has been lost or if the owner’s name changes. (NIST ITL Bulletin, Public Key Infrastructure Technology [NIST, 1997]).

Commercial Wireless Domain: In this document, the commercial wireless domain encompasses the wireless business marketplace generally referred to as cellular or PCS, or similar wireless systems such as wireless LAN, fixed wireless access, land mobile radio, or dispatch systems.

Common Criteria (CC): A multipart standard, meant to be used as the basis for evaluation of security properties of IT products and systems. The CC addresses protection of information from unauthorized disclosure, modification, or loss of use.

Cognitive Radio: A radio or system that senses and is aware of its operational environment and can dynamically, autonomously, and intelligently adjust its radio operating parameters so as to make best use of available spectrum and radio technology. (Note: This is a combination of the WP8A and WP8F definitions.)

Confidentiality: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes. (NIST SP 800-21 [NIST, 1995], which references FIPS Pub 140-1).

Device: A voice or data terminal that uses a wireless bearer for data transfer. Device types may include (but are not limited to) mobile phones, PDAs, laptop computers, PMCIA cards, unattended data-only devices and smart cards if associated with the foregoing. Adopted from the Open Mobile Alliance Device Management Requirements document [OMA, 2003a].

Device reconfiguration: Refers to cases in which the parameters or the software is changed or the hardware itself is reconfigured. In general, device reconfiguration includes reconfiguration of the radio interface, protocol stacks, plug-ins to support different types of content (e.g., voice and video codecs) and applications. Security issues are in the control of the reconfiguration [Falk et al., 2002].

Device management: Management of the device configuration and other managed objects of devices from the point of view of the various management authorities. Device management includes:

- Setting initial configuration information in devices
- Subsequent updates of persistent information in devices
- Retrieval of management information from devices
- Processing events and alarms generated by devices

Adopted from the Open Mobile Alliance (OMA) Device Management Requirements document [OMA, 2003a]. Security is an integral part of all device management operations.

Firmware: Software stored in read-only memory (ROM) or programmable ROM (PROM). Easier to change than hardware but more difficult than software stored on disk. Firmware is often responsible for the behavior of a system when it is first switched on. A typical example would be a “monitor” program in a microcomputer that loads the full operating system from disk or from a network and then passes control to it. (Free On-Line Dictionary of Computing: http://wombat.doc.ic.ac.uk/foldoc/)

Instantiation: Process of setting up for execution.

Integrity: The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner. (NIST SP 800-21 [NIST, 1999], which references FIPS Pub 140-1). Integrity can also refer specifically to fata integrity or system integrity:

- *Data integrity:* The requirement that information and programs are changed only in a specified and authorized manner (NIST SP 800-12, [NIST, 1995]).

- *System integrity:* The requirement that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system (NIST SP 800-12 [NIST, 1995]).

Management authority: An entity that has the right to perform a specific device management function on a device or manipulate a given data element or parameter. For example, the network operator, device manufacturer, enterprise, or device owner may have the authority or share authority for managing the device. Adopted from the Open Mobile Alliance (OMA) Device Management Requirements document [OMA, 2003a]

Media object: Information on a Web server that can be downloaded.

Middleware: Software that provides a link between disparate applications. Go to http://www.computeruser.com/resources/dictionary/definition.html?lookup=6325. Middleware in computing terms is used to describe a software agent acting as an intermediary, or as a member of a group of intermediaries, between different components in a transactional process. The classic example of this is the separation attained between the client user and the database in a client/server situation. http://www.wikipedia.org/wiki/Middleware.

Non-applications software: See operational software.

Nonce: In information technology, a nonce is a parameter that varies with time. A nonce can be a time stamp, a visit counter on a Web page, or a special marker intended to limit or prevent the unauthorized replay or reproduction of a file. Because a nonce changes with time, it is easy to tell whether an attempt at replay or reproduction of a file is legitimate by comparing the current time with the nonce. If it does not exceed it or if no nonce exists, then the attempt is authorized. Otherwise, the attempt is not authorized. (Source: searchSecurity.com Definitions; go to http://searchsecurity.techtarget.com/sDefinition.)

Non-repudiation: Positive verification of a sender's or receiver's participation in a transaction. [SDR Forum 2002b]. Non-repudiation of origin is protection against a sender of a message later denying transmission (NIST SP 800-21 [NIST, 1999], which references NIST SP-800-2). This service provides proof of the integrity and origin of data that can be verified by a trusted third party (NIST SP 800-21 [NIST, 1999], which references ANSI X9.31).

Operational software: All software other than the applications software. Operational software includes the operating system, drivers, radio software, and middleware (i.e., all software needed to support the applications on the wireless device).

Policy-based radio: A radio for which the range of operating parameters is governed by a predetermined set of policies which can be defined at the time of manufacture and/or set or modified by the user or network operator. [Note: WP8A definition]

Privacy: Often referred to as "confidentiality," this category usually refers to the assurance that other parties cannot access a user's personal information. In the case of SDR, however, privacy can apply not only to user data, but also to the executable software, which is the intellectual property of the equipment manufacturer or software developer. Encryption techniques may be used to prevent unauthorized parties from gaining access to private user data, or to proprietary software [SDR Forum, 2002b].

Protection Profile: An implementation-independent set of security requirements.

Public key certificate: An electronic record that binds a public key to the identity of the owner of a public-private key pair and is signed by a trusted entity [NIST, 1997].

Radio software: See definitions in SDR Forum [2002a].

Reconfiguration: Reconfiguration is the change of operational software (programs, parameters, or the software aspects of the processing environment) or hardware (e.g., FPGAs). Reconfiguration can concern arbitrary parts of communication equipment such as protocol stacks, plug-ins to support different types of content and applications, and the hardware configuration.

Reconfigurable radios: Radios whose hardware configuration and software can be changed under software control. (Note: Reconfiguration control of such radios may involve any element of the radio communication network.)

Sandbox method: A security method in which operational software runs in a restricted, controlled execution environment (i.e., a sandbox). The terms “sandbox” and “sandbox security” have specific meanings in the Java development environment (see, for example, http://www.itsecurity.com/dictionary/dictionary.htm). In this document, the “sandbox” term is used more generally but the concept is the same as it is used in the Java community. The term “sandbox” as used herein is similar to the 3GPP Mobile Execution Environment concepts of “domains” and “classmarks” (see Appendix C, Section C.4.2).

Scripted Attack: Security threat based on the use of shell scripts that use attack methods in series. The combination of attack methods has proven more powerful than using any particular hacker package for the following reasons: (1) information gained from the previous method can be used by subsequent methods; (2) the order of attack can usually be randomized to some extent, which makes automatic detection of an attack more difficult; (3) it allows the hacker community to more easily build upon prior successful attacks/work; (4) it provides a ready-made means for inexperienced hackers to start performing very strong attacks.

Security: Security herein refers to computer security or mobile telecom security:

- *Computer Security:* The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) (NIST SP 800-12 [NIST, 1995]).
- *Mobile Telecom Security*: The ability to prevent fraud as well as the protection of information availability, integrity, and confidentiality [3GPP, 2004].

Security Policy: A set of criteria for the provision of security services (ISO/IEC 7498-2-1989).

Security Target: A document of the Common Criteria that presents the implementation-dependent set of security requirements and specifications used as the basis for evaluation of the identified product or system.

Software defined radio: Two definitions of software defined radio are relevant, depending on context:

- *Technical definition of software defined radio:* Software defined radios are elements of a wireless network whose operational modes and parameters can be changed or augmented, post-manufacturing, via software. Software defined radios are a collection of hardware and software technologies that enable reconfigurable system architectures for wireless networks and user terminals [SDR Forum, 2002a; SDR Forum brochure].
- *Regulatory Definition of Software Defined Radio*: A radio that includes a transmitter in which the operating parameters of frequency range, modulation type, or maximum output power (either radiated or conducted) can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions. This definition was not intended to cover devices that use software simply to control functions such as power or frequency within a range approved by the Federal Communications Commission. Receivers also are not covered under this definition [FCC, 2001].

Threat: A potential violation of security (ISO/IEC 7498-2-1989).

Trusted Third Party: An organization or its agent that provides one or more security services and is trusted by other entities with respect to activities related to these security services. [ITU-T, 2003]

Trusted system operation: Confidence that software will execute in the device exactly as intended. SDR security will require some elements to be enforced by hardware measures (e.g., protected memory, which has both a hardware and software component). Such hardware measures are needed to ensure that there is a root security mechanism that cannot be modified by software changes. Trusted system methodology is expensive, however, and should probably be used only on high-end SDR devices [SDR Forum, 2002b].

Validation: The checking of integrity-protected data to detect loss of integrity.

Acronyms

3DES	Triple Data Encryption Standard
3GP	Third Generation Partnership Project
3GPP2	Third Generation Partnership Project 2
AAA	Authorization, Authentication, and Accountability
ACU	Automatic Calibration Unit
AMPS	Advanced Mobile Phone System
BE	Broadcast Encryption
CA	Certification Authority
CAA	Central Authorization Agency
CAMEL	Customized Application for Mobile Network Enhanced Logic
CAPP	Controlled Access Protection Profile
CCA	Covert Channel Analysis
CCRA	Common Criteria Recognition Arrangement
cdma2000	Code Division Multiple Access 2000
CE	Consumer Electronics
CEM	Common Evaluation Methodology
CEST	Center for Science and Technology
CPU	Central Processing Unit
CMRS	Commercial Mobile Radio Service
CRC	Cyclic Redundancy Check
CSE	CAMEL Service Environment
DLOTA	Download Over the Air
DM	Device Management

DRM	Digital Rights Management
DSII	Download, Storage, Installation, and Instantiation
E2R	End-to-End Reconfigurability (Project)
EAL	Evaluation Assurance Level
EMC	Electromagnetic Compatibility
ETR	Evaluation Technical Report
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FOTA	Firmware Over the Air
FPGA	Field Programmable Gate Array
FS	Functional Specification
GPRS	General Packet Radio Service
GPS	Global Positioning Satellite
GSM	Global System for Mobile Communications
HLBD	High-Level Block Diagram
HMAC	Hashed Message Authentication Code
HTTP	Hypertext Transfer Protocol
HW	Hardware
IDS	Intrusion Detection System
IEICE	Institute of Electronics, Information and Communications Engineers
IP	Integrated Project
ISO	International Standard Organization
ITU	International Telecommunication Union
JTRS	Joint Tactical Radio System
KMI	Key Management Infrastructure

LSPP	Labeled Security Protection Profile
MAC	Medium Access Control
MDS	Multimedia Distribution Service
MEMS	Micro-Electro-Mechanical System
MExE	Mobile Execution Environment
MIDP	Mobile Information Device Profile
MMU	Memory Management Unit
MPEG	Moving Picture Experts Group
MPHPT	Ministry of Public Management, Home Affairs, Posts and Telecommunications
MS	Mobile Station
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards And Technology
NPRM	Notice of Proposed Rule Making
NSA	National Security Agency
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OS	Operating System
OTA	Over-The-Air
OTAPA	OTA Parameter Administration
OTASP	OTA Service Provisioning
PC	Personal Computer
PCC	Proof Carrying Code
PDA	Personal Digital Assistant
PKI	Public Key Infrastructure
PP	Protection Profile

PSS	Peripheral-Sharing Switch
PV	Protection Vector
QoS	Quality of Service
RA	Regulatory Agency
RAM	Random Access Memory
R&D	Research and Development
RFI/RFC	Request for Information/Request For Comments
RM	Reconfiguration Manager
RMA	Reconfiguration Management Architecture
RSA	Rivest-Shamir-Adleman; a public-key cryptosystem developed by Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman in 1977 in an effort to help ensure Internet security
RSM	Radio Security Module
SCA	Software Communications Architecture
SCOUT	Smart User-Centric Communication Environment
SDO	Standards Development Organization
SDR	Software Defined Radio
SIG	Special Interest Group
SIM	Subscriber Identity Module
SSL	Secure Sockets Layer
ST	Security Target
STV	Security Threat Vector
TCAM	Telecommunication Conformity Assessment and Market
TCG	Trusted Computing Group
TELEC	Telecommunications Engineering Center
TOE	Target of Evaluation

TSG	Technical Specification Group
UEM	User Equipment Management
UID	User Identification
UIM	User Identity Module
UMTS	Universal Mobile Telecommunication System
USB	Universal Serial Bus
USIM	User Services Identity Module
VCE	Virtual Centre of Excellence
WCDMA	Wideband cdma
WLAN	Wireless Local Area Network
WPKI	Wireless (Application Protocol) Private Key Infrastructure
WWRF	Wireless World Research Forum

Security Considerations for Operational Software for Software Defined Radio Devices in a Commercial Wireless Domain

1 Introduction

The wireless industry companies who participate in the Software Defined Radio Forum desire standards to be developed for all aspects of operational software provisioning and configuration relevant to software defined radio devices utilized in a commercial wireless domain. In this document, the terms *provisioning* and *configuration* include all aspects of software/firmware download, storage, installation, and instantiation. Throughout this document, the acronym DSII is shorthand for identifying the download, storage, installation, and instantiation functionality. DSII does not include the actual execution of the software.

This document focuses only on the security aspects of operational software DSII. Other documents in the software download series focus on different aspects of software download to commercial wireless devices. The definition of operational software includes all software that exists within a wireless device that is not associated with application software. Examples of operational software include the operating system, device drivers, radio control software, and middleware (e.g., the execution environment software). This topic is explained in more detail in Section 2. The definition of a commercial wireless device includes voice or data terminals that use a wireless bearer for data transfer. Device types may include (but are not limited to) mobile phones, personal digital assistants (PDAs), laptop computers, PC add-in cards, unattended data-only devices, and smart cards if associated with the foregoing [OMA, 2003a].

The intention of this document is to provide a broad examination[2] of security requirements for operational software DSII for SDR devices and reconfigurable systems in the commercial wireless domain as well as an introduction to some security methodologies available to satisfy these requirements. The SDR Forum recognizes that there may not be one standard solution set for all hardware and software. For example, the solution for a smart phone may be different from that for an emergency responder radio. As a second example, a proprietary piece of software such as a driver may differ from middleware in regard to security requirements.

This document contains more than just the requirements for over-the-air (OTA) transmission encryption. It is a systemic examination of the end-to-end security requirements from a total systems or network point of view. Future versions of this document will include updated information on security methodologies available to meet these requirements, including references to existing standards and technical specifications developed by external fora as well as solution sets developed in response to requirements unique to software defined radio security. The composite solution sets will provide a complete description of the methods available to satisfy the detailed technical and regulatory requirements described herein.

[2] It is understood that a single document such as this treatise cannot cover every aspect of the broad and wide-ranging field of security aspects in wireless. This document should therefore not be viewed as an authoritative source outside of its immediate scope; it does not provide full and complete solutions.

This document addresses the following security issues:

- Security requirements for software DSII for commercial SDR devices with a primary focus on OTA download security requirements.
- A new security reference model that focuses on the SDR context.
- A description and analysis of existing standards that are applicable to meeting technical and regulatory security requirements.
- An introduction to possible methodologies to satisfy the requirements. This is not the definitive answer for security specifications that address all aspects of operational software security requirements — rather, it is an introduction to promising approaches. The definitive solution sets of available security technologies will be provided in the planned SDR Forum Document DL-SOL, "Methods to Satisfy Security Requirements for Operational Software Download, Storage, Installation, and Instantiation."
- Future technical- and regulatory-related work by the SDR Forum for operational software security.

Security requirements for commercial wireless networks are not static or unchanging; rather, the requirements continuously evolve. As new commercial wireless technologies are inserted into the marketplace, new threats also evolve. Therefore a timeframe to which this document applies will be defined as threats and solutions to the Third Generation (3G) wireless systems (referred to as IMT-2000 in the International Telecommunication Union). This document does *not* address issues related to so-called 4G or neXt Generation (XG) systems that are described in current literature [see Marshall, 2003, for example]. The concept of dynamic spectrum sharing between different networks and services is central to the XG communications networks vision. These types of networks may bring a new set of security concerns; however, this is outside the time scope of this document. Later versions may address these issues.

1.1 Informative Comment Regarding Compliance and Certification

The intent of this document is to suggest methods and provide guidance that does not restrict or limit further validation through formal security testing services. The current United States Information Processing Standards [NIST, 2002] specification of cryptographic methods and the international Common Criteria [ISO, 1999] security requirements were considered during the creation of this document. Manufacturers that implement formal cryptographic security testing shall be able to achieve those certifications without violating the requirements specified by the SDR Forum.

Requirements and methods described within this document should be considered only as guidelines to achieve compliance within the structure of the SDR Forum and do not provide a complete solution when applied to other testing profiles. Certification through a formal testing agency is not required to satisfy requirements of the SDR operational software download, storage, installation, and instantiation approach. One of the goals of this paper is to define a commonality of software DSII methodologies that will help achieve two capabilities, namely, security and interoperability. The latter is important to the cost considerations of implementing multitudinous different methodologies and concomitant inherent security risks for each device.

A tutorial overview of Common Criteria and Protection Profiles is provided in Appendix D.

1.2 Overview of the Document

This document begins with a high-level description of the commercial wireless security issues associated with commercial mobile wireless communications. This includes wireless communications systems used in both the licensed and unlicensed bands. Section 2 sets the framework by describing the unique security requirements associated with software download, storage, installation, and instantiation for SDR-capable devices. SDR Forum Documents DL-DFN, “Overview and Definition of Software Download for RF Reconfiguration” [SDR Forum, 2002a] and DL-REQ, “Requirements for Radio Software Download for RF Reconfiguration” [SDR Forum, 2002b] provide high-level definitions and functional requirements for software download. These functional requirements include:

- Download process requirements
- Requirements specific to the SDR device
- Requirements specific to the network supporting the download process

Section 3 provides a Security Reference Model. This model was developed to address the complex security information space.

Section 4 presents detailed technical operational software DSII security. These requirements include authentication, authorization, protection, and non-repudiation exchange. The authentication mechanism for some wireless devices is mutual authentication. However, devices such as wireless local area networks (WLANs) and wireless personal area networks, operating in the unlicensed spectrum, need only authentication of a valid manufacturer. The SDR device requirements include protected memory and reconfiguration management. The network requirements include network architecture. All of these functions and others described in SDR Forum Document DL-REQ [SDR Forum, 2002b] are relevant to mobile wireless security. However, the requirements described in DL-REQ, including the security requirements are very high-level requirements. It is the purpose of SDR Forum Document DL-SIN to expand on the security requirements by providing detailed technical requirements.

Numerous other standards fora, standards-related organizations, and wireless industry consortia are also doing work in the area of wireless communications security. Section 5 and Appendix B provide a survey and analysis of this work.

Section 6 provides an introduction to some of the proposed security solutions being investigated by the research community and other fora. Section 7 briefly describes the SDR Forum’s future work on operational software security. Sections 8 and 9 provide references and a list of other sources of information, respectively.

Appendix A presents a security structure developed by the SDR Forum and high-level security functional requirements associated with each element of that structure. Appendix B presents a survey of security activities in other fora that are relevant to operational software DSII security. Appendix C discusses specific threats and security objectives against reconfigurable systems.

Appendix D is a tutorial overview of Common Criteria and Protection Profiles. Appendix E presents terminology defined in Internet Engineering Task Force RFC 2119 (IETF RFC 2119 [IETF, 1997]), and Appendix F addresses the special case of security attacks on personal computers.

2 Defining the Problem

The security problem for operational software DSII for commercial SDR devices in a commercial wireless domain has several dimensions, including:

- *Type of operational software download*: Operating system, drivers, radio software, etc. Section 2.1 of this document elaborates on the types of operational software installed in typical commercial wireless devices. This document is not concerned about applications software download except for ensuring that:
    - applications software executable code and data cannot be loaded in an uncontrolled, inappropriate, or inadvertent manner into program and data memory reserved for operational software code and data memory, and
    - techniques that have been developed for applications software download security are examined to determine the extent to which they are applicable to, and adequate for, operational software download security requirements.
- *Involved organizational entities*: Manufacturer, operator/service provider, regulator, device owner, and user. Each of these entities has a different perspective of the security requirements for operational software download. The requirements from the perspectives of different organizational entities are provided in Section 5.2. The regulatory perspective of software download to reconfigurable devices is particularly important, and these perspectives may vary among different regions of the world.
- *Type of device*: Devices that operate in the licensed bands and devices that operate in the unlicensed bands. Depending upon the type of the device, the Internet model of software download from a trusted third-party vendor may be applicable (now or sometime in the future).
- *End-user sophistication*: The security requirements must take into consideration the fact that the user may be unsophisticated and totally uninvolved in the use of security technologies. Hence, the solution must be mostly automated with built-in security protections. This precludes most ad hoc procedures. It may also suggest orderly automatic self-updating. This is probably the case only for the operational software being considered in this document; applications software security measures may need to be handled differently.
- *Timeframe*: Near-term, mid-term, or long-term. In discussing security requirements and solutions, it is imperative that there is a common understanding of the timeframe being addressed.

2.1 Timeframe

The last topic in the above list, the timeframe, needs further elaboration in defining the security problem because security is not a static issue. The United States Federal Communication Commission (FCC) has clearly stated that software changes to software defined radio currently remain the responsibility of the device manufacturer [FCC, 2001, Appendix A, paragraph

2.1043]. Thus, for the near-term, all aspects of radio software download, including security, will be the responsibility of the manufacturer.

The timeframe aspect of the software download security issue is addressed in a paper presented at the Regulatory Conference in London in September 2003 [Moessner, 2003]. Moessner defined the following timeframes for regulatory steps:

- Short term: Type approval of terminals by regulatory agency
- Medium term: User can download air interface from any configuration software provider
- Long term: Adaptive spectrum management

Harada [2003] distinguished between security and regulatory requirements for the present, near future, and future in a fashion somewhat similar to that of Moessner. Harada’s definitions are:

- Present: The hardware and software for the radio are integral and inseparable.
- Near Future: The hardware and software for the radio are not integral. Software manufacturers and hardware manufacturers belong to a common company or a common alliance.
- Future: The hardware and software for the radio may come from different manufacturers; the hardware and software may be certified independently and integrated at the user device.

Because the technology for security must go hand-in-hand with the regulatory steps, the definitions for timeframes for security solutions used in this document (see Table 1) are adopted from a combination of Moessner’s and Harada’s definitions. The present version of this document addresses primarily the near-term operational software download security issues and required specifications; it also introduces mid-term issues and ongoing research that address those issues. Later versions of the document will address more specifically the solution sets needed to solve both the near-term and mid-term requirements in more detail.

Table 1 provides the SDR Forum view of near-term, mid-term, and long-term perspectives. Although this document primarily focuses on the near-term, Section 6 includes an introduction to some promising research that may lead to automated certification in the mid-term. The long-term perspective as defined in the table is outside the scope of this document.

In the near-term, type approval (or its equivalent) of all hardware/software combinations are mandated by the regulators, and the hardware/software is from a single company. For the near-term, even though many security technologies are available, there is a need to make available additional technologies that are sensitive to the difficulty associated with resource limited devices (limitations on processor power, memory, etc.). Mitchell [2004, p. 311] notes that complex security algorithms tend to use a lot of processor and memory, which may have an impact on battery life.

In the mid-term, as defined above, additional security attacks may need to be considered, and security measures will need to be more flexible. In addition, for the mid-term, the software source may be from a trusted third party, which leads to additional requirements such as multiple digital signatures, as noted by Harada [2003], Fitton [2002], and Cook [2003]. It also complicates the task for the regulators and leads to the need for some type of automated certification. Section 6 includes an introduction to some of the ongoing research that is applicable to the mid-term scenario defined in Table 1.

Table 1 Near-Term, Mid-term, and Long-term Perspectives of Security Issues Related to Operational Software Download, Storage, Installation, and Instantiation

Timeframe	Security Element	Software Source	Regulatory Approval
Near-term	OTA, SIM card, kiosk; secondary air interface (e.g., Bluetooth or WLAN)	Manufacturer	Type approval of all hardware/software combinations
Mid-term	OTA, SIM card, kiosk; secondary air interface (e.g., Bluetooth or WLAN), download from the Internet	Manufacturer, trusted third party	Possible automated certification based on independent certification of hardware and software. [See Harada, 2003]
Long-term	Adaptive spectrum management/cognitive radio	Manufacturer, trusted third party	New regulatory rules must be defined

The timing of trusted third-party software and/or automated certification may possibly be different for commercial wireless devices operating under the criteria of licensed spectrum and those operating under the criteria of unlicensed spectrum. The timeframes expressed may be shorter or longer, depending on the individual circumstances of the equipment hardware/software and the regulatory operating environment for licensed versus unlicensed spectrum. In the near-term, there will be new security concerns (such as software from third parties). This will not necessarily require new security solutions, but merely new ways of applying existing security solutions (e.g., multiple signatures).

2.2 Wireless Device Software Categories

In order to define the software download issues being addressed in this document, it is necessary to have a common understanding of the types of software typically installed in commercial wireless devices. Figure 1 depicts software categories that are typical of a third-generation commercial wireless device. The fundamental split shown in the figure is between “operational” software and “applications” software. Applications software download is being investigated by other standards fora. Therefore, security aspects of applications software download are not specifically emphasized in this document, although some application software security mechanisms may be discussed if they are also applicable to operational software download. It is important that download of applications software not be allowed uncontrolled, inadvertent, or inappropriate access to operational software executable code and parameter memory space within the commercial wireless device.

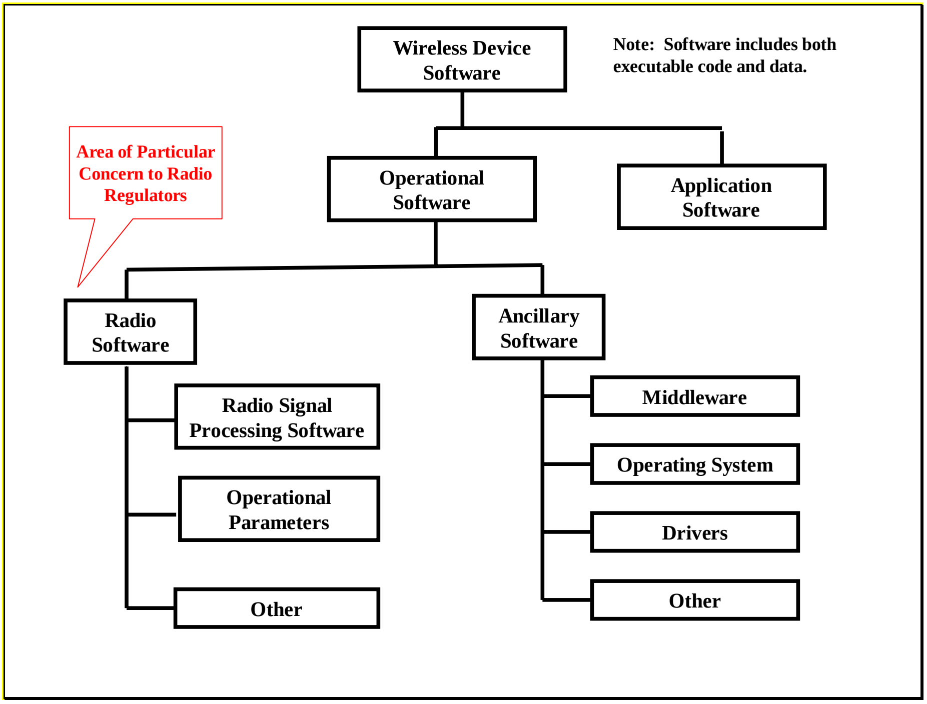


Figure 1. Software/firmware categories for commercial wireless devices

The focus of this document is on “operational software for commercial wireless devices” and is an expansion of the focus of previous documents in this series of SDR Forum documents on software download. The previous two documents in this series, Overview and Definition of Software Download for RF Reconfiguration, and Requirements for Radio Software Download for RF Reconfiguration [SDR Forum, 2002a, 2002b] focused on radio software for RF reconfiguration, as the titles of these two documents imply. However, as the Forum has moved forward, it has found the need to expand the focus of software download. To fully encompass the scope of RF reconfiguration, it is necessary to broaden the perspective because security involves all types of software in the wireless device. Operational software comprises all layers of software within the device except for the applications software; thus, security mechanisms must exist at each layer. Hence, the term *operational software* is introduced as defined below.

Operational software is software that includes applications, middleware, air interfaces, and the operating system. Operational software, sometimes referred to as non-applications software, is the executable code and data that define the functionality by which the wireless device receives or transmits signals, handles phone calls, authenticates information, and updates the software. Operational software also includes the operating system, drivers, and application interfaces. Operational software comprises the following main areas:

1. Radio Software

   Examples of Radio and RF functions include but are not limited to:

   - Update of parameter tables for handoff algorithms
   - Update of the state machine

    - New radio air interfaces
    - Vocoders
2. Ancillary Software
    - Middleware
    - Operating System and Drivers
        - Basic BIOS
        - Function of lowest of drivers

These types of software interact with each other to provide capability support and define device functionality. However, unique security requirements exist for each type of software, and these requirements are derived from different perspectives (regulator, manufacturer, operator/service provider, and user). Suzuki et al. [2003a] discuss a security architecture for software defined radio in terms of three security levels:

- Software security related to regulatory issues (Japanese Radio Law)
- Software security related to rights protection
- Software security related to data protection (user privacy).

Clearly, different security requirements apply to different types of software. As noted by Suzuki et al. [2003a], the organizational entity responsible for this security also is different for different types of software.

In the view of the SDR Forum, the software categories in Figure 1 map to the security stakeholders listed in Table 2. The areas in Table 2 that are shaded in gray are the areas addressed in this document. In general, user stakeholders are primarily concerned about applications software and privacy. User stakeholders generally do not have interest in operational software, except to the extent that operational software is a service/application enabler. Standards fora such as the Open Mobile Alliance are addressing security, digital rights management, and privacy issues associated with applications software download, that is, issues generally of interest to users and content providers [OMA, 2002, 2003d, 2003e, 2003g, 2004b]. Section 5 and Appendix B of this report provide information regarding the standards fora and technical specifications that have been developed that are relevant to each of the types of software identified in Table 2. Although regulators are directly interested in security related to radio software download, indirectly the regulators have concern about other types of software download to the extent that there must be assurances that the software-executable code and data cannot affect in an undesirable or inappropriate manner the execution of the radio software.

Table 2. Security Stakeholders for Various Types of Software for SDR Devices in a Commercial Wireless Domain

	Security Stakeholders for Various Types of Software Download				
Type of Software Download	**Regulators**	**Manufacturers**	**Operators – Service Providers**	**Content Providers**	**Users**
Application software		◆	◆	◆	◆
Radio software (including radio signal processing software and radio operational parameters)	●	●	●		
Middleware		●	●		
Operating system and drivers		●	●		
Legend: ◆ - a stakeholder; ● - covered in this document					

2.3 Security Requirements Overview

One measure of wireless communication system security is the consideration of how robust a system is under threat scenarios, evaluated against the following goals:

- Provide accurate delivery of content (data integrity) from authorized originators to intended recipients, and only to those recipients.
- Conform completely to the terms of its type approval license; this is an end result of security.
- Maintain a complete and accurate record and audit trail of interactions processed (non-repudiation). Identify the originator and receiver of every transaction with no opportunity for repudiation or misrepresentation.

Communications systems using a wireless link have the characteristic that interception of transmitted signals cannot be prevented. Data transmitted over a radio link can be assumed to be in the hands of anyone with a receiver. Further, system receivers must process received information to determine whether it is part of an authorized communication. So the system architecture must make provisions not only to deny access to information content but also to refuse to accept any unauthorized traffic.

A software defined radio has the characteristic that fundamental operating characteristics can be modified by introduction of new software. Provisions must therefore be made to ensure that:

1. Mechanisms are in place to either validate the source of the new software or restrict its access to radio functionality or both. Only trusted sources can unlock critical internal compartments (e.g., the radio software compartment).
2. Consideration must be given to the source of operational software to be downloaded. Trust in that source must be established by certification. An authentication chain must be

maintained back to its source, and source credentials must be checked prior to operational software installation. This process must also ensure that the model and version of the equipment to receive the new code is included within the scope of the certified validation testing. Bootstrapping issues related to authentication must be addressed.

3. Code compartmentalization must be maintained to constrain access to all code modules by only authenticated processes. For example, there must be no way that applications software code can access in an uncontrolled, inappropriate, or inadvertent manner memory space that stores radio software parameters or executable code. The use of security walls to restrict access is a critical security requirement. This requires the use of:

   a. File system security mechanisms and protected memory systems: There is some separation between file system security (protecting files stored in long-term storage such as a hard drive) and run-time production, which is memory protection of the random access memory. Software and hardware methods exist for both of these.

   b. Run time/execution environment security mechanisms (secure encapsulation of processes including the use of protected memory) — this ensures, among other things, that the security software that is running is the security software that should be running (i.e., an unauthorized security software module cannot be substituted).

   Typically an operating system has been used to provide 3a and 3b above. However, for some operational software DSII requirements, current operating system security is not sufficient. Memory management unit (MMU), or more generally protected memory, is an underlying mechanism applicable to those requirements stated above.

4. The communication path for the software from its trusted source to the target system must be valid and protected. During transmission, software is just like any other data, including money and cryptographic keys, needing a high level of transmission integrity. For instance, assuming there is a place in the device to securely store a public key, the download payload could be signed by using the associated private key. The device can check the integrity of the data by using this signature as well as determine (by implication) that the payload came from an authentic source (regardless of the path taken getting there). If the information relating to appropriateness of the payload to the device was also under this signature, then the device could reliably make that determination also.

5. Once the software has been received at the destination system, it must be placed in local storage and processed to make it ready for installation, including authentication measures appropriate to the needed level of security. It can then be installed in the system, and activated. Some provision for rollback to the previous software is often required to permit recovery from problems.

Two very important aspects of security are the following:

- The level of protection needed for operational (non-applications) software/firmware DSII is dependent on the type of software being downloaded. The level of protection and type of protection required are related to the perspective of the regulator, manufacturer, operator, or user. For example, the security of radio software download is paramount to regulators, but operating system software/firmware download is less critical to regulators as long as security walls prevent uncontrolled, inappropriate or inadvertent access to the radio software by non-radio software. The security of the operating system and drivers is very important to operators and manufacturers, however.

- The processing and memory requirements for providing security protection are very important. For example, handheld devices cannot afford the processing and memory capabilities that are implemented in devices and servers elsewhere in the network.

2.4 Unique Security Requirements for Operational Software for SDR Devices in a Commercial Wireless Domain

The "open platform" aspect of software defined radio is the foundation of the security concerns for operational software download. These open platform architectures are being implemented in the near-term as we have defined it. In the mid-term as we have defined it [similar to the definition of Moessner, 2003], there is a possibility of operational software being provided by trusted third-party vendors. Thus, the security concerns for the open platform become greater in the mid-term.

Errant executable code, whether due to human failure or malicious attack on the wireless system, must be prevented from affecting the radio parameters. As noted by Babb et al. [2002], security architectural issues are raised if one assumes that security threats can occur at run time and can affect any part of the terminal. This leads, potentially, to the requirement that a compartmentalization approach be taken to prevent radio parameter changes or radio executable software changes that cause the device to operate outside its authorized operational modes. This potentially implies international regulatory coordination for SDR-based wireless devices.

Threats to wireless systems vary from simple mistakes to carefully orchestrated attempted infiltration with extensive resources. Providing a very high degree of security to all aspects of system architectures is not economically feasible, so some technique for making system trade-off is necessary. An economic evaluation of threats is also in order. For example, an individual attempting to intercept funds transfers might apply significantly greater resources than someone attempting to garner free telephone calls. The economic analysis should be done for both the target and the attacker. In fact, the strength of a particular security system may be defined by the cost of failure.

The SDR Forum has the view that many security tools are already in place to meet the near-term security requirements for operational software DSII for SDR devices and supporting networks. However, additional, more efficient technologies are needed that are applicable to many commercial wireless devices, which have severe resource limitations. In general, many of the security requirements for operational software DSII for SDR devices in a commercial wireless domain are similar to other security requirements for other communication systems. The uniqueness of the media and the hardware and software flexibility in reconfigurable, software defined radio devices, however, present some special potential security threats and requirements, including:

- Security threats during the software creation process (e.g., disgruntled employee who inserts malicious code) and security threats to the software download distribution channels.

- Reconfiguration of hardware.
- Reconfiguration of all levels of the software stack.
- Unique authentication, authorization, and accountability (AAA) requirements as a result of reconfiguration capabilities of the device.
- Trust relationship based on the type of software being downloaded; radio software could be from a very restricted source(s), whereas applications software could be from a wider variety of sources.
- After download, storage, installation, and instantiation, if the security check fails, the device must still operate without further downloads – this is a restoration requirement.
- The processing power and memory of some commercial wireless devices present limitations.
- What must be agreed to regarding international roaming? Do devices that are capable of reconfiguration resulting from operational software download maintain their regulatory status in each regulatory jurisdiction?
- During DSII the device must still be capable of operating (e.g., handsets must be capable of emergency calls). There may be short intervals during installation, however, when radio functions may not be available.
- Due to processor and memory limitations of handsets, the database of information on, for example, the hardware and software capabilities of the SDR-capable device, versions of the software modules installed, the current device configuration, and subscription data must reside within the network.
- The ability must exist to restrict access to critical executable code and memory associated with the radio software through security walls.
- Existing security download mechanisms (e.g., SSL) are typically not flexible or not efficient enough to accommodate the wide range of devices and their security requirements and capabilities due to:
    - Resource (memory and processing power) diversity - some devices are resource rich and others are resource starved
    - Diversity in degree of liability when security is violated (e.g., ring tone glitch has less impact than modification of radio configuration)

2.4.1 Payload and Device Architectural Considerations that Impact Security Requirements

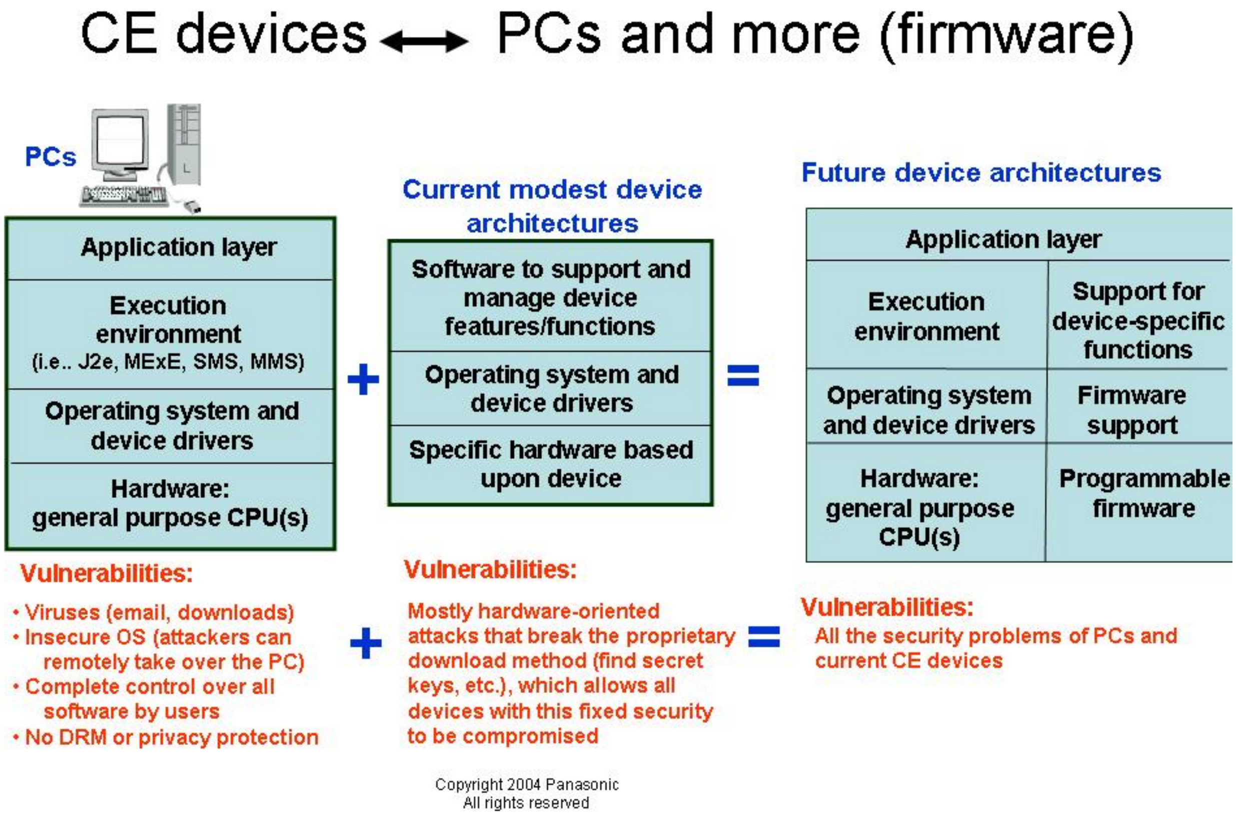
Security measures should match the security need. As discussed in the following paragraphs, the payload (i.e., the type of information to be downloaded, stored, installed, and instantiated) and the device architecture are two factors that greatly influence the level of security required. The examples presented here are just a few of many that illustrate the need for discerning the various security needs of SDR device payloads (Section 3 proposes a modeling system for further analysis).

SDR devices have several SDR-related payloads that, when successfully attacked, will lead to differing amounts and types of damage, such as interference, loss of private data, or removal of functionality. One can argue that all payloads should be treated equally, but the cost (in power and time) of strong security for all downloads is large, which means that more elegant solutions are needed. For instance, parameters that affect the operation of an SDR device will be downloaded far more frequently than those for new radio configuration software. In fact, as SDR devices become more and more “cognitive,” they will receive parameter updates from base-stations very frequently as they adapt to the ever-changing wireless environment. To ask for every parameter update to be signed and to then have the SDR device check the signature will lead to a very short battery life along with poor quality of service (QoS). Nevertheless, the parameters must be kept secure. The wireless channel and the parameter payload can be readily secured by using built-in security measures in today's and future wireless protocols (today's systems suffer from weak keys, but the next generation will not). The main problem is making sure they get installed/instantiated and that this location in memory (short- or long-term) is kept secure.

Current attacks on consumer electronics (CE) devices or personal computers (PCs) are based upon their software and hardware architecture. Therefore, the security mechanisms must reflect the SDR device's system architecture. Obviously, it must contain software definable components that determine how the transmitter will function. It must also be able to execute general telephony functions. In addition, many of these devices will be able to run email applications and surf the Web as well as handle other useful tasks. The ability to perform these tasks means that a general purpose CPU, RAM, and operating system (OS) will reside on SDR devices (as well as many future CE devices as the world becomes ever more interconnected). To reduce the overall cost of an SDR device, some, or all, of the telephony applications/procedures likely will be executed in the general-purpose processing area rather than special-purpose hardware. (Just how much will be moved to the general-purpose execution environment versus remaining in hardware specifically designed for telephony remains to be seen.)

The evolution from current cellular phones to very general purpose, reconfigurable SDR phones will most likely move in steps from the current specific designs to the general areas in future devices. This evolution of device architecture — a much more open architecture than found on current devices — will allow for such devices to be much more useful, user friendly, interconnected and reconfigurable, but it also opens a Pandora's box of new security threats to the SDR device world. Figure 2 depicts this trend and shows how future-generation SDR devices will be susceptible to many of the same security problems that current-day PCs face. Without the implementation of strong, robust security measures, SDR devices will be easily compromised and thus be a veritable plague upon the wireless airways.

Appendix F provides statistics regarding the severity of the growth in the number of attacks on personal computers. This can be considered to be a bellwether for things to come in the commercial wireless domain due to the increasing amount of similarities and overlap in commercial wireless device technology and PC technology.



CE devices ⟷ PCs and more (firmware)

PCs

- Application layer
- Execution environment (i.e.. J2e, MExE, SMS, MMS)
- Operating system and device drivers
- Hardware: general purpose CPU(s)

Vulnerabilities:

- Viruses (email, downloads)
- Insecure OS (attackers can remotely take over the PC)
- Complete control over all software by users
- No DRM or privacy protection

+

Current modest device architectures

- Software to support and manage device features/functions
- Operating system and device drivers
- Specific hardware based upon device

Vulnerabilities:

Mostly hardware-oriented attacks that break the proprietary download method (find secret keys, etc.), which allows all devices with this fixed security to be compromised

=

Future device architectures

Application layer	
Execution environment	Support for device-specific functions
Operating system and device drivers	Firmware support
Hardware: general purpose CPU(s)	Programmable firmware

Vulnerabilities:

All the security problems of PCs and current CE devices

Copyright 2004 Panasonic
All rights reserved

Figure 2. Generic wireless device architecture

2.4.2 Threats to SDR Devices

Obviously, no security would be needed if there were no threats. To better understand SDR security needs, therefore, this document discusses some of the current and, more important, future threats to SDR devices. The following list addresses some of the threats from potential attackers on an SDR device. This list is in no way complete, but it does contain some of the more potent and popular forms of attack. It is provided to give the reader a more concrete exposure to the risks an SDR device will face which will in turn allow a better understanding of the security needs. In addition, this list supports the need for the strong requirements proposed in Section 4.

1. Scripted attacks: automated attacks created by hackers and then made available via the Internet.

   Examples:

   a. Viruses

   b. Trojan horses

   c. Worms

Current CE devices are not susceptible to these attacks but next-generation devices with email and other Internet-aware applications will be vulnerable. These threats represent the greatest potential cost of failure because a successful scripted attack will disrupt many thousands of devices in a short time with little to no effort to the attacker (in a fashion similar to how today’s PCs are disrupted by these attacks).

2. User or attacker (local or remote) loads unlicensed/unsupported OS onto device (accidentally or maliciously). This can be accomplished through a number of methods such as:

   a. Security methods that fail to prevent users from loading their own OS (PC model)

   b. Poor (or nonexistent) RAM memory protection that allows a buffer overflow to overwrite the kernel

   c. OS is not stored securely in long-term storage

   d. Access control bugs

3. SDR phones share a small set of secret keys.

   For example, someone will perform a sophisticated HW attack to attain this set of keys and then publish them on the Internet.

4. Replacing the software payload.

   For example, if weak data integrity algorithms are used (such as CRC), then a drastically different but passable version of the payload can be created that will pass validation checks.

5. Forcing invalid software updates/configurations to be downloaded and possibly installed.

   For example, if the version control mechanism is faulty or becomes compromised, then an attacker can trick an SDR device into loading a “valid and signed configuration,” the problem being that it is valid for a different model and causes the current SDR device to fail. This is especially the case when updates occur without any user intervention or acknowledgment.

6. Attacking the higher level telephony.

   This threat has already occurred in Japan, where an email virus caused phones to aqutomatically dial the U.S. equivalent of 911 (emergency). The telephony will reside in the execution environment and is therefore very susceptible to attack.

7. Bugs in the security software.

   If bugs exist in the security software, they will be found. If the security software cannot be updated, this will create a huge problem that will most likely result in a recall.

8. Hardware tampering.

   Hardware experts can always perform very powerful attacks on SDR devices; these attacks can only be slowed but not prevented by tamper-resistance techniques. Of course such experts could also use their efforts to simply build an SDR device from standard components that are now readily available. Due to the expertise required and the fact that such experts can build their own SDR devices (if they desire), this particular threat can be considered unsolvable. One can conclude from this that HW tamper-resistant methods need be used only if a manufacturer wishes to strongly safeguard proprietary methods.

2.4.3 SDR Download Object/Payload and Potential Costs

Finally, we must distinguish among the various download objects because each download object has a specific security need. Such distinctions are important to allow for tailored security solutions that provide the proper level of security, which in turn allows for the best performance and QoS to the SDR device user.

Six SDR download objects should be considered:

1. *Transmitter configuration software:* Software that affects the transmitter's basic functionality (e.g., modulation/demodulation, filtering). This software can reside in firmware (likely for handhelds) or be executed by a more general purpose processor (e.g., base-stations).
2. *Security software:* As previously mentioned, the security mechanism should be updateable, and if it is, this constitutes an SDR-related download. Furthermore, access control and other SDR management software, as security software, will need to be safeguarded.
3. *Operating system*
4. *Operational parameters:* Given a transmitter configuration, operational parameters constitute data needed to instantiate the configuration for communication.
5. *Protocol stack:* This is code or data that describes a wireless provider's communication protocol
6. *Telephony:* This is the mechanism that provides a user interface along with some other useful communication applications.

Table 3 lists the download objects and what we expect will be the resultant cost of a successful attack on the payload for a single SDR device. This cost can then be defined as a SDR security need for that particular download object/payload. Note that this table provides a cost estimate only; for a particular SDR architecture one may need to adjust the cost. As an example, if the hardware provides validation of the operating system during boot-up, the compromise of the operating system by an attacker has a medium rather than a high cost because at the time of the next boot-up (or even during a routine check by the hardware) the attack will be found and appropriate measures taken. In contrast, a system that has no hardware validation of the OS has a high cost because it may be weeks or months from the compromise of the OS before the user becomes aware that the system has been hacked. An explanation of the expected costs follows.

If the transmitter configuration is compromised, the SDR device could be configured to cause a large amount of interference, which is clearly deleterious and why this object has a VERY HIGH expected cost.

If the security of a system is compromised, then all objects become susceptible to attack, which is why this object also has a VERY HIGH expected cost.

The operating system will be performing some amount of security and also affects the overall functioning of the device, so comprise of the OS will allow some components to be susceptible to attack (which may lead to some interference) and will also mean that the device may cease to function properly. Furthermore, if update mechanisms become broken, then the user must bring the device to a service center or return it to the manufacturer for repair (both of which are costly to the manufacturer). This places the OS expected cost in a MEDIUM to HIGH category, depending upon whether the OS can be easily reinstalled by the user and whether components for checking OS integrity are present.

SDR operational parameters are a tempting target for attackers because they could conceivably be updated often, and if compromised will cause interference to local users communicating on or near the same frequency. Due to the possibility of interference, the cost is estimated at MEDIUM. For some standards that allow a base-station to identify and locate SDR devices that are operating outside of the passed parameters, however, this payload could be reduced to LOW. (Once identified, the wireless operators or base-station could take actions to correct the device and, if the device refuses to operate with the given parameters, to take actions that disable the device and remove it from service, or to contact the local authorities).

The protocol stack and telephony are estimated at LOW cost because attacks on these will cause the device to malfunction in a way that the user will (typically) identify as a problem. With the OS still intact, those components can be reinitialized or reinstalled to fix the problem.

Of importance, note that if “scripted attacks” are possible, the cost will always be VERY HIGH to EXORBITANT, no matter what part of the SDR device is attacked. It is a requirement that SDR security mechanisms prevent this type of attack.

These expected costs will be revisited in Section 4, in which the SDR Forum suggests security requirements for SDR devices. The requirements will be quite strong for SDR objects that have a HIGH security need, but will be adjusted accordingly for those objects that have MEDIUM to LOW costs.

Table 3 Download Objects versus Cost of Breach in Security

SDR Download Object/Payload	Potential Cost to the Manufacturer and/or Interference to Airways if Compromised
Transmitter configuration	VERY HIGH
Security	VERY HIGH
Operating system	MEDIUM to HIGH
Operational parameters	MEDIUM
Protocol stack	LOW
Telephony	LOW

2.4.4 Security Threat Use Cases

Many use cases could be generated for the download, storage, installation, and instantiation for commercial wireless devices due to the many variables. Examples of these variables include:

- What is the download mechanism (e.g., over-the-air, through a personal computer, through a smart card, or other)?
- How is the download initiated (e.g., by the network, by the device, or by the user)?
- What type of software is being downloaded (e.g., radio software, operating system, applications software, or other)?
- When is the new software activated (e.g., immediately after download or at some later time) and what is the triggering mechanism?
- What threats are applicable to each particular use case scenario?
- Who is the perpetrator? (A different use case could be defined for each type of perpetrator.)

It is well beyond the scope of this document to provide use cases for each and every combination of the above parametric variables. Instead, an illustrative use case is provided that provides the basis for the detailed security requirements in Section 4.

2.4.4.1 Categories of Actors for Security Use Cases

Use cases are built from sets of candidate actors. A list of categories of actors for use in developing security use cases for operational software download, storage, installation, and instantiation is provided below. A particular security use case may or may not require the use of an actor for each of these categories of actors. Subsection 2.4.4.2 provides examples of the use of several of the actors defined below.

- Provider (of downloaded component). This may be the manufacturer or a third party. In the near-term for operational software, it will be the manufacturer (i.e., in the near-term, third parties provide only applications software, which is outside the scope of this document).
- Network operator (includes reconfigurability manager)
- Server (supplying downloaded component)
    - Wireless
    - IP
    - Other (e.g., IR, Bluetooth)
- Client in the wireless device
- Agent in the device (as an internal server to actually install authenticated components; includes protection management functionality)
- Authenticator (of component; implies key-based solution)
- Verification engine (within device)
- User (of device)
- Other device (especially compromised device)

- Perpetrator (the hierarchy beneath this is beyond the scope of this document)
- Malevolent application on platform

The Provider, Server and Authenticator are related roles that may be played by the same entity.

2.4.4.2 Example Security Threat Use Cases

Table 4 describes two example security use cases for two over-the-air DSII scenarios. The scenarios utilize the actors described in the preceding subsection. Figures 3 and 4 provide the flow for these two example use case scenarios. The use case in Figure 3 is for a normal update of radio software. The use case in Figure 4 depicts the attempt of a perpetrator to penetrate radio software by masquerading as a server attempting to (falsely) download an operating system update patch that contains malicious software. As usual, in high-level use cases, the detailed interactions (such as discovery of the need for a download, capability exchange, etc.) are not depicted.

Generalization of the threat illustrated in these use cases leads to the requirements discussed in Section 4 of this report.

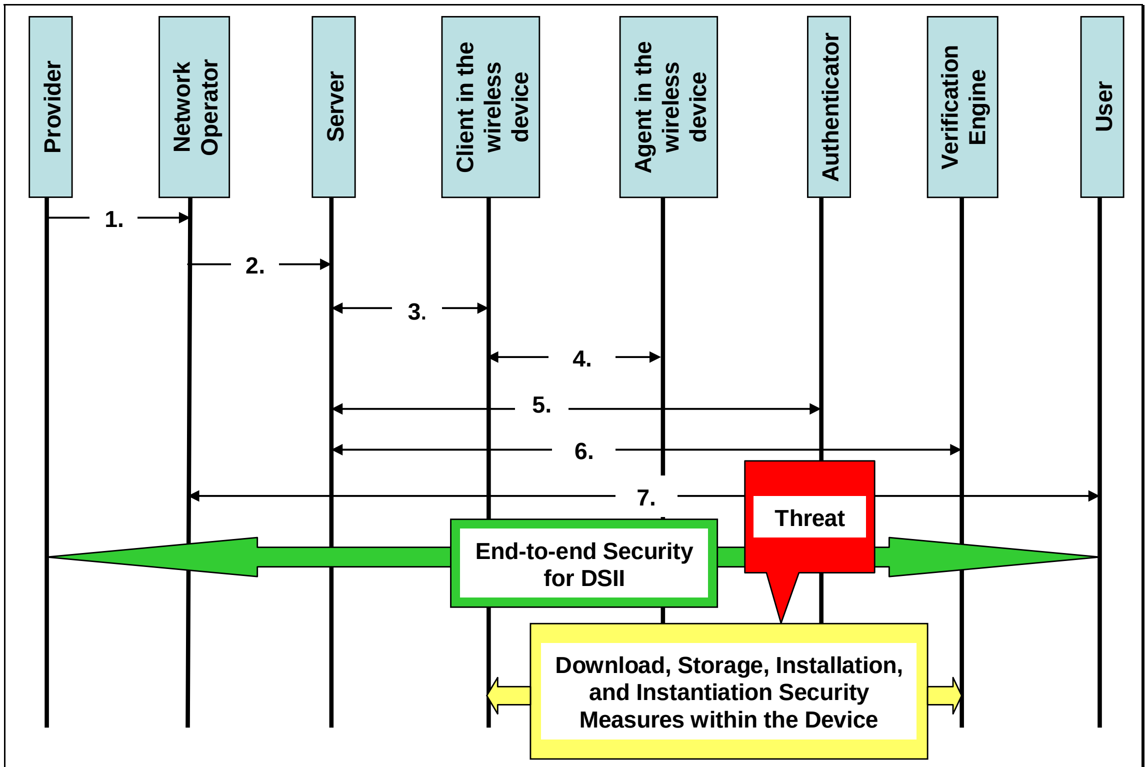
2.4.5 Software/Firmware Authorization for SDR-Capable Devices

At this time, regulatory agencies indicate that they are willing to rely on industry to develop secure technologies that allow software download to SDR-capable devices. Some regulatory agencies, however, require the licensing of each hardware/software combination. Figure 5 depicts the current hardware/software authorization flow for these administrations. The top-right portion of the figure shows the licensing process for “radio” software. Other types of operational software updates, such as operating system updates and driver updates, also need approval from a “qualifying authority” but do not require regulatory authority approval. Ultimately, it is the qualifying authority (service provider, operator, designated management authority, or industry group) that approves the release of the software for download through the appropriate distribution channel. In Figure 5, we assume that there is no threat to the integrity of the code during the transfer of files between the trusted source and the regulatory agency or between the trusted source and the qualifying authority. The threats are in the distribution channels, in spoofing of the distribution channels, or directly to the wireless device. We also assume that the operational software has been thoroughly tested by the manufacturer and/or the operator/service provider.

The radio software is unique in that some administrations may require type acceptance, certification, or conformance assessment for each hardware/software combination. Other administrations use a self-certifying procedure by the manufacturer. Recognizing that there may be many hardware/software combinations for SDR-capable wireless devices, researchers are currently investigating automated calibration and automated certification/authorization procedures [Fung et al., 2003; Okuike et al., 2003].

Table 4 Two Example Use Cases

	Radio Software DSII Scenario (Figure 3)	**Operating System Software Patch DSII Scenario (Figure 4)**
Scenario description	This scenario is a legitimate update of new radio software parameters.	This scenario is an attempt at an illegitimate update of a patch to the operating system in the wireless device.
What is the download mechanism?	Over-the-air	Over-the-air
How is the download initiated?	By the network operator who determines that an update to radio software is needed.	By a perpetrator who masquerades as a server who is attempting to update a patch to an operating system.
What type of software is downloaded?	Radio software parameters	Operating system
When is the new software activated?	Immediately upon the completion of the download, the software is stored in protected memory, installed, and activated for use.	Immediately upon the completion of the download, the software is stored in protected memory, installed, and activated for use.
What is the threat in this example use case?	None	The threat is to the radio software caused by the malevolent distribution of a false update to operating system software. The software includes malicious code that tries to access the radio software when the software update package is downloaded, stored, installed, and activated.
Who is the perpetrator?	None. For this use case scenario, it is assumed that there are adequate security measures in place between the software update provider and the network operator.	A fake server who sends false software update message. Assuming that the perpetrator is successful in distributing the malicious code, it is incumbent on the software in the wireless device to deny access to the storage, installation, activation, and execution of the malicious code that affects the radio software.
ACTORS		
Provider	X	
Network operator	X	
Server	X	
Client in the device	X	X
Agent in the device	X	X
Authenticator	X	X
Verification engine	X	X
User	X	
Other device		
Perpetrator		X
Malevolent application on the device		


Provider
Network Operator
Server
Client in the wireless device
Agent in the wireless device
Authenticator
Verification Engine
User
1.
2.
3.
4.
5.
6.
7.
Threat
End-to-end Security for DSII
Download, Storage, Installation, and Instantiation Security Measures within the Device

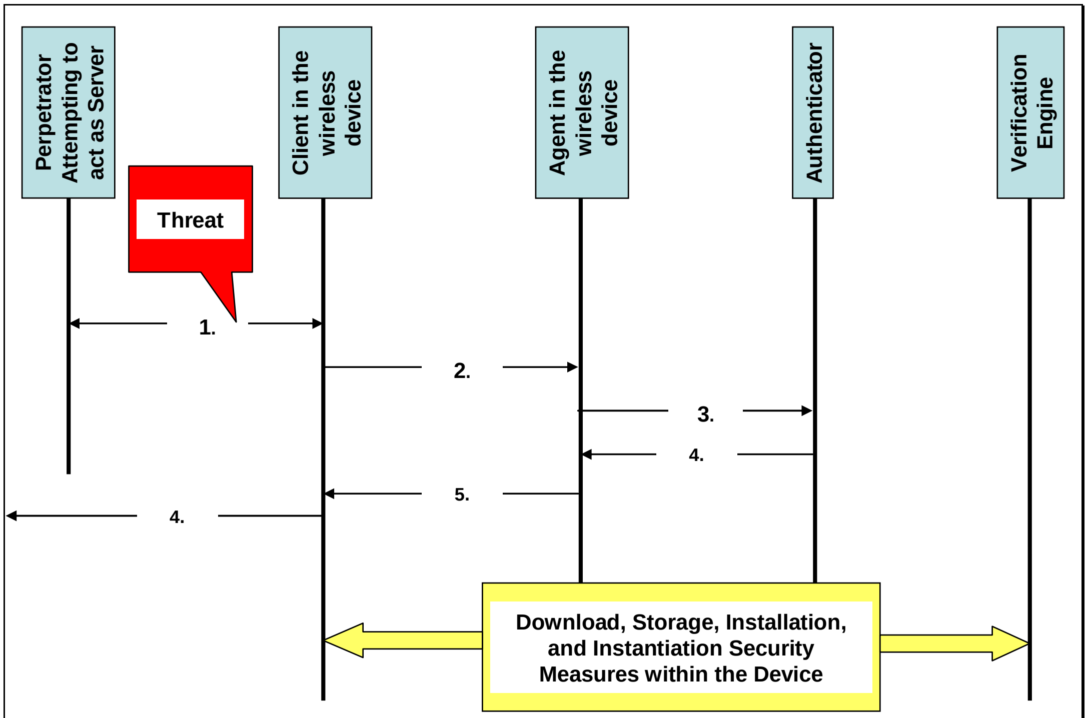
1. Vendor delivers software/firmware package to the operator with appropriate signature(s); see Figure 5.
2. Operator installs software in the device management server which is part of the radio network.
3. Server initiates the protocol to download software/firmware package to the device; secure client-server methodologies are well established.
4. Wireless device internal server initiates and controls the storage, installation, and instantiation of the downloaded software/firmware.
5. Authenticator in the device initiates the authentication protocol with the server.
6. Verification engine within the device initiates the verification protocol with the server.
7. Network operator informs the user of the download; user accepts the download.

Figure 3. Use case flow chart for OTA DSII of radio software

The fact that the hardware as well as all of the software in the SDR-capable wireless device can be changed presents some unique security challenges. Technologies such as field programmable gate arrays (FPGAs) and micro-electro-mechanical systems (MEMSs) provide the capability for hardware reconfiguration under software control. This capability is vulnerable to malicious attack and therefore has a unique security requirement for SDR-capable devices.

Another unique requirement for security for software provisioning and configuration to SDR devices is related to the hardware capability of the devices themselves. Processing power and memory in SDR terminals are somewhat limited compared to personal computers. Therefore, the security mechanisms available to mitigate the security threats may be limited in their capabilities. A good example here is the difficulty of running anti-virus software in a limited memory environment and updating it frequently, as a PC can.

International agreements on roaming of terminals present another aspect of unique security considerations for SDR-capable devices.


Perpetrator Attempting to act as Server
Client in the wireless device
Agent in the wireless device
Authenticator
Verification Engine
Threat
1.
2.
3.
4.
5.
4.
Download, Storage, Installation, and Instantiation Security Measures within the Device

1. Perpetrator attempting to masquerade as a server sends a false message that appears to be an update to an operating system; the software being sent actually contains malicious code that attempts to penetrate the radio software to make the device operate outside its approved power/frequency/bandwidth thresholds.
2. Client in the SDR device accepts the download and passes information to agent in the SDR device.
3. Agent in the device sends message to authenticator.
4. Authenticator in the SDR device does not recognize the signature and informs the agent that the message is not legitimate.
5. Agent passes the bogus message information to the client.
6. Client notifies the network that there has been an attempt to penetrate the security of the network.

Figure 4. Use case flow chart for operating system software patch DSII scenario

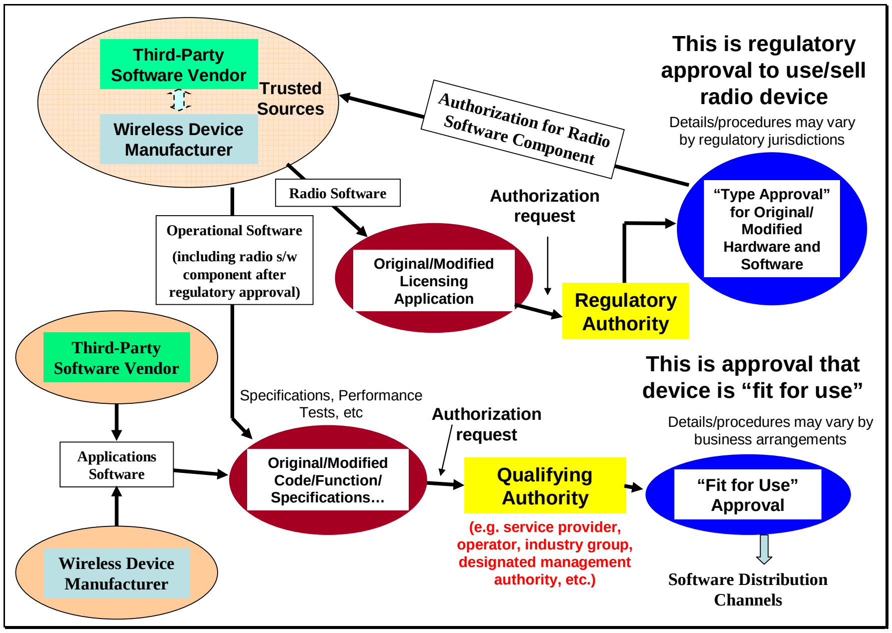

Third-Party Software Vendor
Trusted Sources
Wireless Device Manufacturer
Authorization for Radio Software Component
This is regulatory approval to use/sell radio device
Details/procedures may vary by regulatory jurisdictions
Radio Software
Authorization request
Operational Software
(including radio s/w component after regulatory approval)
Original/Modified Licensing Application
Regulatory Authority
"Type Approval" for Original/ Modified Hardware and Software
Third-Party Software Vendor
This is approval that device is "fit for use"
Specifications, Performance Tests, etc
Authorization request
Details/procedures may vary by business arrangements
Applications Software
Original/Modified Code/Function/ Specifications…
Qualifying Authority
"Fit for Use" Approval
(e.g. service provider, operator, industry group, designated management authority, etc.)
Wireless Device Manufacturer
Software Distribution Channels

Figure 5. Software/firmware authorization process flow

2.4.6 Software Upgrade Distribution Channels

The operational software download channels include the following:

- Download over the air via the normal authorized wireless communication channels
- Download via the Internet
- Download from a computer by a technician at a kiosk or service facility
- Download via a SIM card
- Download from a secondary air interface such as Bluetooth or wireless local area network (WLAN)
- Download via USB connection with the host computer

Figure 6 provides a generalized view of operational software download for reconfiguration. The keys to security, as can be seen in Figure 6, are:

- The trusted source to destination channel and protection of various types of operational software from malicious or inadvertent attacks
- Security mechanisms during the storage, installation, and instantiation within the wireless device (e.g., memory protection, authentication, and so on) to ensure that radio software cannot be inadvertently or maliciously changed by the download, storage, installation, instantiation, and execution of non-radio software)

If the interfaces (red dashed lines in Figure 6) are standardized, much of the rest could remain proprietary. What would be important is that those interfaces verify integrity and a cryptographically authorized source. If that was done in a standard way, the remaining players (hardware and software) could be proprietary. In other words, what goes on in the transmission pipe is really irrelevant as long as appropriate security technologies are used between source and destination. For example, a source developer could transmit his or her signed change to an administrator, and the administrator could then take the change, put it on a memory stick, carry it over to a USB port on a device, and load it in. Then the other interface would kick in and verify the integrity and digital signature. Moreover, the transmission pipe can be anything as long as appropriate certification/digital signature/authorization/authentication/confidentiality measures are employed.

Different types of threats are associated with each type of download. Figure 7 depicts in a general way the threats to secure download, storage, installation, and instantiation. These threats include threats to the distribution channel itself and threats to the fielded SDR-capable device.

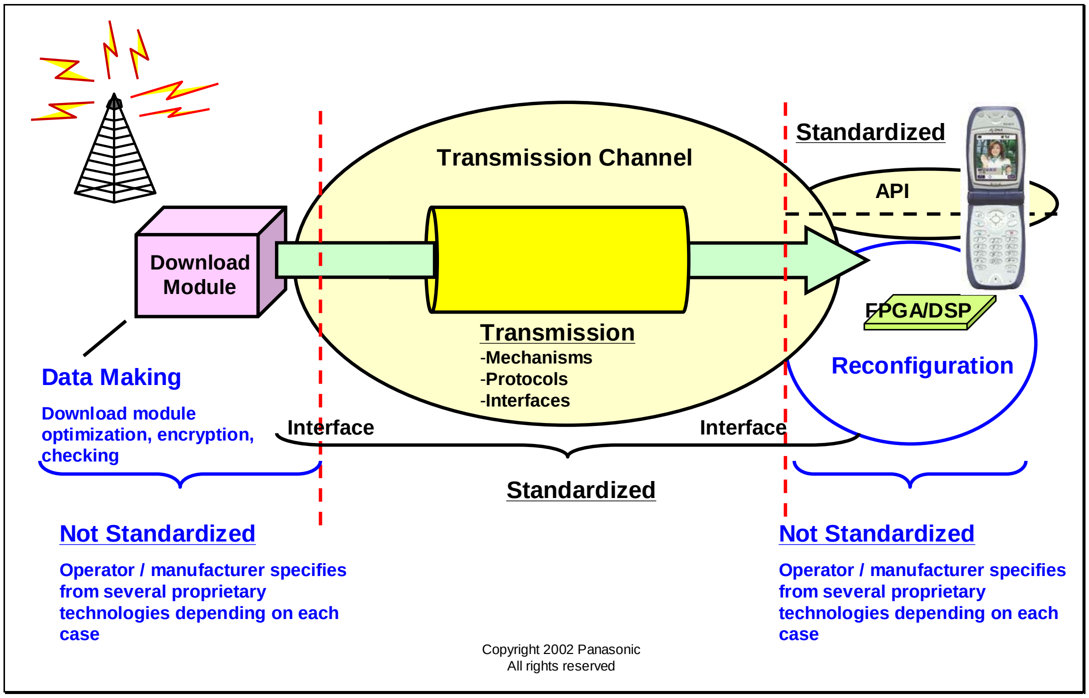

Transmission Channel
Standardized
API
Download Module
FPGA/DSP
Transmission
-Mechanisms
-Protocols
-Interfaces
Data Making
Reconfiguration
Download module optimization, encryption, checking
Interface
Interface
Standardized
Not Standardized
Not Standardized
Operator / manufacturer specifies from several proprietary technologies depending on each case
Operator / manufacturer specifies from several proprietary technologies depending on each case
Copyright 2002 Panasonic
All rights reserved

Figure 6. Generalized view of operational software DSII for reconfiguration

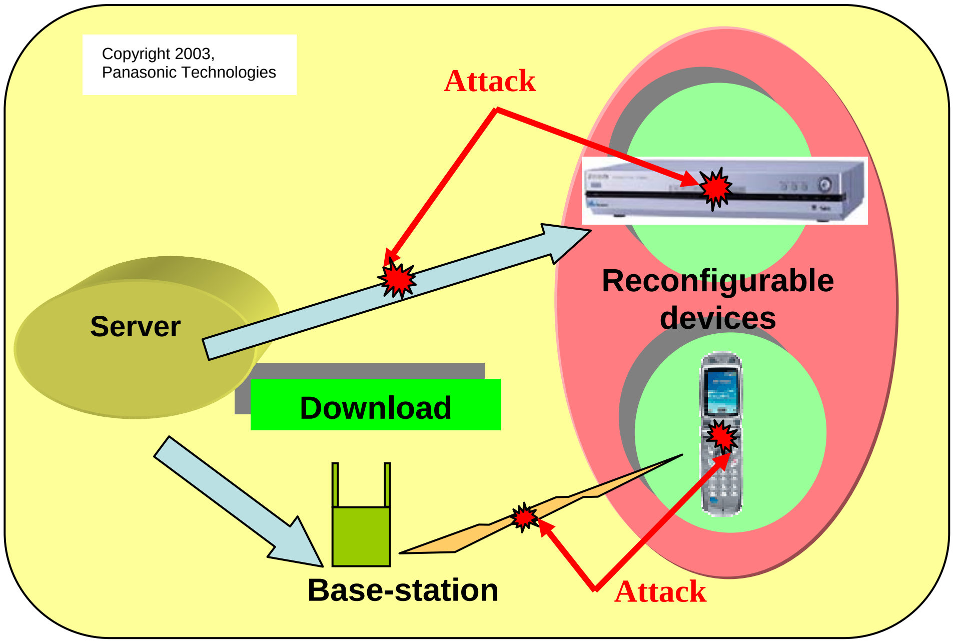


Figure 7. Threats to different types of commercial wireless devices

2.5 System Perspective of Security for Operational Software for Commercial Wireless Devices

In this document, software download security involves more than just the SDR device itself — it involves the entire network. An excellent paper that describes the network aspects of SDR (and/or reconfigurable radios) from a licensed commercial mobile radio service point of view is provided by Pereira [2000]. Many papers have come from the research programs sponsored by the European Commission (see, for example, the papers in the SDR Forum Technical Conferences of 2002 and 2003, the SCOUT Workshop on Reconfigurable Terminals and Supporting Networks on 16 September 2003, and the IST 2003 Summit). Papers on networks that support reconfigurable terminals may be found in Dillinger et al. [2003, Part III].

Figure C-1 in Appendix C illustrates the network aspects of software download from a commercial wireless perspective (specifically the licensed band which is referred to in the ITU as commercial mobile radio service). Depicted in the figure is a generic system model of the entities relevant to operational software download security. This includes public IP networks that could be accessed for applications software download and the operator/service provider IP networks.

3 SDR Forum Security Reference Model

As indicated by the numerous related entries in the References (Section 8; see also Section 9), a large number of papers have been written about various aspects of the complex conceptual space involved with delivering new software modules to working terminals. Protection needed for data is only part of the concern associated with software download, where the full cycle of download, storage, installation, and instantiation of software over wireless links must be considered. The referenced papers describe a variety of approaches; in this document, we provide an overview of the field.

At present, no single solution to the problems associated with download security exists. It will be incumbent for researchers and system designers working in this area to familiarize themselves with the rich resources available, make the needed trade-offs, and to select approaches and components that are best suited to the specific issues at hand.

3.1 Introduction

To assist in navigating this complex space, the SDR Forum has developed the SDR Forum Security Reference Model shown in Figure 8. This model, derived from study of a large number of relevant works in the area, attempts to provide a framework within which specific issues can be placed to put them in perspective with other topics. This model is intended to provide a common context for the DL series of documents as well as other security considerations within the SDR Forum.

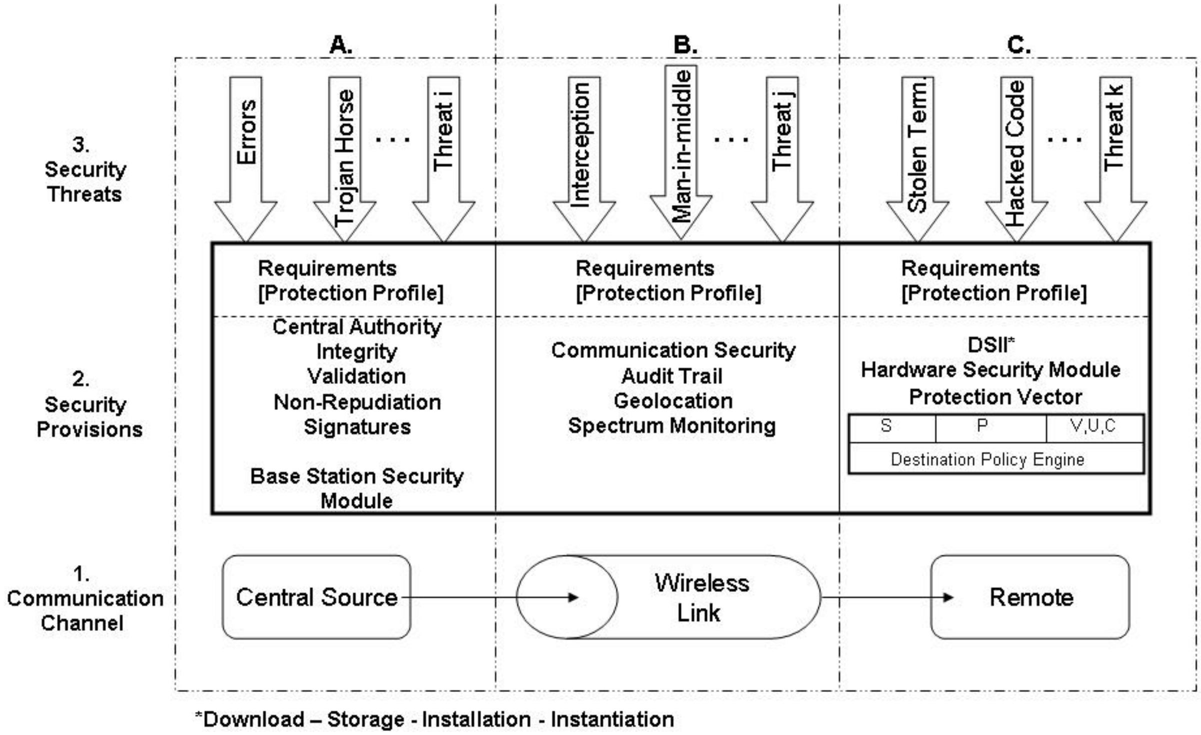


Figure 8. SDR Forum Security Reference Model

3.2 Reference Model Levels

The SDR Forum Security Reference Model consists of three levels, representing the communication channel, security threats, and the intervening security provisions for protecting the link from the threats. In each of the levels, issues relating to the information source, the wireless link, and the destination are considered individually.

For simplicity, this version of the model considers the outbound path that is of primary concern for software download operations. This flow is a one-way transfer of information from a central source to a remote location over a wireless link. Most of the security concerns are the same for outbound, inbound, or full duplex operation. Any differences that might exist can be illustrated with variations of the basic model.

3.2.1 Level 1. Communication Channel

The Communication Channel level comprises the physical components of the system. The source includes all of the infrastructure needed to originate information intended for delivery to the destination, the deployed remote terminal. In the case of a software module to be downloaded into a mobile, the source would include the originator of the code, all of the mechanisms for configuration management, validation of the remote terminal’s right to participate in the network, authorization to proceed with the download, and network facilities to deliver the code, packaged as data, to the radio access network air interface addressed to the destination.

The remaining component of the Communication Channel is the wireless link through which the data travels. There are essential differences between wired and wireless links. One is the mobility provided to the destination. Another is the erratic nature of the link — a higher bit error rate, fading, and loss of signal as the mobile moves out of range. The key difference, from a security viewpoint, is that the signal can be intercepted anywhere the signal strength is sufficient, and therefore false transmissions can be made.

3.2.2 Level 2: Security Provisions

This is an appliqué of protection mechanisms installed in the system to thwart attempts to violate system security. It can include signatures, certificates, and encryption as well as physical security and secrecy to ensure that information entering the channel is valid and to protect it for transmission. After successful download of new software, the Protection Vector (PV) provides a disciplined approach to evaluating the credentials of the package, and making a policy decision to accept or reject the downloaded module after it has arrived at the destination terminal. The evaluation considers the source, reliability of the channel, and local operating considerations in the light of established security and operating policy considerations. This level provides consideration of mechanisms that can protect the bottom level from intrusion.

The security provisions indicated in the model are intended to be suggestive rather than exhaustive. The intent is to indicate what provisions are appropriate to each of the columns.

3.2.3 Level 3: Security Threats

Any occurrence that detracts from perfect operation of the system is a threat, considered in Level 3. Threats generate requirements for security protection. Protection Profiles (PPs) provide a structured method to describe security requirements. A Protection Profile is defined as being "an implementation-independent set of security requirements" [Krall, 2004]. This level is concerned with sources of possible intrusion, disruption, or interception.

The Security Reference Model provides a tool for considering the very complex space of wireless download security. In areas where the threat structure can be identified, systems may benefit from an approach that considers threats first, and then builds the Level 2 constructs to mitigate those threats. Other systems will start with a proposed Level 1 structure, build the Level 2 provisions on top, and then test the Level 2 provisions against a threat taxonomy to explore for possible weaknesses.

3.3 Detailed Description of the Model

In the following subsections we consider the nine areas of the model shown in Figure 8, using the level number and column letter. We describe them in some detail, and give examples of the kinds of considerations that are relevant. We also provide references to specific relevant publications. Our intent is not to provide solutions to problems of wireless download security, but rather to provide a tool to facilitate exploration and consideration of this very complex space. A more detailed discussion of each of the nine model components is given next, with references to some of the papers that have provided source material for this model.

3.3.1 Level 1. Communication Channel

In the commercial wireless world, service providers sell access to a wireless infrastructure. They may own or lease rights to that infrastructure. They specify what terminal models will operate in their service, and sell access to the infrastructures to customers either directly or through a trusted third-party vendor.

Multiple opportunities exist for delivery of software to end users. The first, at time of initial delivery, includes software in both the terminal and user identity module. Later software delivery opportunities occur, for example, if a terminal is brought into a service facility, by connecting the phone to a kiosk or personal computer, by changing the SIM, or through use of over-the-air software download.

3.3.1.1 Block 1A

Software to be downloaded must offer a high degree of assurance that it will not improperly impact the basic performance of the terminal. That assurance, in turn, requires that the source of the software can be trusted. In practice, only the original manufacturer of the terminal should be in a position to change operational software, although third parties will often provide code for applications. Manufacturers must adopt protective means to ensure that radio software cannot be impacted by the download, installation, and execution of other types of software.

The primary mechanism for validation and non-repudiation of the originator of the download resides in Level 2, but Level 1 concerns include considerations of code compatibility across large numbers of terminals, the degree of testing done, the hardware mechanism needed for Level 2 security measures, and potentially the formal proof of correctness. Gallery [2003] suggests the need for a mechanism for the protection of original code, identification of the author, and records of the testing performed and test results, and deals with these issues in detail.

3.3.1.2 Block 1B

Software download is needed for the correction of software errors in the initial code, insertion of new applications, addition of functionality, or conversion to a completely different service. From the perspective of Block 1B, the wireless link, as a delivery mechanism, there is no essential difference between transfer of software to be installed — funds, stock market data, or even ring tones.

3.3.1.3 Block 1C

Block 1C is the target of a great deal of material in wireless security papers. One key issue is the need (or lack thereof) for a hardware module that cannot be altered after shipment to positively identify the terminal and to carry a secret key. Michael et al. [2002] and Cook [2003] make the case for a tamperproof security module based in hardware. A formal analysis should be made to balance the cost of anti-tamper mechanisms versus the value of the information to be protected.

The Mobile VCE has published extensively its Reconfiguration Management Architecture (RMA) described in SDR Forum, 2002]. RMA uses a rule-based “tag file” approach to ensure that only valid combinations are loaded in a terminal.

Lam [SDR Forum, 2003] introduces GPS capability to the terminal to satisfy regulatory emission requirements for roaming.

3.3.2 Level 2: Security Provisions

This level comprises various security mechanisms to protect information traveling through the Level 1 mechanisms; it actually is not required at all. The Communication Channel is perfectly capable of transferring information with no specific security provisions. In practice, however, security provisions are required, and trade-offs among cost, efficiency, and protection are needed. There does not appear to be any single general case, so the details of security provisioning need to be considered for each case.

3.3.2.1 Block 2A

Block 2A is involved with assurance that the source of the information to be transferred is reliable, trusted, and authorized to undertake the transaction. This may involve adding information to establish that the source is bona fide, and may include ancillary information such as the results of software testing. Certificates may be used to ensure that there has been no perturbation in the information during transmission. Signatures may be used to authenticate that an individual or office is who they say they are. A central authority is needed to endorse both parties to the transactions.

Non-repudiation is assurance that the attributed source of the information is correct. Senders cannot claim that they were not the originators of transactions that they did, in fact, send. Signatures are a mechanism whereby some individual or organization indicates its approval of a transaction by signing it. Multiple signatures, representing the concurrence of several involved organizations, will often be needed. An example would be approval of a software correction patch by the equipment manufacturer, service provider, and network operator. Ultimately, however, trust comes into play, and appropriate steps must be taken to ensure that the needed level of trust is in place.

The Base Station Security Module is a hardware-based unit that protects the security of the network end of the wireless link. It ensures that software downloaded to the base-station is properly authorized, and that no inappropriate RF emissions are made.

3.3.2.2 Block 2B

Block 2B includes whatever encryption, transmission security, or low probability of detection facilities are used to protect the information. It is not possible to prevent interception on a wireless link, but demodulation can be made very difficult. If the information is encrypted, its contents are much less likely to be extracted without the proper keys.

An audit trail of the path transited by the download package en route to the destination can be used to establish that the package was not diverted and manipulated along the way. Geolocation and spectrum monitoring can develop information to identify anomalies in terminal behavior from attempts to penetrate the system.

3.3.2.3 Block 2C

Block 2C takes the information after it has been returned to its original state, and puts it into a storage area. Then, after assuring that it has been received correctly and has the proper credentials, it can be introduced into the local software library and utilized.

Included in this block is a process primarily derived from the Mobile VCE work [see Gallery, 2003]. That work is recast into the form of a Protection Vector (PV), a series of numeric values for various system security aspects. Those vector elements are provided to a rule-based Destination Policy Engine that renders a verdict as to whether a given software downloaded should be accepted or not.

The source reliability parameter (S) is an assessment of the reliability of code that is a candidate for download, and is related to Block 2A. Levels of assurance are a statement by the code originator that it is acceptable, identification of the author(s), development by trusted authors, independent trusted third-party test, and formal proof of correctness.

The path vulnerability parameter (P) is an evaluation of the intermediate path between the developer and the target terminal. Path protection mechanisms are digital signatures, public key infrastructure, audit trail and path histories, and trusted intermediate repositories.

Three parameters provide local context for policy evaluation and decision making. First is the inherent value (V) of the content, with a priority structure of worth such as mission critical, money, executable code, data, and audio or visual material. The second Block 2C parameter is urgency (U), rated from high to low. Under some circumstances, it is appropriate to accept information that is extremely urgent even though some risk is involved because its other parameters were lower than desired. The final parameter is criticality (C), which is concerned with the impact on system operations if the received information is faulty. Low criticality would be assigned to such corrections as a spelling error, minor feature addition, or improvement in the user interface.

When all of the PV elements are collected together, a Destination Policy Engine uses policy rules to determine whether the code should be installed. Much of the philosophy here is similar in concept to the Protection Profile (PP) described in: http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf.

The Protection Profile is a set of requirements cast in the form of prevention before system design or during system evaluation. It is also involves policy instantiation and execution during run time. The Protection Vector is a “go-no go” decision after a specific instance of information transfer.

Security provisions will vary from system to system. The military goes to considerable effort and expense to provide secure tactical radios, but makes extensive use of commercial mobile radios and wireless PCS communications for administrative traffic. Wireless telephony discovered, with such systems as AMPS, that inadequate security leads to loss of revenue from stolen service and customer dissatisfaction from lack of privacy.

3.3.2.4 Literature References

Many of the relevant papers spend considerable time discussing Level 2 considerations. It is beyond the scope of this document to analyze and reconcile all of the considerations taken into account by these papers and other work that is going on in the field. These papers do, however, provide a rich source of information to system designers, who can examine the issues they raise in determining the requirements for a specific service.

Michael et al. [2002] provide an extended discussion of the use of public key, symmetric key, hashing, and signatures to provide protection for all stages of the download process from regulatory approval through instantiation in the terminal This document also establishes a requirement for a tamper-proof hardware module.

Fitton [2002] and Cook [2003] (in an elaboration of Fitton’s work) also call for such a hardware element and suggest that multiple signatures will often be desirable, with manufacturer, regulatory, service provider, and network operator as potential signers. In addition, these works describe in detail the following 11 security features derived from consideration of the JTRS SCA:

1. Security Policy Enforcement and Management
2. Information Integrity
3. Authentication and Non-repudiation
4. Access Control
5. Encryption and Decryption Services
6. Key and Certificate Management
7. Standardized Installation Mechanisms
8. Auditing and Alarms
9. Configuration Management
10. Memory Management
11. Emissions Management

The SDR Forum System Security document [SDR Forum 2002] describes the following security measures:

- Central Authorization Agency (CAA) and authorization dissemination
- Encryption
- Certification
- Non-repudiation
- Fault Management

Gallery [2003] proposes a security framework with seven elements:

- Entity Roles and Responsibilities
- Digital Signatures
- Public Key Infrastructure (PKI)
- Virus Scanning
- Trust Relationships
- Proof Carrying Code (PCC)
- Path Histories

3.3.3 Level 3: Security Threats

The threat space is one of the most complex aspects of wireless security because it is very large and sparsely populated. The threat space is large because an attacker can attack any one of millions of terminals anywhere in the world. Further, the attack can take place at any point in the system, so an attack could conceivably occur at billions of possible threat points or places. It is sparsely populated because attacks are rarely seen in the normal course of events. That is to say, the number of calls that are subject to one of the threats is a miniscule fraction of the calls completed without incident. The real threat to a particular system is a subset of the potential threat, and it varies with the intent and skill of the individuals involved. People with a variety of different motivations are in contact with the system on a daily basis — some of them are curious, some careless, and some malicious.

The threats in the Security Reference Model are shown in Figure 8 as arrows attacking individual parts of the system, and deterred by the security provisions protecting those components. Individual threats can strike at any part of the system at any time, and they can be new or ones previously seen. There is no way to develop an exhaustive list of threats because ingenuous individuals will always find new ways to attempt to crack the system.

In addition to malicious threats, disruption of normal operation can be caused inadvertently by users of the wireless system, although good system design should mitigate most such potential problems. In particular, the system should handle overload gracefully to deal with situations such as many users in a traffic jam providing a heavy offered load in a small section of freeway.

Careless or undertrained support staff can also be part of the threat space. Support staff have access to system components and an inherent need to operate inside the security provisions structure.

The SDR Forum System Security document [SDR Forum, 2002] describes a security threat vector (STV) with three components, each with its own subcomponents:

- System Operating Modes
  - Voice communication
  - Data transfer
  - Software download
  - Application execution
- Perpetrators
  - Negligent
  - Unauthorized
  - Malicious
- Security violations
  - Impersonation
  - Unauthorized access
  - Denial of access/service
  - Physical

The SDR Forum System Security document [SDR Forum, 2002] proposes an STV with these elements taken in triplets to provide a taxonomy of 48 different security violation scenarios, each of which can be considered a different threat. The STV provides a tool for the system developer to systematically consider the threat environment.

The SDR Forum Report to the FCC on Issues and Activities in the Area of Security in SDR [SDR Forum, 2002c, Section 3.3.2] was the “mid-year” report to the FCC. It describes a threat model with four components, again, each with its own subcomponents:

- Point of Attack
  - Terminals and UICC/SIM
  - Infrastructure
- Access
  - Physical
  - Remote (either wireless or wireline network)
- Motive
  - Negligent (authorized users who are negligent in their usage of the system)
  - Unauthorized users who are non-malicious
  - Unauthorized users who are malicious
- Consequence
  - Denial of service
  - Interference with other services
  - Digital rights violation

The 36 components of this model cover much of the same threat space as the previously mentioned STV, but with a different taxonomy.

Falk et al. [2002] describe the following list of 12 security threats identified by the EU SCOUT project as exacerbated by introduction of SDR technology and reconfigurability:

1. Download and Execution of Malicious Software
2. Modification of Other Functionality
3. Circumvention of Security Functions
4. Easier Attacks
5. Invalidation of Conformance Requirements
6. User Safety
7. Disturbing Other Users or Other Radio Systems
8. Disregard of Preferences
9. Manipulated Reconfiguration

10. Unreliable Operation
11. No, or Insufficient, Protection of Intellectual Property
12. Illegitimate Access to Private Information

Although this list has an ad hoc structure, it identifies a number of valuable concerns in considering threats to wireless system security. Descriptions of these specific threats are provided in Appendix C, Section C.2.

As we have indicated, and as experience with attacks on personal computers has demonstrated, an exhaustive determination of threats is not possible.

3.4 Relationship of SDR Forum Security Reference Model and the Fitton Security Feature Categories

From the list of 11 security feature categories derived by Fitton [2002] and Cook [2003] from a study of the JTRS SCA, the following seven reside in Level 2 (numbers correspond to the list of 11 security features in Section 3.3.2.4):

1. Security Policy Enforcement & Management
2. Information Integrity
3. Authentication and Non-repudiation
4. Access Control
5. Encryption and Decryption Services
6. Key and Certificate Management
8. Auditing and Alarms

The remaining security features are in Block 1C:

7. Standardized Installation Mechanisms (standard installation mechanism for a given platform; this does not imply a standardized installation mechanism across all platforms).
9. Configuration Management
10. Memory Management
11. Emissions Management

3.5 Summary of SDR Forum Security Reference Model

A significant amount of material has been published on the subject of wireless security, much of it with direct relevance to download. Much of that material is the result of independent work without a common vocabulary and reference model. The arbitrary variations in perspective from paper to paper make it difficult to correlate them, or to extract the considerations relevant to a specific question or problem under consideration.

The SDR Forum Security Reference Model is a three-level construct intended to assist the ongoing work across the field of wireless security. The SDR Forum proposes it as a tool to assist in understanding this complex intellectual space. A designer making a point can refer to the model and say “I am talking about this area …”

4 Detailed, System-Oriented, Technical Security Requirements

The focus of this section is on the technical requirements for operational software download security for SDR devices in a commercial wireless domain. It is critically important, however, to also note the cost implications of security. Cost-benefit trade-offs involve two perspectives, namely:

- The perspective of the perpetrator who is attempting to subvert the security of the communications system
- The perspective of the communication system stakeholders who are attempting to ensure the security of the system

From the former perspective, the value of the information obtained as a result of breaking the security of the system must be more than the cost of breaking the security measures. From the latter perspective, the technical security solution must be economically viable for commercial wireless devices. In other words, the security solution must consider the cost of implementation — if the cost is too high, then other less costly solutions must be found that satisfy the technical requirements at a lower cost. In the end, however, security must be of paramount consideration in any balanced assessment.

The SDR Forum has published high-level functional requirements for radio software download [SDR Forum, 2002b; Hoffmeyer et al., 2004]. These high-level requirements include security requirements such as authorization, authentication, non-repudiation, and protection. In the SDR Forum view, security is the most critical part of operational software DSII and therefore emphasis is placed herein on the security requirements of DSII. This report therefore provides more detailed download security requirements, but does not elaborate on other functional requirements, such as discovery of the need for download, download initiation, capability exchange, and so on.

4.1 Common Requirements

Operational software download security requires consideration of how the hardware impacts, enables, or enforces the security features. The hardware mechanisms include a processing core and a protected internal memory. The SDR Forum asserts that both hardware and software are critical to the security solution. The allocation of function between hardware and software as it applies to the security solution is based on the level of protection required. It may range from solutions that must incorporate hardware to those for which a software mechanism alone is sufficient.

Table 5 presents the SDR Forum view as to which of the security categories presented in Section 3.2 might require hardware solutions, which might require software solutions, and which might require both. The analysis of security download requirements presented in Table 5 is based on the premise of preventing corrupted or malicious software from being downloaded, installed, or instantiated (i.e., executed) on an SDR platform [Fitton, 2002].

Table 5 Basis of Security Enforcement Mechanism

Security Measure	Possible Enforcement Means		
	Hardware	**Software**	**Both**
1. Security Policy Enforcement and Management			•
2. Information Integrity			•
3. Authentication and Non-repudiation		•	
4. Access Control		•	
5. Encryption and Decryption			•
6. Key and Certificate Management			•
7. Standardized Installation Mechanisms			•
8. Auditing and Alarms			•
9. Configuration Management		•	
10. Memory Management	•		
11. Emissions Management			•

In Table 5, the security requirements from SDR Forum Document DL-REQ, Requirements for Radio Software Download for RF Reconfiguration [SDR Forum, 2002b] have been mapped into the 11 security requirement categories originally defined by Fitton [2002] and revised by Cook [2003]. This mapping is provided in Appendix A.

Good security design requires that all of these requirements be included to ensure a secure design. This is a list of "best practices" as established by security experts. Note that several of these requirements require a public key infrastructure (PKI). A PKI is needed to sign the software and configuration parameters for SDR-enabled devices, as well as to create and revoke the digital certificates used to certify compliance.

Table 6 provides specific security requirements that have been mapped into the 11 security feature categories described in Section 3 [originally described by Fitton, 2002] and Cook [2003]. In Table 6, the words "MUST," "MUST NOT," "SHALL," "SHALL NOT," "SHOULD," "SHOULD NOT," "RECOMMENDED," "MAY," and "OPTIONAL" are to be interpreted as described in RFC 2119 [IETF, 1997]. For the convenience of the reader, the definitions of these terms are provided in Appendix E. In this document the term "security measure" refers to a concept similar to "security objectives" in the Common Criteria. These objectives are derived from the threats, policies, and assumptions in the security environment, and they flow into the actual security requirements.

Table 6 Specific Security Requirements that Should Receive Consideration in an SDR Context[a]

Security Requirement for Operational Software Download, Storage, Installation, and Instantiation	**Level of Importance[b]**	**Examples in an SDR Context[c]**
Security Measure Category 0 -- General Requirements (These are requirements that span more than one of categories 1-11 from Table 5.)		
The cryptographic level of the algorithms used should be consistent with the current state of the art, commensurate with the equipment, consistent with the application security required, and designed to prevent a dedicated attacker from using weaknesses in the algorithms to modify the specified operation of the equipment. This requirement crosses all categories.	SHOULD	Security should be a balance of complexity versus the threat to the impact on the device and the network. For example, threats to the radio emission characteristics require stronger security protection mechanisms than threats to voice coders..
Support Discretionary Access Control for objects in the file system. This category crosses Categories 4, 6, 7, and 10.	SHALL	Creator of file is the owner and can grant or deny permission to read/write/execute for other users.
Include a unique nonalterable identifier (e.g., serial number). This requirement crosses Categories 4, 6, and 8.	SHALL	Same example as above.
Prevent an unauthorized user from changing the device configuration. This requirement crosses Categories 4, 6, and 8.	SHALL	Same example as above.
Security Measure Category 1 — Security Policy Enforcement and Management Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C		
Support the enforcement of policies for multiple jurisdictions.	SHALL	Devices that cross international borders under differing type acceptances.
.Prevent unauthorized users from altering national regulatory compliance elements within the jurisdiction of operation.	SHALL	Type acceptance could not be violated, or the level or type of download be constrained, based on jurisdiction.
Mechanisms are required to determine security primitives for hardware/software combinations in conjunction with capabilities/service	SHALL	Security policy in a given jurisdiction enforces conformance to local type acceptance by not allowing certain operations to occur even if valid in other jurisdictions.

Security Requirement for Operational Software Download, Storage, Installation, and Instantiation	**Level of Importance**[b]	**Examples in an SDR Context**[c]
Security Measure Category 2 — Information Integrity **Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C**		
Ensure data integrity by cryptographic means.	SHALL	Failure to perform a data integrity check allows attacker to replace stored security data with their own versions.
All communication between the software download servers and clients must be integrity protected.		Avoid transmission path being compromised.
Ensure the integrity of system reconfiguration information by cryptographic means.	SHALL	Device management could not be purloined by attacker.
If a mathematical calculation is used to ensure information integrity, the calculation result be encrypted or otherwise protected by a suitable authentication mechanism to ensure that the calculation result has not been altered.	MUST	Failure to encrypt the value used for integrity checking will allow a user to replace security data and the integrity value with their own version.
Verify the source/origin.	SHALL	Trusted source verification and auditing. See Figure 5.
Ensure the integrity of the downloaded software components prior to execution.	SHALL	Use a checksum or maybe even forward error correction to ensure that the software has not been corrupted during transmission.
Security Measure Category 3 — Authentication and Non-repudiation **Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C**		
Provide authentication of download providers prior to download.	SHALL	Prevent download from a rogue server; an example of this in the Internet world is “phishing.”
Provide authentication of the device itself to the download providers prior to download.	MAY	Authentication of device is needed for billing, registration, and update of services.
Support non-repudiation of receipt of downloaded software.	MAY	A client cannot deny having received an update.
At least one signature should be used for download and storage with the number of signatures increasing with each additional entity responsible for device deployment and operation The number of minimum signatures increases from one signature to two or more when the device is operating in licensed spectrum.	SHOULD	One signature for the device manufacturer or software creator, another for the OEM or network operator, a third signature if there is any regulatory or certification entity.
The same signature tree should be used for the download, storage, installation, and instantiation of ancillary software (e.g., operating systems, drivers, middleware); one signature from the originator of the software and one signature from the network operator.	SHOULD	Same example as above.

Security Requirement for Operational Software Download, Storage, Installation, and Instantiation	**Level of Importance**[b]	**Examples in an SDR Context**[c]
Security Measure Category 4 — Access Control (Includes Authentication Processes) **Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C**		
Support Digital Rights (DRM)-controlled applications where required by vendors or owners of the software.	SHALL	Proprietary telephony codes/applications must be safeguarded. DRM is the standard method for providing control access and distribution of protected content.
Support differentiation of roles in download process.	SHALL	Administrator role is authorized to perform reconfiguration (e.g., network operator). Monitor role is authored to query device (e.g., manufacturer allowed to see revision status) Some fundamental properties of the SDR should be changeable only by authorized individuals.
Protected memory and digital signatures utilized to ensure the proper access to software by authorized entities.	SHALL	MExE use of class marks (see Section B.1.1 and Figure B-2)
Respect customization preferences (user, network, operator).	SHALL	Changes to base-station radios need to accommodate specific system configurations that have been defined to avoid loss of customization parameters by operator.
Support a hardware ID that cannot be changed.	SHALL	Similar to the 48-bit Ethernet MAC address that uniquely identifies every device; should be changeable by nobody; can be used for configurations, for software download, and device authentication for applications that are user-agnostic
Security Measure Category 5 — Encryption and Decryption **Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C**		
Maintain the confidentiality of user identity information in the air.	SHALL	SIM-type information if needed for reconfiguration management.
Store private cryptographic keys securely.	SHALL	Service provides assigned keys for reconfiguration that are embedded in device.

Security Requirement for Operational Software Download, Storage, Installation, and Instantiation	Level of Importance[b]	Examples in an SDR Context[c]
Prevent unauthorized users from access to another user's private cryptographic keys.	SHALL	Multiple keys present in device — perhaps a key for radio characteristics of band, mode and power; another key for voice coder; and so forth.
Public cryptographic keys (root keys) used to verify certificates be stored so that the value cannot be modified without proper authorization.	MUST	Could be stored in non-volatile memory or read-only memory; user certificates are only as trustworthy as the root and its intermediates.
Verify the integrity periodically during execution.	SHOULD/MAY	For medium security applications, the checksum is verified at every invocation. For high security applications, a periodic self-test examines the desired checksum with the actual checksum of the software in memory.
The data link between the server and the client device be confidentiality protected.	MAY	If there are multiple download actors, they should be segregated into individual protected conduits
Prevent unauthorized users from altering critical system parameters/data.	SHALL	Control should be consistent with the authorization chains in Figure 5. Critical data such as security profiles, configuration version numbers, RF, or power should not be modifiable by owner of the device.
Support data confidentiality when requested by the user or provider.	SHALL	Examples would be the downloading of a special purchased codec or vendor-supplied code that is not intended for other users.
Security Measure Category 6 — Key and Certificate Management **Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C**		
Crytographic keys be stored in non-volotile storage. Key lengths, formats and key tags identifying the function of the key, expiration dates are requirements that MAY need to be standardized. How, when, and where keys and certificates are updated and replaced and what security mechanisms are required to protect these items whle they are in transit from the point of creation until they are stored in protected memory of an SDR device are requirements which MAY need to be standardized.	SHALL	Similar to the 48-bit Ethernet MAC address that uniquely identifies every device; should be changeable by nobody; can be used for configurations, for software download, and device authentication for applications that are user-agnostic. Not subject to hacking.

Security Requirement for Operational Software Download, Storage, Installation, and Instantiation	Level of Importance[b]	Examples in an SDR Context[c]
Security Measure Category 7 — Standardized Installation Mechanisms **Applicable Block in SDR Forum Reference Model – 1C**		
Include installation and user guidance with each product.	SHALL	Relevant information on enabling or disabling download if controlled by a user and/or how to initiate download if permitted. Instructs the user on how to securely update a device; required for even the lowest level of security certification.
Include a common central installer that controls all installation processes within the device.	SHOULD	Avoid difficulty of managing differing and/or potentially conflicting mechanisms.
Security Measure Category 8 — Auditing and Alarms (e.g., the receipt of an improperly signed software download should be recorded). **Applicable Blocks in SDR Forum Reference Model — 2A, 2B, 2C**		
Audit pertinent recorded security parameters affecting terminal operations and download parameters including source, time, data identity and other metadata.	SHALL	Relevant and appropriate data are captured and made available for subsequent forensics or tracing (e.g., provide alarms for the following events: (1) detectable operational anomalies and power anomalies; (2) the receipt of an improperly signed software download; (3) numerous failed attempts for password entry).
Security Measure Category 9 — Configuration Management **Applicable Block in SDR Forum Reference Model — 1C**		
The terminal device or network that supports the SDR device maintains an installation log that lists details of the SDR device configuration as well as the identifier and version number of all installed software.	SHOULD	In cellular environment these elements are needed for device management.
Security Measure Category 10 — Memory Management **Applicable Block in SDR Forum Reference Model — 1C**		
A memory protection mechanism must be employed.	SHALL	During software security execution, the memory space used by the security method should not be alterable by other simultaneously executing applications (i.e. buffer-overflow attacks)

Security Requirement for Operational Software Download, Storage, Installation, and Instantiation	**Level of Importance**[b]	**Examples in an SDR Context**[c]
Security Measure Category 11 — Emissions Management **Applicable Block in SDR Forum Reference Model — 1C**		
Comply with regulatory emissions standards in the jurisdiction of operation.	SHALL	Avoid radio operations not consistent with regulations of relevant jurisdictions.

[a] The use of this table should not be construed to be a generic requirement imposed on commercial wireless devices. It is intended to be a set of requirements that are deemed to be important when implementations are undertaken utilizing SDR concepts *and* download of operation software is provided for. The need for any specific requirement listed can and may vary with specific implementations.

[b] The Level of Importance column utilizes accepted industry terminology to convey in this usage only the level of attention that should be accorded to a particular requirement. It is not a specification for implementation of any specific product.

[c] The examples in this column are provided only to illustrate the meaning of the specific requirement.

4.2 Additional Requirements from Different Perspectives

4.2.1 Operator Requirements

Operator requirements for SDR are described in Alvarez et al. [2003]. The operator requirements include requirements for base-station and terminal reconfiguration, billing, and global interoperability. These general requirements spawn specific security requirements. Many of the security requirements described by Alvarez et al. are similar to those listed under the general requirements. The following specific security requirements, however, are particularly relevant to operators:

- The reconfiguration process must be under the control of authorized entities (the qualifying authority depicted in Figure 5). Operators must have visibility of what is on the terminal and what is being downloaded to the terminal; thus the operator is at least one of the principal qualifying authorities.
- The network signaling information must be protected.
- The performance and capabilities of the equipment must be protected.
- Network functionality that supports the reconfiguration process must be protected.
- The potential availability of open interfaces that will allow both trusted and untrusted[3] third parties (as well as the base-station and terminal device manufacturers) to develop new software radio modules for base-stations and/or terminal devices is of concern to operators. If not allowed, some of the advantages associated with reconfigurability will be lost, as the introduction of a new technology or capability will depend on its availability from the original equipment manufacturer. This leads to additional certification and control issues due to a potentially larger security threat of download and installation of malicious or defective software in the units in question.
- Currently the usual source of operational software for the terminal is the manufacturer, but if the interfaces to the underlying hardware are made public (and especially if these interfaces are standardized and used by a wide range of manufacturers), there may be a series of untrusted (and/or unintended or undesired) third-party companies developing many types of operational software for the terminal. This increases the chance that defective or malicious software will be created, downloaded, and installed. Therefore, certification that the software has undergone appropriate testing to ensure its proper operation and is under the control of the appropriate qualifying authority and distribution authority is mandatory.
- Operators are concerned about how SIM/USIM should be involved in the authentication procedures to certify that some changes in the device can be made only if the operator allows/recommends this. Consideration should be given to whether or not even the secret key, or part of it, could be located in the SIM/USIM.

[3] "Untrusted" is a particular and high-magnitude concern, especially if an unintended and undesired source.

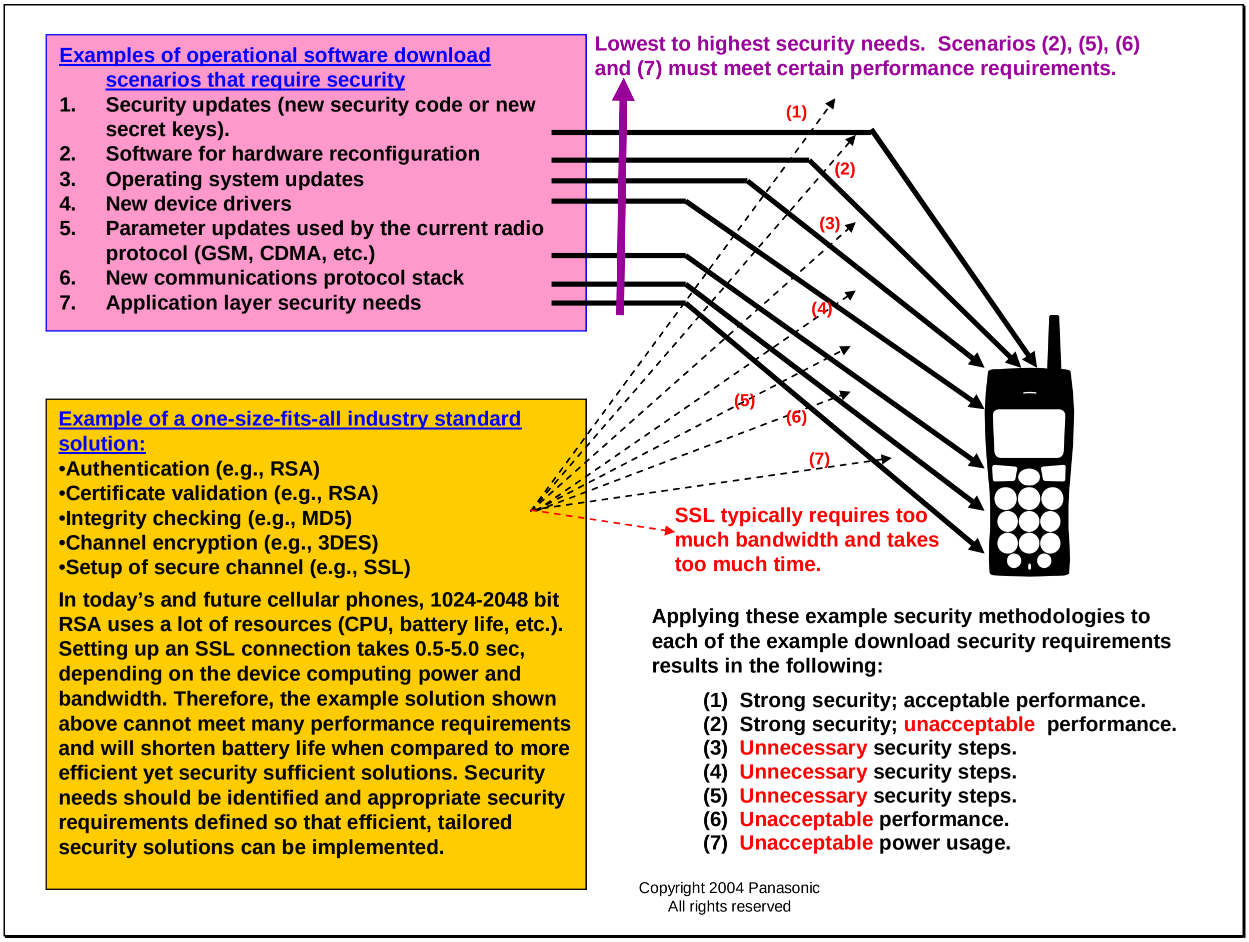
4.2.2 Manufacturer Requirements

There is agreement within the SDR Forum that as long as there is no other reasonable alternative, the hardware manufacturer has the responsibility for the proper operation of his equipment. This includes the manufacturer responsibility to prevent software being loaded to his equipment unless the software download and installation is manufacturer authorized. This view is also the current view of regulators around the world.

The need to securely update firmware/device configurations is increasingly important. Device configuration affects basic features of devices, and thus compromising it may lead to severe liability to manufacturers. For example, misconfiguration of an SDR device may violate spectrum regulation requirements. Specific issues from a manufacturer's perspective include:

- Existing secure download mechanisms (e.g., SSL) are not flexible or efficient enough to accommodate the wide range of devices and their security requirements and capabilities.
- Resource capacity is diverse (resource starved, resource rich).
- Diversity exists in degree of liability when security is violated; for example, a ring-tone glitch has less impact than modification of radio configuration).
- Current security technologies provide a "one-size-fits-all" approach to configuration download security. However, one-size-fits-all solutions provide security that is either too much, too little, or too costly. It is *very* inefficient. Such solutions cannot accommodate all commercial wireless devices with a wide dynamic range of capabilities and resources and present different degress of liability to the secure download mechanism.
- In a single commercial wireless device, different downloadable modules require different levels of security due to the range of liabilities carried by these devices. Current security solutions do not address this problem. For example, reconfiguring an MPEG encoder/decoder is not as mission critical as reconfiguring an FPGA used for baseband filtering.
- Current technologies for authentication, certificate verification, and key exchange need too much CPU power and memory resources.
- Security has many associated costs:
    - Processor and memory costs
    - Hardware footprint costs
    - User costs
    - Cost of failure (security is broken)
    - Cost of continued certification and accreditation
- The cost of security must be properly balanced with its benefits.
- To provide the best service to the consumer while satisfying security requirements, a CE device should contain multiple pluggable security mechanisms.

Figure 9 illustrates how different software DSII scenarios lead to different levels of security requirements. Thus, a one-size-fits-all solution is an issue of concern to both manufacturers and operators.



Examples of operational software download scenarios that require security

1. Security updates (new security code or new secret keys).
2. Software for hardware reconfiguration
3. Operating system updates
4. New device drivers
5. Parameter updates used by the current radio protocol (GSM, CDMA, etc.)
6. New communications protocol stack
7. Application layer security needs

Lowest to highest security needs. Scenarios (2), (5), (6) and (7) must meet certain performance requirements.

Example of a one-size-fits-all industry standard solution:

•Authentication (e.g., RSA)
•Certificate validation (e.g., RSA)
•Integrity checking (e.g., MD5)
•Channel encryption (e.g., 3DES)
•Setup of secure channel (e.g., SSL)

In today's and future cellular phones, 1024-2048 bit RSA uses a lot of resources (CPU, battery life, etc.). Setting up an SSL connection takes 0.5-5.0 sec, depending on the device computing power and bandwidth. Therefore, the example solution shown above cannot meet many performance requirements and will shorten battery life when compared to more efficient yet security sufficient solutions. Security needs should be identified and appropriate security requirements defined so that efficient, tailored security solutions can be implemented.

SSL typically requires too much bandwidth and takes too much time.

Applying these example security methodologies to each of the example download security requirements results in the following:

(1) Strong security; acceptable performance.
(2) Strong security; unacceptable performance.
(3) Unnecessary security steps.
(4) Unnecessary security steps.
(5) Unnecessary security steps.
(6) Unacceptable performance.
(7) Unacceptable power usage.

Figure 9. Example of how different software download scenarios lead to different security solutions

4.2.3 End-User Requirements

As noted in Table 2 (Section 2.2), the end user is primarily concerned about the application software download and privacy issues related to software download and any access to the user's wireless device by unauthorized individuals. Although the end user is interested in new service capabilities and features resulting from operational software download (e.g., a new air interface), the end user does not have any unique security requirements related to such downloads. Personal privacy issues are not specifically addressed in this document, although some of the technologies used to address personal privacy are applicable to operational software DSII security issues.

4.2.4 Regulator Requirements

There is general interest in software defined radio by a number of regulatory agencies (RAs). As noted in Table 2, regulators are primarily concerned with the security of radio software. They are less concerned about the security of other types of operational software (e.g., operating systems) unless download of these other types of software could either inadvertently or intentionally cause improper operation of the radio software.

In the application arena, the failure of the application such as a game may result in disappointment of the customer with no additional harm done. In the radio software arena, failure of the radio software, such as frequency selection and modulation, may result in a customer having a non-functional radio device or, worse, a device that functions inappropriately and disturbs other users or other radio services. The mechanisms to download may be the same, but the specifics and scope can vary to satisfy the imposed criteria. The following regulatory requirements apply to one component of operational software, namely, radio software:

- Regulators require, in general, that the device must provide some means of indicating its current “type approval” or “conformance acceptance,” often a physical label attached to the device. However, the specific need with SDR is that the indications must be associated with the radio configuration that is downloaded because the radio characteristic of the device is changed after a download and reconfiguration. Consequently, the currently accepted practice of a physical label becomes untenable. Therefore, download and device management may need to include how an electronic variant (proposed in some regulatory jurisdictions) of this labeling might be accommodated and how the device could provide information as to its current version/variants.
- Regulators require that the radio must not be able to operate with an unapproved configuration. Therefore, a security mechanism must be built into the radio to prevent malicious or accidental reconfiguration.
- Regulators may require a “stronger” authentication for radio software download. Verification of a downloaded module may need different techniques than other downloads.
- To support the interest of regulators, the reconfigurable device should support a feature whereby it is possible to carry out a post-download audit to ensure that the radio software executing in the device is an approved software load for that device.

The requirements for ensuring proper operation of reconfigurable wireless devices are common to all regulatory agencies worldwide. The various regulatory agencies have somewhat differing approaches as to how these requirements should be satisfied, however. Some of the differing perspectives of different regulatory agencies is provided in the following subsections. Also, in different regulatory jurisdictions, the actors who are responsible for carrying out the solution may not be the same.

4.2.4.1 Perspective of Regulatory Requirements in the United States

The FCC's First Report and Order [FCC, 2001] stated that industry standards organizations are still investigating security issues, and further stated, in paragraph 32:

> We continue to believe that the best approach is to rely on a general requirement that manufacturers take adequate steps to prevent unauthorized changes to the software that drives their equipment.

The FCC [2001] also asserted that it may need to specify more detailed security requirements at a later date as software defined radio technology develops. Thus, it is clear that in defining the operational software download problem, it is necessary to define the timeframe being addressed. The FCC, in December 2003, issued a Notice of Proposed Rule Making and Order [FCC, 2003], which, inter alia, asked for comments on the following:

> We, therefore, believe it is time to revisit the SDR rules to determine if changes are needed concerning whether the SDR rules should be permissive or mandatory, the types of security features that an SDR must incorporate, and the approval process for SDRs that are contained in modular transmitters.

In particular, the FCC is investigating the following statement from the preceding NPRM [FCC, 2001]:

> Required SDRs to incorporate security features to ensure that only software that is part of an approved hardware/software combination can be loaded into an SDR. The exact methods are left to the manufacturer.

The FCC is investigating whether to require that an SDR-capable device be declared as such or whether this is left as an option to the manufacturer asking for a license for the device.

4.2.4.2 European Perspective of Regulatory Requirements

As noted by Babb et al. [2002], there are three types of rules:

1. Regulatory: For a mobile phone to carry the European Community's CE mark it must conform to the radio parameters (radio frequency, interference, etc.) and safety regulations in force throughout the European Union.
2. Type approval.
3. Operator approval: Assurance that the phone functions in the desired manner when connected to a particular operator's network.

The Telecommunication Conformity Assessment and Market (TCAM) Surveillance Committee in Europe has developed a questionnaire regarding SDR and is evaluating the results of that questionnaire. It is not anticipated that security requirements for operational software download will be substantially different from those of other administrations.

Faroughi-Esfahani et al. [2002] provide a summary of the European perspective of reconfigurable systems, including a view of the regulatory changes between the present and the future.

4.2.4.3 Japanese Perspective of Regulatory Requirements

A Japanese perspective of SDR regulatory issues is provided by Suzuki [2002], who identifies the following regulatory issues related to software download security:

1. Security system for granting certification and preventing illegal modification of SDR equipment
2. Test methods that permit hardware and software to be tested separately
3. Configuration control of modification history

The last two items are particularly significant, and considerable ongoing research in Japan is particularly related to the second item [Harada, 2003; Harada et al., 2003; Suzuki et al., 2003a, 2003b, 2003c].

4.3 Standardization Requirements

The requirements discussed in Section 4.2 drive the standardization requirements. Watanabe et al. [2003] categorize the requirements as follows:

1. Secure downloading framework and associated mechanisms and protocols
2. Certification mechanism of configuration data
3. Management and control framework of configuration data
4. Standardization of a description language

The SDR Forum view is that the requirements and security criteria must be standardized, not the specific implementations that are designed and developed to meet the requirements and criteria. Additional security specifications may not be needed beyond those either already in place or in the process of being developed by other organizations. Two aspects of the criteria must be specified:

- What kinds of protection mechanisms are required?
- How can the manufacturer demonstrate that the security mechanisms employed in the manufacturer's device/system satisfy the criteria and regulatory policies?

4.4 Protection Profile Requirements

One tool for defining system security architecture is a Protection Profile, which is a description of system vulnerabilities, threats that might take advantage of them, levels of comparative economics, and measures taken to mitigate the associated risk. Appendix D provides a set of tutorial charts that describe the Common Criteria and Protection Profile methodology.

In an effort to define the secure download problem, the SDR Forum is reviewing the importance of a Protection Profile that follows the methods used by formal certification laboratories in the context of commercial wireless SDR. Simply stated, a Protection Profile is the definition of what is being protected, what it is protecting against, what organizational policies it must adhere to, and what assumptions govern its operation. Protection Profiles are requirements documents, not implementation documents. The material in this section is not a full Protection Profile as outlined in Appendix D. However, this material is indicative of a potential view on a Protection Profile for secure software download.

4.4.1 What Is and Is Not Being Protected

This document limits the scope of an SDR Protection Profile to include only software modifications to the system that are the result of the download process. Attacks to the system or radio that are not initiated from the download, storage, installation, and instantiation processes, such as physical attacks or component changes whether initiated by a manufacturer or user, will not be included within the download profile. Also software attacks that originate from a change to the environment that is the result of introducing new code or system updates done through a process outside of a software download will not be protected within this profile.

Within the Software Defined Radio download process, the SDR community is trying to achieve several targets and has defined the protection profile to protect the following boundaries:

- The radio system should operate only when connected to known approved hardware.
- The radio system should operate only when it is loaded with approved software.
- Components of the radio system should be easy to change for an authorized entity.
- The radio system should operate in a tested and defined manner at all times, including during unexpected system events or failures.

A software download can be initiated from a number of sources. It can originate from a trusted entity such as the service provider or manufacturer, or from an untrusted entity such as the radio end user. Each of these sources may be aware or unaware of their actions. The profile will include actions by all types of download originators whether or not they are deliberate in their actions.

4.4.2 What We Are Protecting Against

It is understood that the protection profile protects against a limited list of security threats. These threats can be divided into classes. Each of the following classes is identified, followed by some representative examples of the types of threats found in the class.[4] Because new threats occur regularly, the list is primarily a guide to determining these threats.

- *Class 1: Modifications that affect regulatory characteristics or safety provisions of the device (including loss of data integrity).* This first class of threat includes modification of

[4] The threats described in the following subsections were provided by Intel and are similar to the threats described in Appendix C, which is an input contribution to the SDR Forum by Siemens [Falk et al. 2002].

the device to increase or decrease transmitter power. Examples include modification to the transmission or receiver characteristics to operate outside specified frequencies, and in general any change to the spectral definition of the radio device

- *Class 2: Modifications that affect system performance or malicious operation. This class of threat attacks or circumvents the system processes. Processes that are targeted can include security modules, billing operations, or enable features or functions that are not authorized to the existing customer.*
- *Class 3: Modifications that cause system failure, interruption or degradation.* This class of threat includes anything that affects the performance of the system is operation. Attacks will slow down operation, cause the system to fail, or permit interruptions from the normal flow or operation.
- *Class 4: Modifications that impact user privacy or allow credential theft or illegal system access.* This type of threat is the most common deliberate threat. It involves acquiring information that is not intended for the attacker.

The following scenarios are classified by threat. It is not important here to identify whether the attack is accidental or deliberate. These scenarios motivate the need to further investigate and understand security issues when involved with download/reconfiguration and were used to derive the security objectives listed above.

4.4.2.1 Class 1

- *Invalidation of Conformance Requirements*
  Regulatory bodies pose requirements on radio equipment concerning user safety, electromagnetic compatibility (EMC immunity, EMC emission), and radio spectrum use (e.g., blocking, spurious emissions, transmitter requirements). Conformance with these requirements has — depending on the regulatory procedures —been tested by either a regulatory body or an authorized testing house, or it has to be asserted by the manufacturer by stating conformance (self-approval). Reconfiguration poses the threat that radio equipment is altered in such a way as to invalidate the conformance requirements during the operation of the equipment.
- *User Safety*
  Reconfiguration of radio equipment could, when the hardware allows, even endanger the health and safety of the user — for example, when radiated power is too high.

4.4.2.2 Class 2

- *Download and Execution of Malicious Software*
  Software download is a key component for reconfiguration, particularly in the post-manufacture environment. It poses the threat that malicious software is downloaded that causes harm by accident or by intention. The software could simply not work properly or not implement the expected functionality and thereby pose a threat to reliability and availability. It could as well, however, intentionally implement malicious functionality as, for example, dialing premium rate numbers in the background, or any other of the threats described below.

- *Modification of Other Functionality*
  The purpose of a reconfiguration is to modify certain properties or functions of reconfigurable equipment. Other functionality not intended or authorized to be reconfigured could be affected by a reconfiguration.

- *Circumvention of Security Functions*
  Security functions — for example, for secure network access to a cellular system or an Intranet or for m-commerce — have to be trustworthy themselves, but rely furthermore on secure storage of and protected access to cryptographic material and policy information. Unprotected reconfiguration could help to weaken or circumvent security functions not related to reconfiguration and thereby make them useless.

4.4.2.3 Class 3

- *Unreliable Operation*
  A configuration could be installed and activated that does not work at all or works improperly. The consequence would be unsatisfied users and high costs for customer care for the service provider. Also, reconfiguration servers, software, and configuration information required to perform a reconfiguration could be unavailable or not function properly.

4.4.2.4 Class 4

- *Disturbing Other Users or Other Radio Systems*
  Reconfiguration could lead to emissions that harm other users and radio systems. In addition to emitting in unauthorized frequency bands, using too high power, or using wrong modulation schemes, access to the radio medium could be modified in ways that have a negative impact on other users. Because a single user or a small set of users could have an advantage in using “improved” configurations that implement unfair behavior, this threat shows that the user cannot be given full control over reconfigurable equipment. This threat is obviously related to conformance requirements, but its scope is broader when certain properties are required by operators or non-regulatory standards — for example, using the assigned spectrum efficiently and providing good service to all customers.

- *Disregard of Preferences*
  Communication services could be used that do not match the preferences and expectations of the end user concerning services available, quality of service provided, and the cost involved. Also the preferences of service providers and network operators could be disregarded. Because the intentions and preferences of users, different network operators and service providers could be contradictory, this point is not easy to solve. An example of possibly contradicting preferences is the selection of the radio access technology and network. Whereas users would probably prefer the cheapest technology that suits their service requirements, operators obviously have an interest in the usage of the most profitable service and network, and especially a service and network they themselves offer.

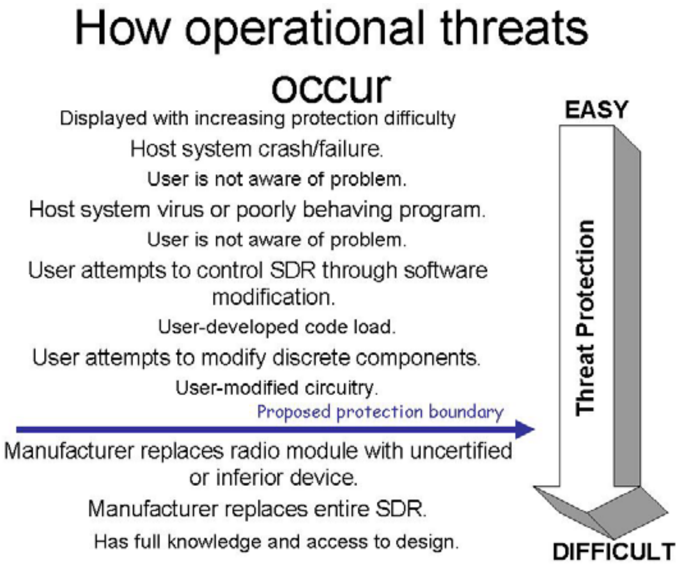
- *Manipulated Reconfiguration*
  The reconfiguration of terminal equipment will be supported by functions in the network— for example, to assist or perform mode monitoring or the mode switching decision. The reconfiguration process will be distributed among several entities in the fixed part and the mobile part of the communication system. Information used or even required for the reconfiguration or any other information exchanged between the involved nodes can be manipulated, and therefore the reconfiguration process could be influenced in illegitimate ways.

- *Easier Attacks*
  Reconfiguration could also make attacks against the wireless communication system easier and bring it in the range of a greater base of potential attackers. Attackers no longer have to rely on such expensive equipment as signal generators or spectrum and protocol analyzers, nor do they have to build their own special equipment involving, for example, reverse engineering and modification of proprietary, highly integrated devices. Instead, they have easy access to open interfaces and can simply reconfigure off-the-shelf equipment according to their intentions.

- *No, or Insufficient, Protection of Intellectual Property*
  Both hardware and software manufacturers have an intention to protect their development effort and to receive fair compensation. Reconfiguration could make reverse engineering easier, and software could be used or copied illegally. When the user or the service provider can freely add desired features, differentiation of products by supported features will not work in the same way as for current equipment.

- *Illegitimate Access to Private Information*
  Sensitive information is required for reconfiguration. Access to information about the end users' preferences, used services, or the current location and configuration has to be controlled to protect the private sphere of a user. Additionally, information related to a service provider or a network operator can be required to be kept confidential when the involved companies do not want to share data about their customers or network internals with competitors.

Figure 10 represents a list of threats of increasing severity, starting with unexpected actions and proceeding to user-initiated efforts and going all the way to knowledgeable manufacturers circumventing regulations. With each increasing threat, the ability to protect radio devices against these threats grows in complexity. An indicator arrow is shown clearly identifying a proposed protection boundary, which includes everything that can be performed by an end user.



How operational threats occur

Displayed with increasing protection difficulty

Host system crash/failure.

User is not aware of problem.

Host system virus or poorly behaving program.

User is not aware of problem.

User attempts to control SDR through software modification.

User-developed code load.

User attempts to modify discrete components.

User-modified circuitry.

Manufacturer replaces radio module with uncertified or inferior device.

Manufacturer replaces entire SDR.

Has full knowledge and access to design.

Figure 10. Difficulty of protection versus the type of threat to operational software

5 Survey and Analysis of Operational Software Security Solutions for Commercial Wireless Devices

This section presents a brief analysis of existing specifications and standards relevant to DSII. It is based in part on Appendix B, which provides the results of a brief survey of existing and planned technical specifications and standards relevant to security for operational software DSII. These technical specifications are being developed by a number of standards fora. Only the most significant of the relevant specifications are summarized in Appendix B. The following subsections provide a high-level analysis of the results of this brief survey.

5.1 Unresolved Security Issues

As evidenced by recent reports of breaches to operational software security [see, for example, Reuters, 2004], unresolved security issues for operational software clearly exist. No breaches of security to the radio software component of operational software have been reported, however. Nevertheless, threats to all types of operational software, including radio software for SDR-capable devices as described in Section 2 and Appendix C (Section C-2), must be addressed. The requirements generated from these threats are provided in Section 4. The points to be emphasized here are:

- Security issues do exist that need to be addressed.
- Appropriate standards fora are in the process of addressing these issues.

Third-Generation Partnership Project (3GPP) security specifications and summarized in Appendix B. Several security issues have been identified in analyses of these security specifications conducted by others [Køien, 2004]. Several of these issues are related to wireless security for Universal Mobile Telecommunication System (UMTS) networks, including:

1. *Confidentiality and Integrity.* Confidentiality in UMTS covers both user-related system signaling and user data. However, integrity protection covers only system signaling (between the mobile station and the radio network controller) and does not cover user data [Køien, 2004].
2. *Inter-Network Security:* Mobile networks primarily use Signaling System No. 7 (SS7) for communication between networks for authentication, location update, call control, and so forth. The security of the global SS7 network as a transport system for signaling messages (including authentication messages) is open to major compromise [3GPP, 2000]. This is not a UMTS network security issue, but it nevertheless affects the security of UMTS networks.
3. *Security Features:* As noted in 3GPP's *A Guide to 3rd Generation Security* [3GPP, 2000], the network operator has many choices as to what security features of UMTS are implemented and used. Rose notes that it is very difficult to determine exactly what security is provided by operators [Rose and Køien, 2004]. He also notes that few of the early handsets support encryption and that many networks are running without any encryption at all. From the perspective of the manufacturers, this is problematic in regard

to radio software protection. As noted in Chapter 4, regulators at present continue to put the burden of proper operation of wireless devices on manufacturers. Therefore, the security provisions for radio software protection cannot be left optional to the operators.

As noted earlier, security is an end-to-end issue and not just a radio software security issue. All aspects of the networks that can affect the DSII to an SDR-capable device must be considered when considering security. Therefore, the issues delineated above are germane to the security issues considered in this document, even though if the root of the issue is outside the wireless network.

The cdma2000 security specifications have the same deficiency as the UMTS security specifications in regard to the user integrity protection, namely, that integrity protection applies only to system signaling information and not to user data. This could be a problem when trying to extend the existing 3GPP2 security specifications to cover operational software download scenarios. Rose and Køien [2004) note in comparing cdma2000 with UMTS that even though the details differ, the security philosophy for the two technologies is similar. Therefore, it is not surprising that the issues listed above on 3GPP UMTS security are the same as those for cdma2000 security.

5.2 Relationship Between SDR Forum Operational Download Security and OMA Security

The SDR Forum is an associate member of the Open Mobile Alliance (OMA). As a result, the Forum can directly provide input to OMA. In addition, companies that are members of both organizations can provide input contributions to either or both. An analysis of the OMA download, OMA device management requirements (including security), and OMA security documents illustrates some commonality of concerns about security issues that require the development of additional technical specifications. Therefore, there is *potentially* significant mutual interest between the SDR Forum security concerns and those of OMA. Figure 11 depicts the relationship between SDR Forum documents on download and security and the Open Mobile Alliance over-the-air download and security documents.

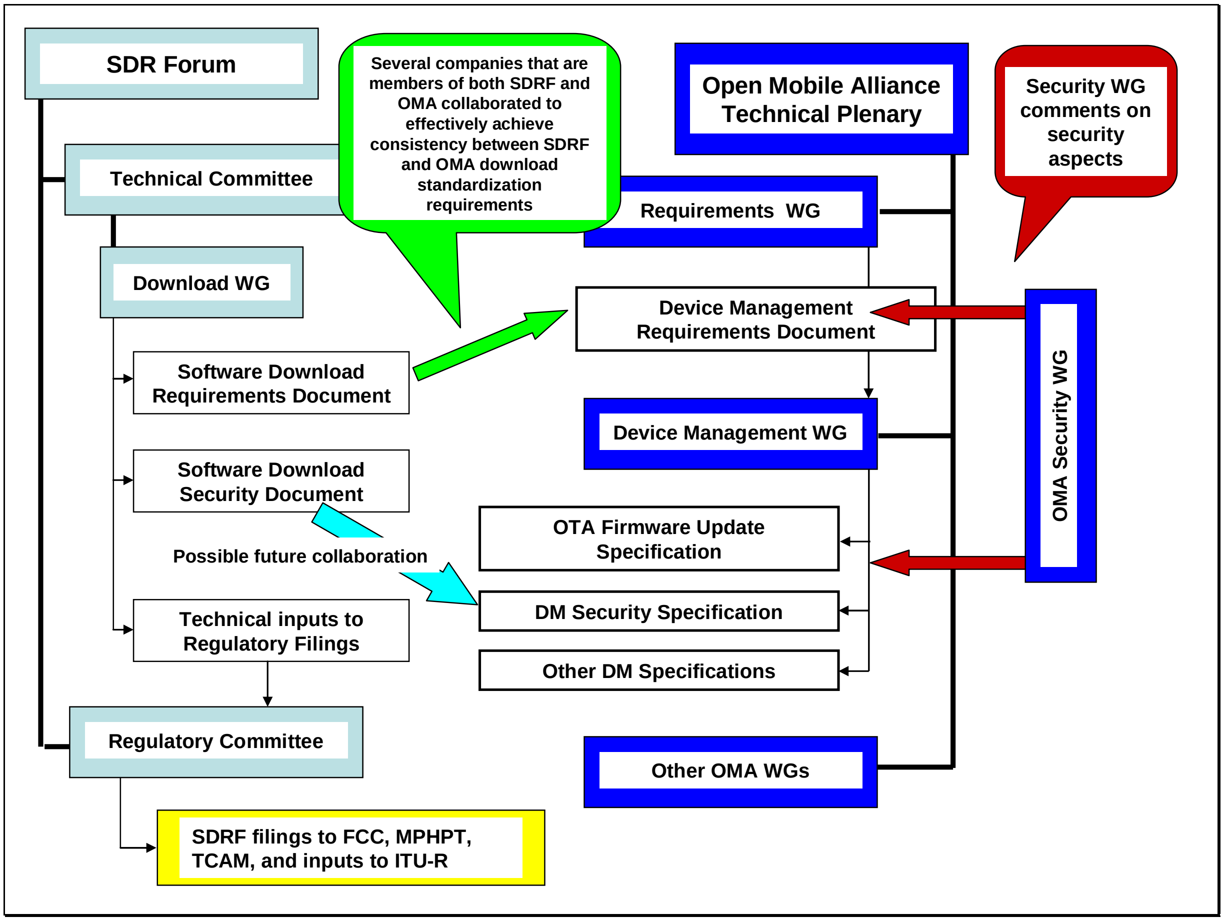

SDR Forum
Technical Committee
Download WG
Software Download Requirements Document
Software Download Security Document
Possible future collaboration
Technical inputs to Regulatory Filings
Regulatory Committee
SDRF filings to FCC, MPHPT, TCAM, and inputs to ITU-R
Several companies that are members of both SDRF and OMA collaborated to effectively achieve consistency between SDRF and OMA download standardization requirements
Open Mobile Alliance Technical Plenary
Security WG comments on security aspects
Requirements WG
Device Management Requirements Document
Device Management WG
OMA Security WG
OTA Firmware Update Specification
DM Security Specification
Other DM Specifications
Other OMA WGs

Figure 11. Synergism between SDR Forum and OMA documents

6 Introduction to Methods to Satisfy Operational Software Security Requirements

Security requirements change with time. Therefore, the solutions to meet these requirements also must change with time. This section provides a high-level overview of security solutions for both the near-term and mid-term as defined in the Executive Summary.

6.1 Introduction to Near-term Methods to Satisfy Operational Software Security Requirements

In the near-term, the source of operational software will be the commercial wireless device manufacturers, and regulatory approval will be required for all hardware and software combinations of radio software. Using this definition and these assumptions, in the near-term, security methods have been developed or are currently being developed that provide security for operational software download, storage, installation, and instantiation. These security techniques include those specifications summarized in Appendix B that provide data integrity assurances, data confidentiality, authorization and authentication, non-repudiation for the entire software DSII process.

Although many security technologies are available as measures to satisfy the requirements, the unique requirements for SDR devices in a commercial wireless domain cannot be met with a “one-size-fits-all” approach — this near-term issue was discussed in Section 4. Therefore, any security technologies that were summarized in Section 5 and Appendix B may not meet all near-term security requirements. Our preliminary assessment is that near-term security requirements that may not be fully met with existing technologies due to:

- Unique authentication, authorization, and accountability requirements
- Trust relationship based on the type of software being downloaded
- Resource constraints — limitations of processing power and memory
- International roaming considerations
- Controlled access considerations
- Existing security download mechanisms (e.g., SSL), which typically are not flexible or are not efficient enough to accommodate the wide range of devices

The above assessment will be further investigated as part of the SDR Forum’s ongoing work. Investigation into the “methods to satisfy” for the requirements in Table 6 is an ongoing work effort within the SDR Forum, as described in Section 7. Version 2 of this document will contain a full analysis of all of the existing security technologies versus the list of requirements provided in Section 4 (which will also be updated in Version 2).

The material presented below represents potential solutions. Information provided herein is based, in part, on an input contribution to the SDR Forum [Falk et al., 2002] (see Appendix C, especially Section C.4.2). The SDR Forum does not take any particular position on these solutions and neither endorses nor rejects any particular approach.

To prevent harm from potentially malicious software, two basic approaches can be taken:

- *Sandbox Method:* Manufacturers have implemented sandbox techniques.
- *Trust-Based Method:* Trust-based security technologies are widely used in commercial wireless devices and use signed content.

Signed content involves a trust relationship between the provider and the recipient and uses a central authority structure and security process methodology. This technology is currently widely implemented in commercial wireless devices.

Authentication methods by which the terminal can verify the software module to be loaded is a key component of security for operational software download and installation. Security standards that include authentication as a component of the security specification are being developed in the Open Mobile Alliance [OMA, 2003c, 2003d, 2004a]. In the meantime, as those standards are being completed, proprietary mechanisms for operational software can, and are, being used. This is not a problem because manufacturers are keenly aware of the criticality of protecting operational software and their ongoing responsibility for proper operation of their devices in conformance with applicable regulations. It is important, however, to standardize the firmware OTA update specifications and security aspects related to such updates, as the Open Mobile Alliance is doing. This work will continue throughout 2004 and early 2005.

The local storage in the terminal for reconfiguration modules also needs protection. Although the requirement is implementation independent, the solution to this requirement is likely to be proprietary because it is integral to the design of the commercial wireless device.

To limit illegitimate usage of software, digital rights management may be required. Such standards are being developed by the Open Mobile Alliance [OMA, 2004b].

In summary, many technologies are clearly available for meeting near-term requirements; however, additional technologies are needed due to the inappropriateness of the “one-size- fits-all” approach.

6.2 Introduction to Mid-term Methods to Satisfy Operational Software Security Requirements

This section provides an introduction to some of the ongoing research that is applicable to satisfying the mid-term security requirements for operational software download. The material presented in this section represents potential solutions advanced outside of the SDR Forum. The SDR Forum does not take any position on these solutions and neither endorses nor rejects any particular approach. Investigation into the “methods to satisfy” are ongoing work efforts within the SDR Forum, as described in Section 7.

The mid-term requirements include:

- Independent certification of hardware and software

- Validation and authorization of combinations of certified hardware and independently certified software
- Automatic calibration
- The availability of operational software from a trusted third-party vendor.

These issues will be addressed further in Version 2 of this document. This section of the present document is focused toward providing a brief review of some key ongoing research that is relevant to satisfying the mid-term requirements, including architecture and framework issues.

6.2.1 Research in Japan Relevant to the Mid-Term Software Download Security Issues

Considerable research in Japan has focused on security and related regulatory aspects of operational software download to SDR devices. Two sources of information regarding this research are:

- *IEICE Transactions on Communications*, December 2003: Special issue on software defined radio technology and it application [Harada et al., 2003; Suzuki et al. 2003a, 2000b, 2000c].
- Symposium on Download Security and Regulatory Issues, April 14, 2003, Keio University Mita Campus. This conference was held in collaboration with the SDR Forum.

These papers particularly address the mid-term issues of trusted third-party software, independent certification of hardware and software, automatic certification, automatic calibration, and standardization requirements. Of particular interest is the reporting on the testing that was conducted and the prototype systems that have been developed by the Telecom Engineering Center (TELEC) [Suzuki et al., 2003a, 2003b, 2003c].

6.2.2 Security Aspects of the European Commission E2R Research Program

The End-to-End Reconfigurability (E2R) Project is an integrated project (IP) of the 6th Framework Programme of the European Commission, addressing the core of the strategic objective “Mobile and wireless systems beyond 3G.” The E2R project consortium is composed of major manufacturers, operators, academia, and regulators.

E2R undertakes major R&D activities in Europe on reconfigurability in the commercial wireless sector including reconfigurable base-stations and reconfigurable cellular phones. E2R will provide an end-to-end reconfigurability solution that includes:

- all OSI layers including the physical layer
- both equipment and network architectures
- studies of the impact of the reconfiguration on the user service provisioning
- investigations of more efficient utilization of spectrum, radio and equipment resources

The E2R Programme, because it includes all aspects of E2E reconfiguration, includes security requirements for download and reconfiguration. The E2R Programme consists of six work packages. Work Package 3 concentrates on the support of reconfigurability of network entities and terminals by network functions for secure download, reconfiguration management and validation.

More information on the E2R Programme and descriptions of the work packages may be found at the following web sites:

- http://e2r.motlabs.com/
- http://e2r.motlabs.com/workpackages/index_html/view

It is anticipated that the results of this collaborative research will impact the availability of advanced security mechanisms and technologies in the mid-term as defined herein.

6.2.3 Wireless World Research Forum

The Wireless World Research Forum (WWRF) is a global organization, which was founded in August 2001. Members of the WWRF are:

- manufacturers
- network operators/service providers
- R&D centers
- universities
- small and medium enterprises

The Wireless World Research Forum has recently initiated work on security in the WWRF Security and Trust Special Interest Group (SIG2). This Special Interest Group is focused on identifying and promoting research areas that strive to understand and resolve the needs of users, operators, service providers, and other players for secure and trustworthy wireless systems. Resolving these issues is a necessary part of WWRF's mission to guide the research and development of applications, services, and underlying technologies. SIG2 will gather input and views from both industry and academia, synthesize these views to influence future visions and research priorities, and share results across the forum. It is anticipated that this research vision will influence the development of security technologies and methodologies applicable to commercial wireless operational software issues in the mid-term.

More information on WWRF can be found at: http://www.wireless-world-research.org/

6.2.4 Mobile Virtual Centre of Excellence

Mobile VCE is the operating name of the Virtual Centre of Excellence in Mobile and Personal Communications Ltd., a collaborative partnership of 23 mobile communications companies and eight UK universities. Mobile VCE began as a national initiative in 1996 but today operates as an international organization, reflecting the nature of the industry.

Mobile VCE is a collaborative partnership engaged in industrially led, long-term research in mobile and personal communications. Mobile VCE has pioneered new collaborative processes whereby its industrial members take a pro-active lead in defining and steering the research, which is undertaken by pan-university teams drawn from Mobile VCE's academic members.

The research scope and impact of Mobile VCE both have a global dimension with research contributions to such major international industry bodies as the Wireless World Research Forum and the Software Defined Radio Forum.

The research programme of the Mobile VCE is defined in its Core Programmes. The current programme (Core 3 Research Programme) extends from 2002 to 2005 and is structured into three work areas:

- Personal Distributed Environment
- Interworking of Networks
- Wireless Enablers

One of the primary research topics being emphasized in the Interworking of Networks area is the topic of security requirements and effective security architectures for interworked networks. It is anticipated that this Mobile VCE research will influence the development of security technologies and methodologies applicable to commercial wireless operational software issues in the mid-term. As noted earlier, the security issues associated with operational software download, storage, installation, and instantiation are end-to-end network issues; therefore the research being conducted in the Mobile VCE Core 3 Research Programme is relevant to the near-term requirements discussed earlier.

The Mobile VCE has published extensively its Reconfiguration Management Architecture (RMA), which is described in the SDR Forum System Security document [SDR Forum, 2002]. It uses a rule-based "Tag File" approach to ensure that only valid combinations are loaded in a terminal.

More information on Mobile VCE can be found at:
http://www.mobilevce.com/frames.htm?overview.htm

6.2.5 SDR Device Security Architecture Proposal

A secure SDR device architecture has been proposed [SDR Forum, 2003; Lam et al., 2003; Doan et al., 2002]. Key features of this architecture are:

- Separate hardware and software certification
- Radio Security Module (RSM) — A systems software module whose functionality includes installation, storage, operation, and termination of software in the terminal; when the terminal roams to another country, the RSM ensures that only software that is appropriate for use in that country is allowed to run.
- Global Positioning System (GPS) — Used to determine in which geographical location the wireless device is operating; this information can be used to determine appropriate

operational characteristics (frequency, power, modulation). This is an approach to supporting global roaming.

- Automatic Calibration Unit (ACU)

In considering this architecture, some key questions must be addressed, including:

- Is this a cost-effective solution for commercial wireless devices? Will commercial wireless device manufacturers that have a very small profit margin accept this architecture, which requires a separate microprocessor controlled chipset?
- Should GPS be required for a commercial wireless device? (This is part of the proposed SDR device security architecture.)
- Is this an architecture that can be or should be standardized?

6.2.6 Proposed Framework for Secure Operational Software

A number of papers present security frameworks and/or architectures for download to commercial wireless devices [see, for example, Fitton, 2002; Cook, 2003; Michael et al., 2002]. The framework of Fitton and Cook was discussed in Chapter 3 from the viewpoint of software download and installation requirements. The framework provided by Michael et al. [2002] provides solutions for verification of the declared identity of the source that produces the software to be downloaded, control and verification of the integrity of the downloaded data, disabling the ability to run unauthorized software on the SDR device, and secrecy of the downloaded data. The proposed system solution includes:

- Four cryptographic techniques
  - Secret/symmetric key
  - Public/asymmetric key
  - Cryptographic hashing
  - Digital signatures
- Tamper resistant hardware

Version 2.0 of this SDR Forum document will provide an assessment of this proposed security framework scheme to meet the requirements stated in Section 4 herein.

7 Future Work

Figure 12 depicts future work of the SDR Forum in download, storage, installation, and instantiation (DSII) security. The three boxes at the top of the diagram are SDR Forum documents that have already been completed, including this version of DL-SIN. As shown in the figure, the Forum will ask for comments on DL-SIN Version 1.0 via a formal RFI/RFC (Request for Information/Request for Comments). It is envisioned that Version 2.0 of this document will be developed as a result of the responses to that RFI/RFC. It is anticipated that DL-SIN Version 2.0 will include a richer suite of recommended security requirements. It is further anticipated that DL-SOL (see Preface) will provide example technical specifications related to "methods to satisfy" for both the near-term and mid-term solutions. Note in Figure 12 that the SDR Forum is intent on providing DSII security-related documents to various industry fora and regulatory agencies around the globe.

The RFI/RFC will be a request for additional *information*, including the following:

- Information regarding the applicability of this document:
    - What types of devices?
    - What markets?
- DSII security use cases
- DSII security threats and threat models
- Additional detailed requirements for DSII security
- Additional information for regulatory requirements from a global perspective and from each region of the world
- Information for two additional columns for Table 6 (Specific Security Requirements that Should Receive Consideration in an SDR Context)[5]
    - First additional column: For each requirement in the table, specify alternative examples of the methods to satisfy the requirement.
    - Second additional column: For each requirement in the table, specify which standards fora are working on a specification that includes a method to satisfy this requirement.
- Information and analyses of the completeness of technical specifications as examples of alternative methods to satisfy the DSII security requirements; this would result in an update of the information in Section 5 and Appendix B.
- Additional text for the alternative methods to satisfy the requirements for both the near-term and mid-term as we have defined these timeframes herein.

The RFI/RFC will also include a request for *comments* on the following;

[5] Note: The title of the table will change because it will include examples of methods to satisfy (i.e., solutions) as well as requirements.

- Specific comments on DL-SIN Version 1.0 and how this document can be improved to meet the needs of various stakeholders as delineated in Section 4.
- The desirability of creating one or more Protection Profiles for SDR devices that operate in the commercial wireless domain
- The need for a formal analysis regarding the balance of the cost of anti-tamper mechanisms versus the value of the information to be protected. The SDR Forum views that this is an important analysis that needs to be undertaken.
- Comments on future work and future inter-fora cooperation on DSII security requirements and solutions development

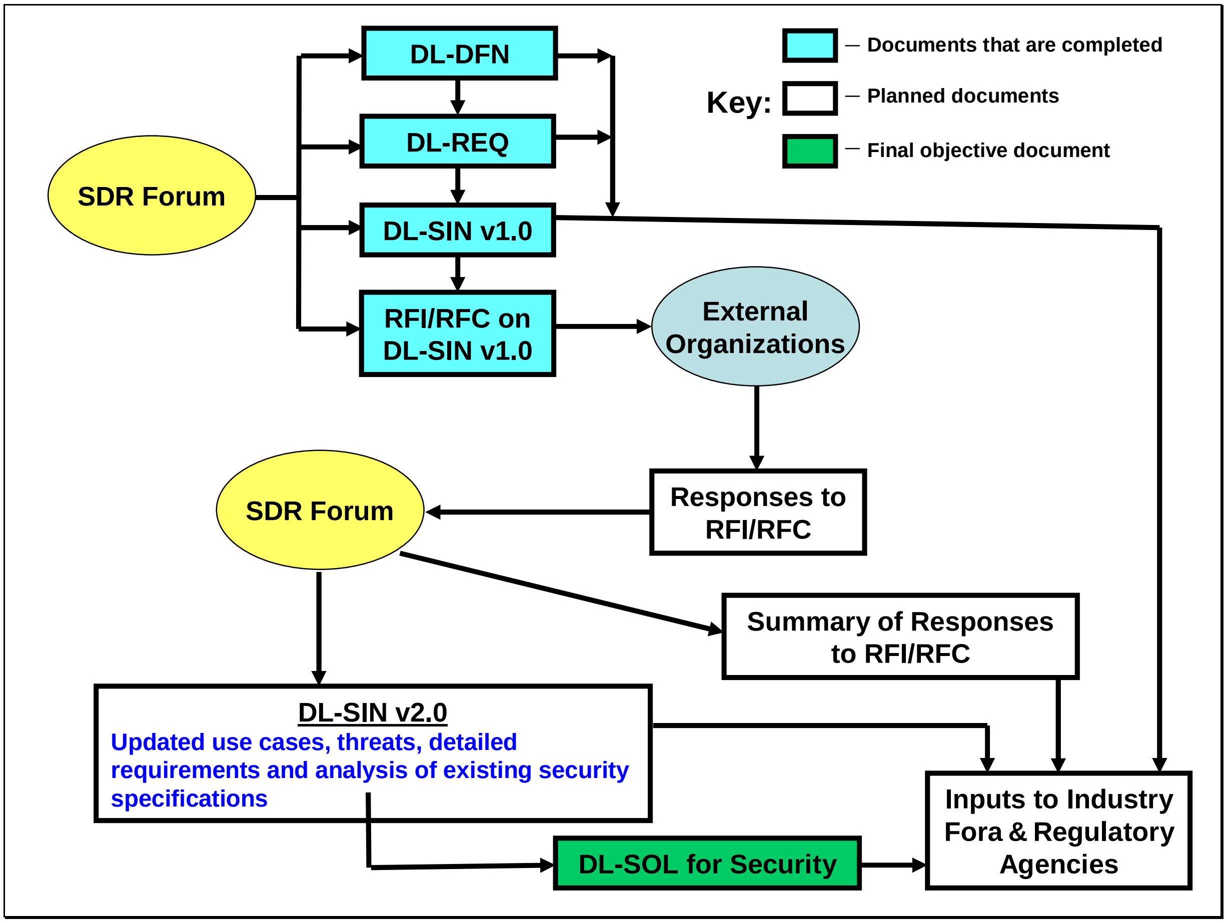

DL-DFN
DL-REQ
DL-SIN v1.0
RFI/RFC on DL-SIN v1.0
SDR Forum
Key:
– Documents that are completed
– Planned documents
– Final objective document
External Organizations
Responses to RFI/RFC
SDR Forum
Summary of Responses to RFI/RFC
DL-SIN v2.0
Updated use cases, threats, detailed requirements and analysis of existing security specifications
DL-SOL for Security
Inputs to Industry Fora & Regulatory Agencies

Figure 12. Future SDR Forum work on DSII security issues

8 References

3GPP (1999), *Universal Mobile Telecommunications System (UMTS); Security Principles,* UMTS 33.20 v3.1.0 (1999-02).

3GPP (2000), *A Guide to 3rd Generation Security*, 3G TR 33.90 0v1.2.0 (2000-01).

3GPP (2001a). *3G Security - Security Principles and Objectives,*3GPP TS 33.120 v4.0.0 (2001-03)

3GPP (2001b), *3G Security - General Report on the Design, Specification and Evaluation of 3GPP Standard Confidentiality and Integrity Algorithms*, 3GPP TR 33.908 v4.0.0 (2001-09).

3GPP (2001c), *3G Security — Security Threats and Requirements*, 3GPP TS 21.133 v4.1.0, (2002-12).

3GPP (2002a), *Mobile Execution Environment (MExE) Functional Description (Release 5)*, Version 5.0.0, March.

3GPP (2002b), *Security — Security Architecture, (Release 5)*, TS33.102-500: 3G Version 5.0.0, June.

3GPP (2003a), *3G Security — Security Architecture*, 3GPP TS 33.102 v 6.0.0 (2003-09).

3GPP (2003b), *3G Security — Generic Authentication Architecture (GAA) System Description*, 3GPP TR 33.919 v1.0.0 (2003-12).

3GPP (2003c), *USIM Application Toolkit (Release 6)*, 3GPP TS 31.111 v6.0.0 (2003-12).

3GPP (2003d), *Security Mechanisms for the (U)SIM Application Toolkit, Stage1*, 3GPP TS 22.048 v5.0.0 (2003-06).

3GPP (2003e), *Security Mechanisms for the (U)SIM Application Toolkit, Stage2*, 3GPP TS 23.048 v5.8.0 (2003-12).

3GPP (2004), *3rd Generation Partnership Project: Vocabulary for 3GPP Specifications (Release 6)*, 3GPP TR 21.905 v6.5.0 (2004-01).

3GPP2 (1999), *OTASP and OTAPA*, 3GPP2 N.S0011, January.

3GPP2, (2002a), *Over-the-Air Service Provisioning of Mobile Stations in Spread Spectrum Standards*, 3GPP2 C.S0016-B v1.0, October.

3GPP2, (2002b), *Physical Layer Standard for cdma2000 Spread Spectrum Systems*, C.S0002-C, May.

Alvarez, M., Bender, P., and Conaty, G. (2003), Operator and Regulatory Requirements for Software-Defined Radio, SCOUT Program Workshop on Reconfigurable Terminals and Supporting Networks, 16 September.

Babb, D. Bishop, C. and Dodgson, T. (2002). Security Issues for Downloaded Code in Mobile Phones, *Elect. & Commun. Engineering J.*, Vol. 14, pp 219 - 227.

Cook, P. (2003). *A Structure for Software Defined Radio Security*, SDRF-03-I-0010-V0.0.

Dillinger, M., Madani, K. and Alonistioti, N., editors, (2003). *Software Defined Radio — Architectures, Systems and Functions*. John Wiley & Sons: West Sussex England.

Doan, T., Lam, C., Sakaguchi, K., Takada, J., and Araki, K. (2002). Digital Pre-Distortion Linearizer for a Realization of Automatic Calibration Unit, *Proceedings of the SDR 2002 Technical Conference*, HW-3-02, November.

Falk, R., Faroughi-Esfahani, J., and Dillinger, M. (2002). *Reconfigurable Radio Terminals — Threats and Security Objectives*, SDR Forum Document SDRF-02-I-0056.

Faroughi-Esfahani, J., Falk, R., Drew, N., and Bender, P., (2002). A Regulatory View on Security Requirements for Reconfigurable Radio," SDR Forum Technical Conference, San Diego, Paper no. SW3-03.

FCC (2001), *First Report and Order, Authorization and Use of Software Defined Radios*, ET Docket No. 00-47, September.

FCC (2003), *Notice of Proposed Rule Making and Order, Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies* (ET Docket No. 03-108); *Authorization and Use of Software Defined Radios* (ET Docket No. 00-47), December.

Fitton, J. (2002). Security Considerations for Software Defined Radio, SDR Forum Technical Conference, Paper no. SW3-04, November.

Fung, C., Doan, T., Sakaguchi, K., Takada, J. and Araki, K. (2003). Novel Security Architecture that Enables Global Roaming of SDR Terminal, Inst. of Elect. and Commun. Engineers Symposium on Download Security and Regulatory Issues (Keio University), April 2003.

Gallery, E. (2003). A Policy-Based Framework for the Authorisation of Software Downloads in a Mobile Environment. 2003 Software Defined Radio Technical Conference, Session SY-2.

Harada, H., (2003), *Research and Development on Regulatory Issue of SDR*, Yokosuka Radio Communications Research Center, Communications Research Laboratory (CRL), Independent Administrative Institute, Japan, September 17 presentation to SDR Forum.

Harada, H., Kuroda, M., Morikawa, H., Wakana, H., and Adachi, F., (2003). The Overview of the New Generation Mobile Communication System and the Role of Software Defined Radio Technology, *IEICE Trans. Commun.*, Vol. E86-B, No. 12, December, pp. 3374 - 3384.

Hoffmeyer, J., Park, I., Majmundar, M., and Blust, S (2004). Radio Software Download for Commercial Wireless Devices, *IEEE Comm. Mag*., Vol. 42, No. 3, pp S26-S32) March.

IETF (1997), Key Words for Use in RFCs to Indicate Requirement Levels, March; available at http:www.ietf.org/rfc/rfc2119.txt.

ISO (1999), The Common Criteria for IT Security Evaluations (CC), ISO standard 15408; available at: http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=27632&ICS1=35&ICS2=40&ICS3=.

IST (1999), IST-1999-12070 TRUST, Deliverable D4.3, Report on Assessments of Novel Solutions on System Aspects of Reconfigurable Terminals and Recommendation for Standardisation, WP4, 2001.

IST (2002), IST-24091, SCOUT Deliverable D4.1.1 Requirements on Network and Security Architecture and Traffic Management Schemes for Download Traffic based on IP Principles in Cellular and Ad Hoc Networks, Oct. 2002.

ITU (a). Security Principles for International Mobile Telecommunications-2000 (IMT-2000), ITU-R Recommendation M.1078; available for purchase through the ITU at: http://www.itu.int/publications/index.html.

ITU (b). Evaluation of Security Mechanisms for IMT-2000", ITU-R Recommendation M.1223; available for purchase through the ITU at: http://www.itu.int/publications/index.html.

ITU (c). Technology Trends, Final version has been submitted for publication. Will be available for purchase through the ITU at: http://www.itu.int/publications/index.html.

ITU-T (2003), Compendium of Approved ITU-T Security Definitions (and Addendum); available through ITU Electronic Bookstore at: http://ecs.itu.ch/cgi-bin/ebookshop/

Køien, G. (2004), An Introduction to Access Security in UMTS, *IEEE Wireless Communications*, Vol. 11, No. 1, pp8-18, February.

Krall, E. (2004), *Common Criteria, General Dynamics*; SDR Forum Document SDRF-04-I-0019.

Lam, C., Doan, T., Sakaguchi, K, Takada, J., and Araki, K (2003), Novel Security Architecture that Enables Global Roaming of SDR Terminal, *Proceedings of the 2003 IEICE General Conference*, SB-10, March.

Marshall, P. (2003), Beyond the Outer Limits: XG — Next Generation Communications, Wireless World Research Forum, NYC, 27-28 October 2003, available at http://www.wireless-world-research.org/meeting/2003/WWRF10/WWRF10-Oct03.asp.

Michael, L. Mihaljevic, M., Haruyama, S. and Kohno, R. (2002). A Framework for Secure Download for Software-Defined Radio, *IEEE Comm. Mag*., v. 40, no. 7, pp 88-96.

Mitchell, C. (editor) (2004), *Security for Mobility*, IEEE Press, London.

Mitola III, J. (2002), *Software Radio Architecture: Object Oriented Approaches to Wireless Systems Engineering*, Wiley, New York.

Moessner, K. (2003), SDR Technology — Managing Soft Terminals; Regulatory Round Table on Software Defined Radio; Mobile Virtual Center of Excellence; University of Surrey Centre for Communication Systems Research, UK; September.

Moessner, K., Gultchev, S., and Tafazolli, R. (2001), Software Defined Radio Reconfiguration Management, IEEE Personal Indoor and Mobile Radio Conference (PIMRC).

NIST (1995, October). *An Introduction to Computer Security: The NIST Handbook*, NIST Special Publication 800-12.

NIST (1997). NIST ITL Bulletin, Public Key Infrastructure Technology, July.

NIST (1999, November). *Guidelines for Implementing Cryptography in the Federal Government*, NIST Special Publication 800-21.

NIST (2001), *Security Requirements for Cryptographic Modes*, FIPS Pub. 140-2.

Okuike, K., Uchikawa, H. Ikemoto, K. Umebayashi, K., and Kohno, R. (2003). A Security Framework Using ACS (Automatic Certification System) for Software Defined Radio. Inst. of Elect. And Commun. Engineers Symposium on Download Security and Regulatory Issues (Keio University), April 2003.

OMA (2002). Download Architecture, Open Mobile Alliance OMA-Download-ARCH-v1_0-2002-0610, June; publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html.

OMA (2003a). *Device Management Requirements, Version 1.0*, July 24 2003; OMA-REQ-DevMngmt-V1_0-20030724-C.

OMA (2003b).. *OMA Device Management Version 1.1.2*. December; publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html.

OMA (2003c). *SyncML Device Management Security, Version 1.1.2*, Open Mobile Alliance OMA-SyncML-DMSecurity-V1_1_2-20031209-A, December; publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html.

OMA (2003d). *Generic Content Download Over The Air Specification, Version 1.0*, Open Mobile Alliance OMA-Download-OTA-v1_0-20030221-c, February; publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html.

OMA (2003e). *WAP Push Security Requirements*, Open Mobile Alliance OMA-RD_PushSecurity-V1_0-20030811-D, August.
OMA (2003f). *SyncML Device Management Protocol, Version 1.1.2*, Open Mobile Alliance OMA SyncML-DMProtocol-V1_1_2-20031203-A.
OMA (2003g). *Signed Content Version 1.0*, Open Mobile Alliance Approved Specification, OMA-Security-SignedContent-v1_0-20030110-d, January.
OMA (2003h). *Certificate and CRL Profiles v1.1*, Open Mobile Alliance Approved Specification, OMA-Security-CertProf-v1_1-20030116-d, January.
OMA (2004a), *Firmware Update Management Object*, Candidate Version 1.0, 27 April.
OMA (2004b). *OMA DRM Specification v2.0*, Open Mobile Alliance OMA DRM-V2_0-20040108-D, January; publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html.
OMA (2004c). *WKPI Draft Version 1.0*, Open Mobile Alliance OMA-WAP-WPKI-V1_0-20040126-D, publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html.
Pereira, J. (2000). Redefining software (Defined) Radio: Reconfigurable Radio Systems and Networks. *IEICE Trans. on Commun*., V. E83-B, No. 6.1174-1182, June.
Reuters (2004). World's First Mobile Phone Virus Created, Reuters, 16 June.
Rose, G., and Køien, G. (2004). Access Security in CDMA2000, Including a Comparison with UMTS Access Security, *IEEE Wireless Communications*, Vol. 11, No. 1, pp19-36, February.
SCA (2004a), Software Communications Architecture Specification, Modular Software-Programmable Radio Consortium under Contract No. DAAB-15-00-3-0001, available for download at: http://www.jtrs.saalt.army.mil/SCA/SCA.html.
SCA (2004b). SCA Reference Implementation, Communication Research Centre, Canada; available for download at: http://www.crc.ca/en/html/scari/home/home.
SDR Forum (2002). *SDR System Security*. SDR Forum Document SDRF-02-A-0006.
SDR Forum (2002a). *Overview and Definition of Software Download for RF Reconfiguration*. SDR Forum Document SDRF-02-A-0002, August 2002.
SDR Forum (2002 b). *Requirements for Radio Software Download for RF Reconfiguration*, SDR Forum Document SDRF-02-A-0007, November 2002.
SDR Forum (2002c). *Report to FCC on Issues and Activities in the Area of Security in SDR*. SDR Forum Document SDRF-02-A-0003.
SDR Forum (2003). *Secure Global Roaming Architecture for Software Defined Radio*. SDR Forum Document SDRF-03-I-0052-V0.00, C. F. Lam, H. J. Wang, K. Sakaguchi, J. Takada, and K. Araki, Tokyo Institute of Technology, November.
Sun Microsystems (2000). *Mobile Information Device Profile*, Sun Microsystems, JSR-37, Java2 Platform, Micro Edition, 1.0, September.
Sun Microsystems (2002). *Mobile Information Device Profile, v2.0*, Sun Microsystems, JSR-118, JCP Public Draft Specification, Java2 Platform, Micro Edition.
Suzuki, Y. (2002). Interoperability and Regulatory Issues around Software Defined Radio (SDR) Implementation, *IEICE Trans. Commun*., Vol. E85-B, No. 12, pp. 2564-2572, December.
Suzuki, Y., Oda, K., Hidaka, R., Harada, H., Hamai, T., and Yokoi, T. (2003a). Technical Regulation Conformity Evaluation System for Software Defined Radio, *IEICE Trans. Commun.*, Vol. E86-B, No. 12, December 2003, pp. 3392-3400.

Suzuki, Y., Harada, H., Uehara, K., Fujii, T., Yokoyama, Y., Oda, K., and Hidaka, R. (2003b). Adaptability Check during Software Installation in Software Defined Radio, *IEICE Trans. Commun.*, Vol. E86-B, No. 12, December 2003, pp. 3401-3407.

Suzuki, Y., Yokoi, T., Iki, Y., Kawaguchi, E., Nakajima, N., Oda, K., and Hidaka, R. (2003c). Development of Experimental Prototype System for SDR Certification Simulation, *IEICE Trans. Commun.*, Vol. E86-B, No. 12, December 2003, pp. 3408-3416.

Tuttlebee, W. (2002). *Software Defined Radio, Enabling Technologies*. West Sussex England: John Wiley & Sons.

Watanabe, F., Ohashi, M., Nakamura, H., and Iwai, H. (2003). Expectations on Software Defined Radio (SDR) in Standardization Fora on Future Mobile Communication Systems, *IEICE Trans. Commun.*, Vol. E86-B, No. 12, December 2003, pp. 3366-3373.

9 Other Sources of Information

The following articles, papers, and documents are additional sources of information on topics related to DSII security beyond those specifically referenced and listed in Section 8, References.

Common Criteria Protection Profiles (see Section 4.5 of SDR Forum Document DL-REQ, Requirements for Radio Software Download for RF Reconfiguration) and available at the following web sites:
Common Criteria home page: http://csrc.nist.gov/cc/
http://www.commoncriteria.org/protection_profiles/pp.html
Some Protection Profiles: http://www.iatf.net/protection_profiles/

Communications Research Centre. (2004). Software Communications Architecture Reference Implementation, available for free download at: http://www.crc.ca/en/html/rmsc/sdr/projects/scari

Cook, K., and Martinez, C. (2001), "Future Scenarios: Developing end user and operator requirements for software reconfigurable radio," IST Summit 2001, Barcelona 10-12 September.

Cromwell, B. (2003). Securing Unlicensed WLAN Data Communications, www.rfdesign.com February.

Ellison, C. and Schneier, B. (2000)., "Ten Risks of PI: What You're not Being Told about Public Key Infrastructure, Computer Security J., Vol. XVI

Java Community Process, JSR 124 Client Provisioning, www.jcp.org/en/jsr/detail?id=124

JTRS. (2004). Software Communications Architecture, available at: http://jtrs.army.mil/sections/technicalinformation/fest_technical_sca.html

Karygiannis, T. and Owens, L. (2002). Wireless Network Security: 802-11, Bluetooth and Handheld Devices, NIST Special Publication 800-48.

Kiran, S., Lareau, P., and Lloyd, S (2002). PKI Basics — A Technical Perspective, PKI Forum, November

Lee, A. (1999). Guideline for Implementing Cryptography in the Federal Government, NIST Special Publication 800-21.

Longo, E., Stapleton, J. (2002). PKI Note: Smart Cards, PKI Forum, April

Modular Software Programmable Radio Consortium, *Software Communications Architecture Specification*, http://www.jtrs.saalt.army.mil/SCA//SCA.html

Nash, H., Housley, R., Linn, J., Nystrom, M., Mullenger, H., and Stapleton, J. (2002). Understanding Certification Path Construction, PKI Forum, September

NIST Security Page: http://csrc.nist.gov/

NIST (2002, November). Wireless Network Security, NIST Special Publication 800-48.

Palicot, J. and Lester, C. (2003). A New Concept for Wireless Reconfigurable Receivers, *IEEE Comm. Mag*. v. 41, n. 7, 124 —132.

Polson, J., Christensen, E., Tarver, B, and Gifford, S., (2003). Common Software Download Requirements for Software Defined Radios," SDR Forum Technical Conference, San Diego, Paper no. SW3-01.

Polydoros, A, Rautio, J., Razzano, G., Bogucka, H. Ragazzi, D., Dallas, P., Mammela, A., Bendix, M., Lobeira, M. and Agarossi, L. (2003). WIND-FLEX: Developing a Novel

Testbed for Exploring Flexible Radio Concepts in an Indoor Environment, IEEE Comm. Mag. v. 41, n. 7, 116-122

Rajagopalan, T. (2003). Over-the-Air Firmware Updates of Mobiles. Wireless Security Perspectives, June.

SDR Forum (1999). Architecture and Elements of Software Defined Radio Systems as Related to Standards.” SDR Forum Technical Report 2.1.

SDR Forum (2002). SDR System Security. SDR Forum Document SDRF-02-A-0006.

SDR Forum (2003). Terminal Classification Guide. SDR Forum Document SDRF-03-W-0004-V1.00.

Shiba, H., Uehara, K., and Araki, K. (2003). A Study on Security Architecture for Software Defined Radio, Inst. of Elect. And Commun. Engineers Symposium on Download Security and Regulatory Issues (Keio University), April.

Srikanteswara, S., Palat, R., Reed, J. and Athanas, P. (2003). An Overview of Configurable Computing Machines for Software Radio Handsets. *IEEE Comm. Mag.* v. 41, no. 7, 134-141.

Sun Microsystems (2000). Mobile Information Device Profile - JSR-237, Java2 Platform, Micro Edition 1.0, September.

Sun Microsystems (2002). Mobile Information Device Profile - JSR-118, Java2 Platform, Micro Edition 1.0, September.

Tsunoda, K. (2003). Wireless LAN Security Tutorial, Inst. of Elect. and Commun. Engineers Symposium on Download Security and Regulatory Issues (Keio University), April.

Appendix A: Security Structure and High-Level Security Functional Requirements

This appendix provides a summary of the high-level security requirements found in the SDR Forum Document, Requirements for Radio Software Download for RF Reconfiguration, DL-REQ, [SDR Forum 2002b]. Requirements are provided in the following table for each of the elements of the security structure that the SDR Forum has developed. The security structure is based on the Software Communications Architecture (SCA) developed for military applications of software defined radio. The security structure may be found in Cook [2003], which is based on Fitton [2002]. More information on the SCA may be found in Software Communications Architecture Specification [SCA, 2004a] and SCA Reference Implementation [SCA, 2004b].

SDR Forum Document SDRF-03-I-0010, Structure for SDR Security [see Fitton, 2002; Cook, 2003]			**SDR Forum Document DL-REQ, Requirements for Radio Software Download for RF Reconfiguration [SDR Forum, 2002b]**
Security Measure	*H/W*	*S/W*	*High level functional requirement in SDR Forum Document DL-REQ*
1. Security policy enforcement and management	X	X	Section 4.4: “Because of differences in regulatory policies around the globe, a security policy mechanism needs to be downloadable.”
2. Information integrity	X	X	Several sections of the document refer to data integrity, including Section 4.1.9. After the download is complete, there shall be a final integrity test performed on the downloaded software. For example, cryptographic encapsulation or a cyclic redundancy test may be performed to check the integrity of the software. In case of an integrity test failure, the SDR device may request the download server to retransmit the software partially or fully.
3. Authentication and non-repudiation		X	Section 4.1.4 Authentication; Also see Section 4.4 Security Considerations
4, Access control		X	Not specifically treated in DL-REQ; however access control is implied by authentication and authorization.
5. Encryption and decryption	X	X	Section 4.1.8 Protection; See also Section 4.4 Security Considerations
6. Key and certificate management	X	X	Section 4.4 Security Considerations including Trusted System Operation, Authentication, Authorization, Integrity, Privacy, Non-repudiation, and Auditing. PKI is discussed in Section 4.1.9 and key management requirements are discussed briefly in Section 4.1.10: Requirement: The request of an installation key from the download server to grant permission to install the download radio software on the SDR device.
7. Standardized installation mechanisms	X	X	Section 4.1.10 Installation

SDR Forum Document SDRF-03-I-0010, Structure for SDR Security [see Fitton, 2002; Cook, 2003]			**SDR Forum Document DL-REQ, Requirements for Radio Software Download for RF Reconfiguration [SDR Forum, 2002b]**
Security Measure	*H/W*	*S/W*	*High level functional requirement in SDR Forum Document DL-REQ*
8. Auditing and alarms	X	X	Alarms are not specifically treated in DL-REQ. Auditing is treated as part of Section 4.3.4 Network Architecture Requirements: Requirement: The network architecture shall support the following reconfiguration management functionalities to control and coordinate radio software download and SDR device reconfiguration in the network: ♦ Maintaining a database of current configurations and capabilities of SDR devices in the network ♦ Scheduling radio software downloads to SDR devices ♦ Providing a network architecture that is able to support efficient downloads to large number of SDR devices ♦ Maintaining software repositories of trusted third-party vendor and original equipment manufacturer (OEM) software modules, and coordinating SDR device access to these repositories for efficient downloads ♦ Communicating with local RMs residing on each SDR device to co-ordinate download and reconfiguration processes ♦ Communicating with local RMs residing on each SDR device to co-ordinate and assist with mode identification, mode monitoring, mode negotiation, and mode switching ♦ Standardized auditing
9. Configuration management		X	Section 4.2.4 Reconfiguration Management — Requirement: The SDR device shall be equipped with a Reconfiguration Manager (RM) that oversees the processes of radio software download, installation, reconfiguration, testing, and recovery. This RM shall reside in a secure software area in the SDR device that is not subject to reconfiguration. The RM shall be responsible for: ♦ Enabling full or partial reconfiguration of all protocol stack layers of the SDR device ♦ Controlling and managing reconfiguration processes at the SDR device ♦ Ensuring that any anticipated configuration adheres to the given radio access system standards and thus does not affect neighboring channels or systems Communicating with the RM residing on the network side to coordinate radio software downloads and reconfiguration

SDR Forum Document SDRF-03-I-0010, Structure for SDR Security [see Fitton, 2002; Cook, 2003]			**SDR Forum Document DL-REQ, Requirements for Radio Software Download for RF Reconfiguration [SDR Forum, 2002b]**
Security Measure	*H/W*	*S/W*	*High level functional requirement in SDR F Doc DL-REQ*
10. Memory management	X		Section 4.2.1 Memory Management - Requirement: The SDR device shall be equipped with sufficient additional memory space beyond what is required for its normal mode of operation to support the functions such as mode monitoring, service discovery, mode negotiation, mode switching, radio software download, in-situ testing, installation, reconfiguration, reset and recovery, and reconfiguration management.
11. Emissions management	X	X	Spectrum requirements for download are treated briefly in DL-REQ, but spectrum management, per se, is not.

Appendix B: Survey of Security Activities in Various Standards Fora[*]

This appendix provides a brief summary of security specifications either already developed or being developed by a variety of fora external to the SDR Forum. The SDR Forum has existing formal relationships with some of these organizations such as the Open Mobile Alliance (OMA) and the International Telecommunication Union (ITU). The specifications/standards overviewed in this appendix are directly relevant to the requirements described in Section 4 of this document.

B.1 Third Generation Partnership Project (3GPP)

B.1.1 Universal Mobile Telecommunication System (UMTS)

Køien [2004] provides an introduction to access security in the Universal Mobile Telecommunication System (UMTS). The article includes an assessment of the confidentiality, integrity, and authorization components of wireless security. It does not deal with the ability to prevent fraud (accountability), which is a component of security (along with confidentiality, integrity, and authentication) in the 3GPP definition of security [3GPP, 2004]. The 3GPP security specifications cover the interconnections from the user device to the home subscription data base and authentication center; that is, the specifications provide for end-to-end security.

One problem with the UMTS security specifications identified by Køien [2004] is that the integrity provisions apply only to signaling and not to user data. This is a problem for some operational scenarios. It also is a problem when trying to extend the existing 3GPP security specifications to cover operational software download security.

The 3GPP UMTS security principles document [3GPP, 1999] provides the security principles for UMTS. This document provides a description of threats to UMTS and the requirements that have developed to counter the specific threats that are described. The threat analysis includes threats against:

- The radio interface
- The system infrastructure
- Applications
- Terminal equipment

The threats against these elements of the network include loss of confidentiality, loss of integrity, and denial of service. The 3GPP guide to 3G security [3GPP, 2000] and the 3GPP security threats and requirements document [3GPP, 2001c] also provide specific threat scenarios and requirements. The requirements developed from the threats define the features that are to be supported by UMTS. Security mechanisms used to satisfy the requirements and features for UMTS are outlined in the security principles document [3GPP, 1999]. For the USIM and the mobile terminal, these requirements include protection against unauthorized reading or

[*] Current as of date of publication.

modification of data and executable code. This is essentially the compartmentalization requirement that was described as being a requirement for operational software security (particularly for radio software security).

The security principles document [3GPP, 1999] states that it may be necessary to establish trusted third parties for providing certain types of services such as directories, trustworthy time stamps, and so forth. Trusted third parties may be hierarchically ordered (e.g., certification authorities). This UMTS principle may be important for establishing the future capability for the download of operational software from trusted third-party vendors.

The following references provide additional information on 3GPP security specifications:

- [3GPP, 2000] — Guide to 3G security
- [3GPP, 2001a] — Principles and objectives
- [3GPP, 2001b] — Confidentiality and integrity
- [3GPP, 2003a] — Security architecture
- [3GPP, 2003b] — Authentication

The USIM Application Toolkit, as specified in TS 31.111 [3GPP, 2003c], provides the capability for operators or third-party providers to create applications that are resident on the USIM. There exists a need to secure messages transferred over the network to applications on the USIM, with the level of security chosen by the network operator or the application provider. The requirements are identified in TS 22.048 [3GPP, 2003d]. The mechanisms to satisfy these requirements are specified in TS 23.048 [3GPP, 2003e].

Figure B-1 provides an end-to-end view of UMTS network elements that are covered by the 3GPP security specifications. It is beyond the scope of this brief overview to cite all of the relevant 3GPP technical specifications. However, the security architecture [3GPP, 2003a] defines five security groups, which cover the entire end-to-end UMTS network architecture. Each of these feature groups meets certain threats and accomplishes certain security objectives specified in the 3GPP threats and requirements document [3GPP, 2001c]. The five security feature groups are:

- **Network access security:** The set of security features that provide users with secure access to 3G services, and in particular protect against attacks on the (radio) access link.
- **Network domain security:** The set of security features that enable nodes in the provider domain to securely exchange signaling data, and protect against attacks on the wireline network.
- **User domain security:** The set of security features that secure access to mobile stations.
- **Application domain security:** The set of security features that enable applications in the user and in the provider domain to securely exchange messages.
- **Visibility and configurability of security:** The set of features that enable the user to determine whether a security feature is in operation and whether the use and provision of services should depend on the security feature.

The network domain security features provide for inter-network security. The user domain security features provide for security between the USIM and the mobile station (MS). This implies a compartmentalization capability within the wireless device. The application domain security provides a capability for third-party applications software download. This could be extended with proper security provisions to operational software download.

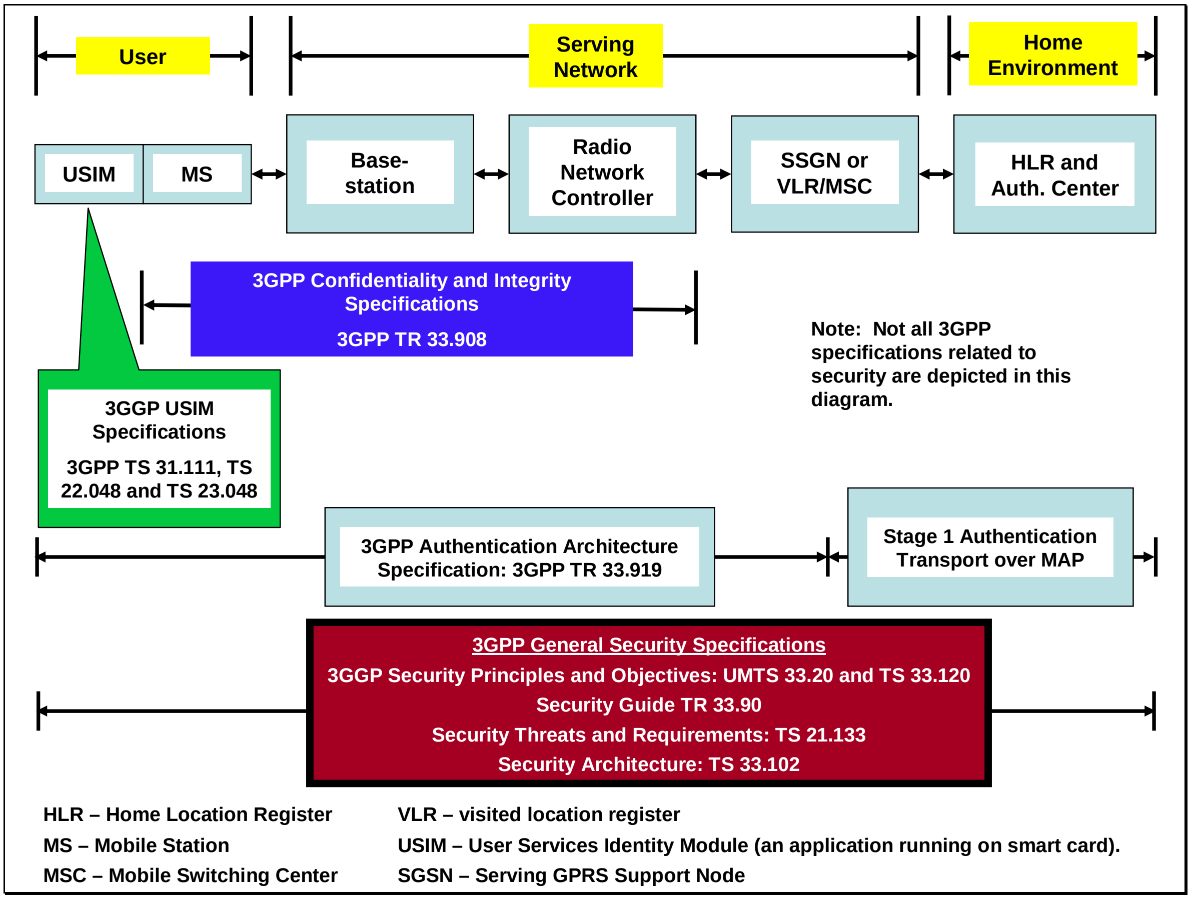

User
Serving Network
Home Environment
USIM
MS
Base-station
Radio Network Controller
SSGN or VLR/MSC
HLR and Auth. Center
3GPP Confidentiality and Integrity Specifications
3GPP TR 33.908
Note: Not all 3GPP specifications related to security are depicted in this diagram.
3GGP USIM Specifications
3GPP TS 31.111, TS 22.048 and TS 23.048
3GPP Authentication Architecture Specification: 3GPP TR 33.919
Stage 1 Authentication Transport over MAP
3GPP General Security Specifications
3GGP Security Principles and Objectives: UMTS 33.20 and TS 33.120
Security Guide TR 33.90
Security Threats and Requirements: TS 21.133
Security Architecture: TS 33.102
HLR – Home Location Register
MS – Mobile Station
MSC – Mobile Switching Center
VLR – visited location register
USIM – User Services Identity Module (an application running on smart card).
SGSN – Serving GPRS Support Node

Figure B-1. UMTS security architecture and key security specifications

Several issues are related to wireless security for UMTS networks:

- Confidentiality and Integrity
- Inter-Network Security
- Security Features

B.1.2 Mobile Execution Environment (MExE) Specifications

The SDR Forum has received an input contribution [SDR Forum, 2002d, Appendix C] from the 3GPP-T2 Working Group regarding the 3GPP Mobile Execution Environment specification, Mobile Execution Environment (MExE) Functional Description Stage 2 (Release 4) [for details, see 3GPP, 2002]. The 3GPP was formerly a sub-working group under Technical Specification Group (TSG) T-2.

Because security is linked to the success of applications, content, and commerce in the mobile environment, it has received attention within MExE. To prevent attack either from unfriendly sources or from transferred applications damaging the MExE device, a security system is required. Figure B-2 depicts the MExE network security architecture extended for radio software download.

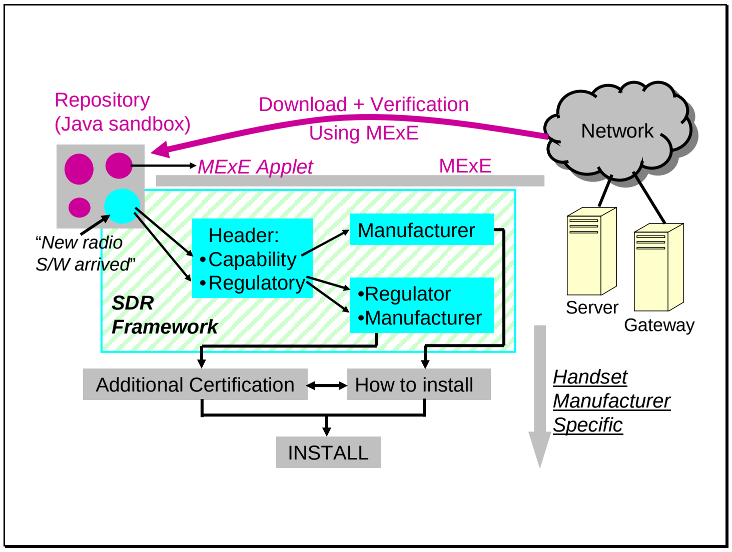


Figure B-2. MExE download architecture adapted for SDR

The fundamental elements that make up the basis of MExE security are:

- Application authentication
- Application authorization to a given domain, which is a set of permissions linked to authentication authority (root certificate)
- User permissions
- The management of the whole security system that MExE defines

The structure of this framework is a matrix of various logical areas or "domains," entities that have permission to control the download and execution of software in the domains, and a list of actions that are allowed to be performed by software executing in each of these domains.

The domains are currently defined as: MExE Security Operator Domain, MExE Security Manufacturer Domain, MExE Security Third Party Domain, and the MExE Untrusted Area.

The actions that have controlled access include:

- Device core function access (includes functions that are an essential part of the phone functionality)

- Support of core software download
- (U)SIM smart card low level access
- Network security, property, and services access
- User private data access
- MExE security functions access
- Application access
- Lifecycle management
- Terminal data access
- Peripheral access
- User interface input/output access

To enforce the MExE security framework, a MExE device is required to operate an authentication mechanism for verifying downloaded MExE executables. Successful authentication will result in the MExE executable being allowed to run in one of the trusted domains. Because the MExE device may want to authenticate content from many sources, a public key-based solution is mandatory. Before trusting an MExE executable, the MExE device will check that the MExE executable was signed with a private key for which the MExE device has the corresponding public key. The corresponding public key held in the MExE device must either be a root public key (securely installed in the MExE device, e.g., at the time of manufacture) or a signed public key provided in a certificate, which, in turn, must be authenticated by a certificate chain present on the device.

MExE also allows "core software download," which provides a means to update the core device software subsystems, including the software that runs the radio and communication functions. It is thought that a typical usage scenario would be for the user to download and run an installation application that would be responsible for maintaining the integrity of the device during the upgrade. Software such as this requires that the application performing the core update execute in the manufacturer domain.

The details of the MExE security framework are documented in the MExE functional description document [3GPP, 2002].

B.2 Third Generation Partnership Project 2 (3GPP2)

Rose and Køien [2004] summarize the security features of cdma2000 and compare those features to those of UMTS. Not surprisingly, many of the features are similar, and in fact, the two systems have a common basis for authentication and key distribution. The key parts of the cdma2000 security architecture are:

- The home network
- The serving network
- The mobile station

- The User Identity Module (UIM)

The physical layer security standard is provided in document C.S0002-C[3GGP2, 2002b). Thus, the cdma2002 architecture is very nearly the same as the UMTS security architecture given in Figure B-1. One difference is that the UIM may or may not be removable. If it is removable, it is referred to as the R-UIM.

The cdma2000 specifications include secure over-the-air service provisioning and over-the-air parameter administration [3GGP2, 1999, 2002a]. OTA service provisioning (OTASP) provides a secure mechanism by which new subscribers can activate new wireless services or current subscribers can request changes in their existing service without the intervention of a third party. One of the prime objectives of OTASP is to provide a secure authentication key to a mobile station to facilitate authentications. OTA parameter administration (OTAPA) provides a secure mechanism for OTA update of certain parameters of a mobile station. It is performed without the knowledge of the user and can be employed at any time that the terminal is powered up. It does not interfere with normal usage of the terminal; that is, phone calls can be made or received even when OTAPA is taking place. The security mechanism prevents unauthorized OTA programming of the mobile station parameters. Potentially, these capabilities could be extended to be useful for over-the-air operational software download.

The cdma2000 security specifications also have the same deficiency as the UMTS security specifications in regard to the user integrity protection, namely, that integrity protection applies only to system signaling information and not to user data. This could be a problem when trying to extend the existing 3GPP2 security specifications to cover operational software download scenarios. Rose and Køien [2004] note that in comparing cdma2000 with UMTS, even though the details differ, the security philosophy for the two technologies is similar. Therefore, it is not surprising that the issues listed in the preceding section for 3GPP UMTS security are the same as those for cdma2000 security.

B.3 Open Mobile Alliance (OMA)

The Open Mobile Alliance mission is to facilitate global user adoption of mobile data services by specifying market-driven mobile service enablers that ensure service interoperability across devices, geographies, service providers, operators, and networks. To ensure service interoperability, OMA is developing a wide range of specifications that are technology neutral, or independent of what technology is being used (GSM/UMTS technology, cdmaone/cdma2000 technology, or other wireless communications technologies). Much of the work is applications related. However, interoperable services require service enabler specifications ,some of which are applicable to operational software.

As a point of clarification, the term “non-applications software” [OMA, 2003a, Section 5.5] is used within OMA the same way as the term “operational software” is used in this, and other, SDR Forum documents.

Figure B-3 depicts the relationship among several key OMA specifications that specify download protocols and/or security protocols. Also included is the OMA device management requirements document that will drive future OMA device management download and security specifications. The documents identified in Figure B-3 are briefly described in the following subsections.

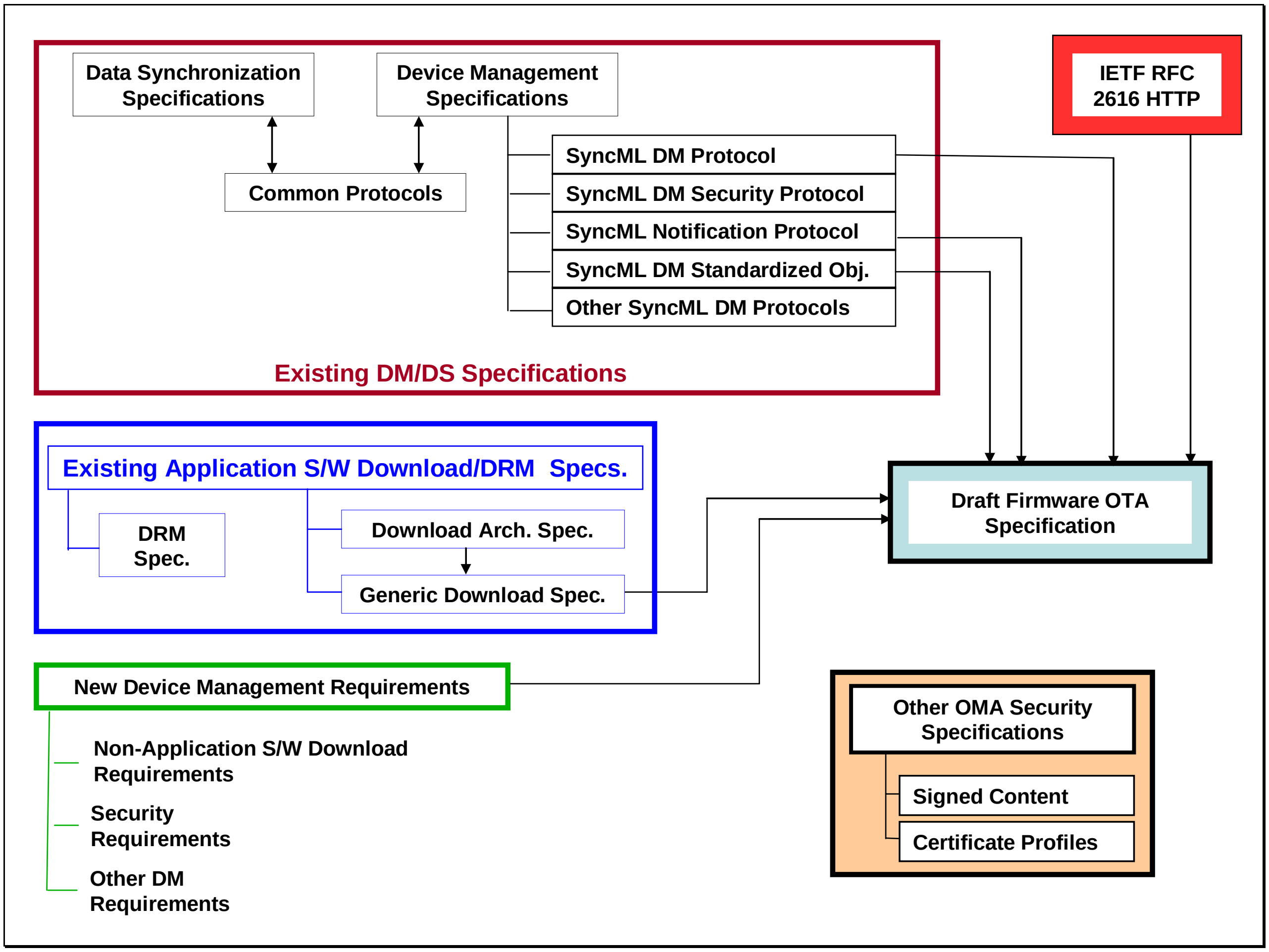

Data Synchronization Specifications
Device Management Specifications
Common Protocols
SyncML DM Protocol
SyncML DM Security Protocol
SyncML Notification Protocol
SyncML DM Standardized Obj.
Other SyncML DM Protocols
Existing DM/DS Specifications
IETF RFC 2616 HTTP
Existing Application S/W Download/DRM Specs.
DRM Spec.
Download Arch. Spec.
Generic Download Spec.
Draft Firmware OTA Specification
New Device Management Requirements
Non-Application S/W Download Requirements
Security Requirements
Other DM Requirements
Other OMA Security Specifications
Signed Content
Certificate Profiles

Figure B-3. Open Mobile Alliance specifications on software download and security

B.3.1 Existing OMA Specifications Related to Software Download and Security

The OMA has existing technical specifications applicable to meeting some of the security requirements for operational software download. The following subsections briefly summarize:

- OMA device management security
- OMA applications software download and digital rights management
- OMA device management requirements that extend device management protocol capabilities

B.3.1.1 OMA Device Management and Data Synchronization Specifications

The OMA has approved specifications for device management and data synchronization, which are publicly available at: http://www.openmobilealliance.org/tech/publicmaterial.html [OMA, 2003b]. The SyncML Protocol allows remote management of any device that supports this protocol. One of the data management specifications that is particularly important to software download security is SyncML Device Management Security [OMA, 2003c]. The document specifies the mutual authentication between the device and the device management server as well as the requirement and methodology for *confidentiality* and *integrity*, depending upon the type of information being exchanged between the device and server.

The SynclML-DM Security Protocol provides for encryption of managed objects and the encryption of information between device management servers but does *not* provide for confidentiality of data being transferred between the device and the device management server.

The Hashed Message Authentication Code-MD5 (HMAC) is used to ensure integrity of SyncML Device Management messages; the HMAC is used on every message transferred between the device and the device management server.

The credentials exchanged between the device and server include:

- Server ID
- A user name that identifies the device to the server
- A password
- A nonce, which prevents replay attacks where the hashing algorithms are used with static data

B.3.1.2 OMA Application Software Download and DRM

Two OMA applications specifications relevant to software download are the OMA download architecture specification and the content download OTA specification [OMA, 2002, 2003d]. The components of the architecture include the OTA download for media objects and digital rights management (DRM) of media objects (i.e., the management and control of the usage of the media objects on the device). *Digital rights management* allows the content owners to define and enforce restrictions on how the content is used.

The current applications software download OTA specification (referred to as OMA DLOTA) leverages the HTTP download mechanisms, but adds a number of features, including application-layer confirmation of installation [OMA, 2003d]. There is currently an approved DLOTA, v2.0 requirements document. Version 2 of the DLOTA specification will add functionality to converge the HTTP and MIDP OTA protocols. The key principles of OMA DLOTA include:

- Execution environment neutrality
- Content independence
- Generic download mechanism
- Extensibility to address unique requirements of content-specific environment
- Migration strategy from existing DLOTA mechanisms

Two security mechanisms considered by OMA for use in digital rights management were public key infrastructure (PKI) and broadcast encryption (BE). The former is a well-known technique. The latter is a key management technique that can guarantee that only compliant devices can decrypt the content, without requiring authentication of the device. It is claimed that this results in very simple, one-way protocols. OMA decided to use a trust model based on PKI in the DRM specification [OMA, 2004b].

In the OMA DRM PKI trust model, it is assumed that devices are provisioned either at the time of manufacture or later, with public and private keys and associated certificates signed by a certification authority (CA). A device manufacturer could be a certification authority.

B.3.1.3 OMA Device Management Requirements

The OMA has created a new device management requirements document [OMA, 2003a]. This requirements document specifies new device management requirements that are not met by the existing device management specifications [OMA, 2003b]. This requirements document includes a use case and associated high-level functional requirements for non-application software download [OMA, 2003a, Section 5.5]. Non-applications software is defined by OMA to include radio software, operating systems, drivers, and firmware. The requirements document includes the following security requirements:

- *Authentication:* Mutual authentication is required between the device management server and the device.
- *Authorization:* The device management server MUST be authorized to perform any device management functions.
- *Integrity protection:* All data communication between the device management server and device MUST be integrity protected.
- *Confidentiality protection:* All data communication between the device management server and a device that is personal to the user or confidential to the owner of the information MUST be confidentiality protected. The data link between the software originator and the device management server MAY maintain data confidentiality.
- *Smart card security:* Provisioning data on a smart card SHALL be protected against unauthorized modification.

The above is not a complete description of the OMA device management security requirements, but is representative of the type of DM security requirements specified by OMA in the Device Management Requirements document [OMA, 2003a]. As with all standards fora, it should be anticipated that the requirements documents of the Open Mobile Alliance will be updated from time to time.

B.3.2 OMA Firmware OTA Update

The Open Mobile Alliance has initiated work on a specification for firmware OTA update [OMA, 2004a]. The document specifies the download of update package(s), the subsequent installation of the update package(s) to update firmware, and a mechanism for reporting success or error status. The OTA firmware update protocol shall support the following process steps:

- Firmware update initiation
- Device information exchange
- Firmware download
- Firmware installation
- Notification of firmware update

The above steps are very similar to the functional requirements for radio software download specified by the SDR Forum [2002b], except that security aspects of download are not included. This is expected to be a focus of OMA Device Management work in the near future.

Two download mechanisms may be used:

- SyncML DM Protocol v1.1, which shall adhere to large object handling [OMA, 2003f].
- OMA Generic Content Over The Air Specification [OMA, 2003d].

Thus, the DLOTA specification, which was originally intended for applications, is being used for firmware download and update.

B.3.3 OMA Security Working Group Documents

The OMA Security Working Group has two approved documents:

- Signed Content, Version 1.0 [OMA, 2003g]
- Certificate and CRL Profiles [OMA, 2003h]

In addition, the Security Working Group has a draft specification on Wireless Application Protocol Private Key Infrastructure (WPKI) [OMA, 2004c].

B.4 Other Fora

B.4.1 International Telecommunication Union

The International Telecommunication Union (ITU) has security activities in both the Telecommunication Standardization Sector (ITU-T) and the Radiocommunication Sector (ITU-R). In ITU-T, the security standardization is focused in Study Group 17 (Data Networks and Telecommunication Software). Most of this work is focused on wireline data communications networks. In ITU-R, the security work is focused in Study Group 8 (Mobile, Radiodetermination, Amateur, and Related Satellite Services). Within ITU-R SG8, Working Party 8F (International Mobile Telecommunications-2000 and Systems Beyond IMT-2000) is responsible for ITU-R recommendations on mobile security, including:

- ITU-R Recommendation M.1078, Security Principles for International Mobile Telecommunications-2000 [ITU, a].
- ITU-R Recommendation M.1223, Evaluation of Security Mechanisms for IMT-2000 [ITU, b]

WP8F plans to update these security documents and possibly create new security recommendations. WP8F has also developed a report on technology trends that includes software defined radio [ITU, c]. It is expected that future recommendation(s) from WP8F will address global issues associated with software defined radio including circulation and security issues.

B.4.2 Trusted Computing Group

The Trusted Computing Group (TCG) [https://www.trustedcomputinggroup.org/home (retrieved 14 April 2004)] is an industry standards body comprising computer and device manufacturers, software vendors, and others with a stake in enhancing the security of the computing environment across multiple platforms and devices.

TCG develops and promotes open industry standard specifications for trusted computing hardware building blocks and software interfaces across multiple platforms, including PCs, servers, PDAs, and digital phones. This enables more secure data storage, online business practices, and online commerce transactions while protecting privacy and individual rights.

Appendix C: Reconfiguration Threats and Security Objectives*

Software Defined Radio Forum Contribution SDRF-02-I-0056

Committee: Technical

Title: Reconfigurable Radio Terminals – Threats and Security Objectives

Authors: Rainer Falk (Siemens AG)
Jafar Faroughi-Esfahani (Motorola UK)
Markus Dillinger (Siemens AG)

Source Markus Dillinger
Siemens AG
Otto.Hahn- Ring 6, D-81739 Munich, Germany
+49 89 636-44826
markus.dillinger@icn.siemens.de

Date: 4th November 2002

Distribution: Technical Committee

Document Summary:

This contribution concentrates on security requirements specific to the *reconfiguration* of communication equipment, where reconfiguration means that parameters or software in the device is changed. While some emphasis lies on the reconfiguration of the radio interface, reconfiguration can in general concern arbitrary parts of communication equipment as for example protocol stacks, plug-ins to support different types of content (as voice and video codecs), and applications. Main security issues are the control of the reconfiguration, that is who has the authority to reconfigure which parts of communication equipment, protection of the reconfiguration signaling, privacy of reconfiguration information as for example information on the current configuration of a user's equipment and of his preferences, the correctness and availability of information on which the reconfiguration is based, secure download of software required for reconfiguration, and issues concerning the radio emission and associated conformance requirements of radio equipment.

Notes of importance:

NOTICE

This document has been prepared by the European SCOUT project to assist the SDR Forum (or its successors or assigns). It is intended for discussion purposes only. It may be amended or withdrawn at a later time and it is not binding on any member of the SDR forum or any member of the SCOUT project.

* Appendix C is an input contribution to the SDR Forum as it was submitted in November 2002 [Falk et al. 2002].

C.1 Introduction

Re-configurable Radio systems is expected to play a critical role in the area of mobile/wireless communications by increasing flexibility; reducing deployment as well as operation and maintenance costs; creating new business opportunities and employment; facilitating enhancement and personalization [10]. Software defined radio (SDR) or re-configurable terminals will be the strongest candidate to give the answer of how to utilize the radio resources and meet the optimal user satisfaction.

Reconfiguration allows to upgrade and adapt equipment to user preferences and local conditions. Besides the installation of bug fixes, it will be possible to adapt and upgrade communication protocols, codecs, base-band processing algorithms or the complete air-interface (software defined radio). Main drivers for reconfigurable equipment are the desired support of several wireless standards to enable the use of the same equipment in different regions and for different communication systems as well as the fast introduction of new services into mobile networks without requiring the end users to buy first new mobile terminals before they can use the new services. But reconfigurable equipment is not only an issue for mobile terminals themselves, but requires system support in the form of new functions as reconfiguration managers that support and control the reconfiguration process and software download servers that provide required software.

Without protection mechanisms, the increased flexibility and openness of reconfigurable terminals could be misused in severe ways. Functionality that has by now been fixed during manufacture, can now be changed, extended and upgraded during the regular operation. It is essential to introduce suitable protection mechanisms that ensure a secure, safe, and reliable operation. The overall goal is to ensure that a terminal is configured only in “good”, intended ways. The precise security requirements depend on what functionality of mobile terminals actually will be made reconfigurable and to which extent, and to whom interfaces to control or influence reconfigurable parts will be opened. Further security requirements derive from additional functionality required in the network to support the reconfiguration.

This contribution concentrates on security requirements specific to the *reconfiguration* of communication equipment, where reconfiguration means that parameters or software in the device is changed. While some emphasis lies on the reconfiguration of the radio interface, reconfiguration can in general concern arbitrary parts of communication equipment as for example protocol stacks, plug-ins to support different types of content (as voice and video codecs), and applications. Main security issues are the control of the reconfiguration, that is who has the authority to reconfigure which parts of communication equipment, protection of the reconfiguration signaling, privacy of reconfiguration information as for example information on the current configuration of a user’s equipment and of his preferences, the correctness and availability of information on which the reconfiguration is based, secure download of software required for reconfiguration, and issues concerning the radio emission and associated conformance requirements of radio equipment.

Security is still required for aspects that are not specific to reconfiguration as for example protection of the air interface and controlled access to the network with authentication of the user and the network. More information on mobile systems security that is not specific to reconfiguration can be found for example in the relevant standards documents as 3GPP TS33.102 that describes the 3G security architecture [2].The IST SHAMAN project investigates important research issues for the security of future mobile systems. The IST PAMPAS project develops a research roadmap for privacy and security for beyond-3G systems and applications to prepare the ground for research initiatives in the upcoming 6th framework program. While areas requiring further research are identified, no actual research work is done on these topics.

The remainder of this contribution is structured as follows: Section C.2 describes security threats introduced by reconfiguration. Section C.3 outlines a generic reconfiguration system model that has been used to investigate and describe the reconfiguration security issues. The security objectives relevant to reconfiguration are contained in section C.4. The main issues are security of the security of the reconfiguration process and the secure download of radio and core software as well as the control of radio emissions. Furthermore, special situations as an emergency call could require that security issues are handled specifically. Section C.5 ends with a summary and an outlook.

C.2 Reconfiguration Threats

The possibility to reconfigure mobile equipment introduces also new threats as — without suitable protection mechanisms — the reconfigurable equipment could be reconfigured in undesirable ways. Therefore it has to be ensured that only desired reconfigurations can in fact take place, and — as the operation of a communication system relies on reconfiguration — that a desired reconfiguration in fact can take place.

Reconfiguration allows to change properties of communication equipment that have previously been fixed by their mere design. This improved flexibility poses the threat that changes are made to the configuration of communication equipment that contradict the interests and expectation of end users, network operators and service providers, equipment manufacturers and regulatory authorities. The overall objective is to provide a reliable service that fulfils the expectations of all involved stakeholders.

The following reconfiguration-specific security threats could occur by accident or by intention. They motivate the need to investigate and understand the security issues involved with reconfiguration and to derive the security objectives and select or develop suitable security features.

- *Download and Execution of Malicious Software*
  Software download is a key technology for reconfiguration. It poses the threat that malicious software is downloaded that causes harm by accident or by intention. The software could simply not work properly or not implement the expected functionality and thereby pose a threat to the reliability and availability, but it could as well intentionally implement malicious functionality as for example dialing premium rate numbers in the background, or any other of the threats described below.

- *Modification of Other Functionality*
  The purpose of a reconfiguration is to modify certain properties or functions of reconfigurable equipment. Other functionality not intended or authorized to be reconfigured could be affected by a reconfiguration.

- *Circumvention of Security Functions*
  Security functions, for example for secure network access to a cellular system or an Intranet or for m-commerce, have to be trustworthy themselves, but rely furthermore on secure storage of and protected access to cryptographic material and policy information. Unprotected reconfiguration could help to weaken or circumvent security functions not related to reconfiguration and thereby make them useless.

- *Easier Attacks*
  Reconfiguration could also make attacks against the wireless communication system easier and bring it in the range of a greater base of potential attackers. Attackers do not have to rely anymore on expensive equipment as signal generators or spectrum and protocol analyzers, or have to build own special equipment involving e.g. reverse engineering and modification of proprietary, highly integrated devices. Instead they get easy access to open interfaces and could simply reconfigure off-the-shelf equipment according to their intentions.

- *Invalidation of Conformance Requirements*
  Regulatory bodies pose requirements on radio equipment concerning user safety, electromagnetic compatibility (EMC immunity, EMC emission), and radio spectrum use (e.g. blocking, spurious emissions, transmitter requirements). Conformance with these requirements has — dependent on the regulatory procedures — either be tested by a regulatory body or an authorized testing house, or it has to be asserted by the manufacturer by stating conformance (self approval). Reconfiguration poses the threat that radio equipment is brought into market where conformance requirements are violated during the operation of the equipment.

- *User Safety*
  Reconfiguration of radio equipment could, when the hardware allows, even endanger the health and safety of the user, for example when radiated power is too high.

- *Disturbing Other Users or Other Radio Systems*
  Reconfiguration could lead to emissions that harm other users and radio systems. Besides emitting in wrong frequency bands, using too high power, or wrong modulation schemes, also access to the radio medium could be modified in ways that have a negative impact on other users. As a single user or a small set of users could have an advantage in using “improved” configurations that do implement unfair behavior, this threat shows that the user cannot given full control over his reconfigurable equipment. This threat is obviously related to conformance requirements, but its scope is broader as certain properties could be required by operators or non-regulatory standards for example to use the assigned spectrum efficiently and to provide good service to all customers.

- *Disregard of Preferences*
  Communication services could be used that do not match the preferences and expectations of the end user concerning available services, provided quality of service,

and the involved cost. Also the preferences of service providers and network operators could be disregarded. As the intentions and preferences of users, different network operators and service providers could contradict, this point is not easy to solve. An examples for possibly contradicting preferences is the selection of the radio access technology and network. While a user would probably prefer the cheapest technology that suits his service requirements, operators have obviously an interest in the usage of the most profitable service and network and especially that a service and network offered by themselves and not by a competitor is used.

- *Manipulated Reconfiguration*
The reconfiguration of terminal equipment will be supported by functions in the network, for example to assist or perform mode monitoring or the mode switching decision. The reconfiguration process will be distributed between several entities in the fixed part and the mobile part of the communication system. Information used or even required for the reconfiguration or any other information exchanged between the involved nodes can be manipulated and therefore the reconfiguration process could be influenced in illegitimate ways..

- *Unreliable Operation*
A configuration could be installed and activated that does not work at all or not properly. The consequence would be unsatisfied users, and high costs for customer care for the service provider. Also reconfiguration servers, software, and configuration information required to perform a reconfiguration could not be available or not function properly.

- *No or Insufficient Protection of Intellectual Property*
Both hardware and software manufacturers have an intention to protect their development effort and to receive a fair compensation. Reconfiguration could make reverse engineering easier, and software could be used or copied illegally. When the user or the service provider can freely add desired features, differentiation of products by supported features will not work in the same way as for current equipment.

- *Illegitimate Access to Private Information*
Sensitive information is required for the reconfiguration. Access to information about the end users' preferences, used services, or the current location and configuration has be controlled to protect the private sphere of a user. But also information related to a service provider or a network operator can be required to be kept confidential when the involved companies do not want to share data about their customers or network internals with competitors.

C.3 Reconfiguration System Model

Figure C-1 shows a generic system model of the entities relevant for the investigation of the reconfiguration security threats and objectives.

Reconfiguration support nodes as reconfiguration managers (RM) and download servers (DL) can be placed in the radio access network (RAN), in the core network, or in a public network connected by a gateway (GW). A reconfigurable terminal provides a reconfiguration interface for the communication between the local reconfiguration manager and the reconfiguration support nodes. A reconfigurable part is called “reconfiguration class”. A reconfiguration class can for example correspond to the radio interface, to voice or video codecs, to communication protocols, to user applications, or to ring tones. The reconfigurable terminal contains a local module store where software, parameters, and further configuration information is stored.

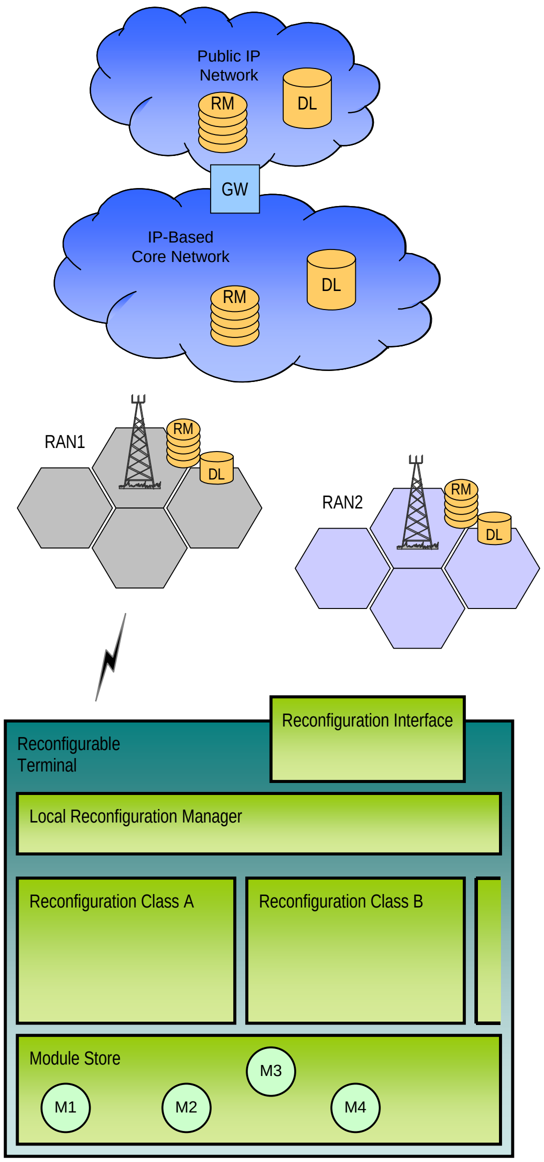
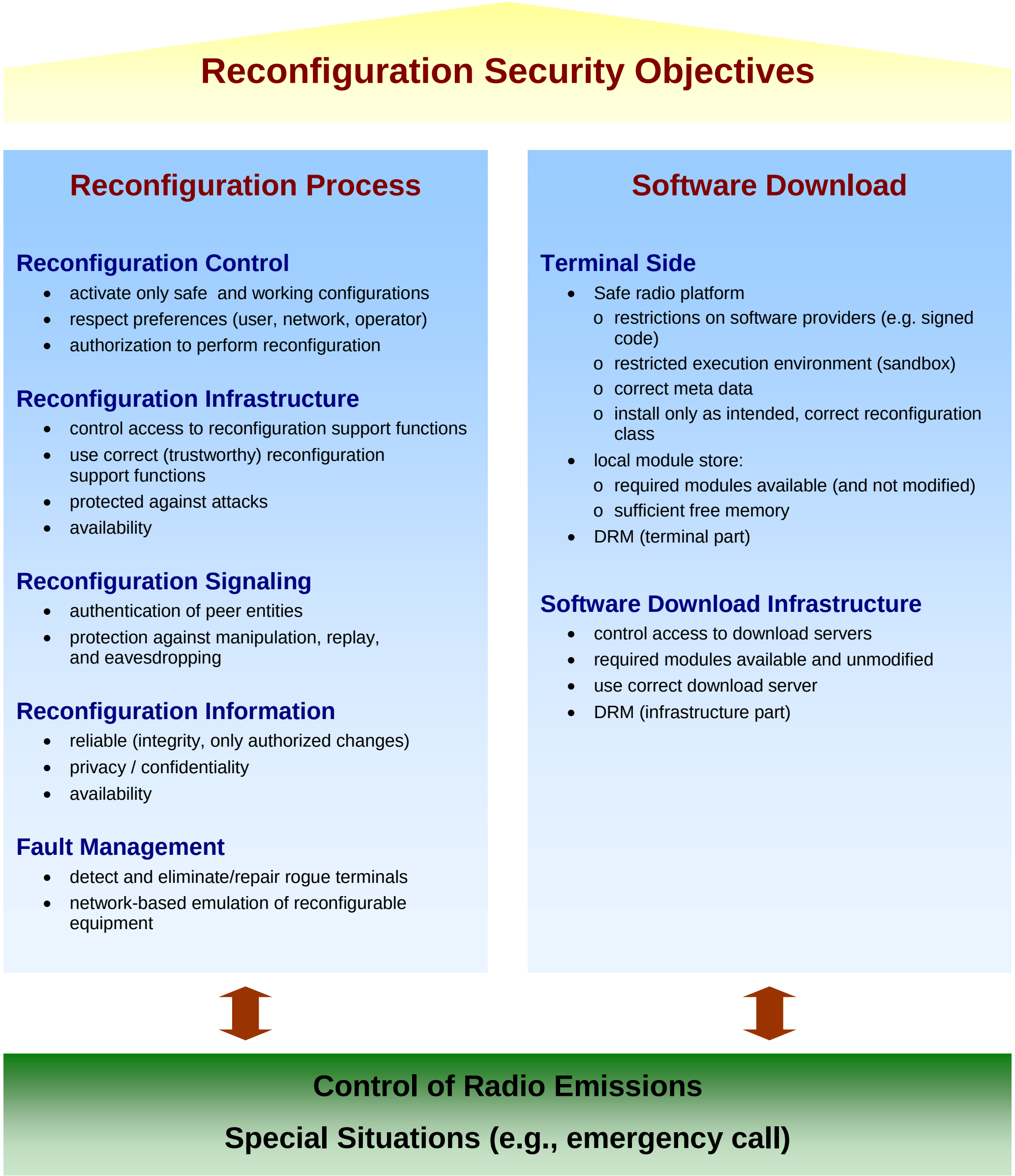


Figure C-1. Reconfiguration system model

C.4 Reconfiguration Security Objectives

Mobile communication systems using and supporting reconfigurable equipment require also security for aspects that are not specific to reconfiguration as for example protection of the air interface and controlled access to the network with mutual authentication of the user and the network, or protection of signaling traffic within and between operators. More information on security of mobile systems that is not specific to reconfiguration can be found for example in the description of the 3G security architecture [2].



Reconfiguration Security Objectives

Reconfiguration Process

Reconfiguration Control

- activate only safe and working configurations
- respect preferences (user, network, operator)
- authorization to perform reconfiguration

Reconfiguration Infrastructure

- control access to reconfiguration support functions
- use correct (trustworthy) reconfiguration support functions
- protected against attacks
- availability

Reconfiguration Signaling

- authentication of peer entities
- protection against manipulation, replay, and eavesdropping

Reconfiguration Information

- reliable (integrity, only authorized changes)
- privacy / confidentiality
- availability

Fault Management

- detect and eliminate/repair rogue terminals
- network-based emulation of reconfigurable equipment

Software Download

Terminal Side

- Safe radio platform
  - o restrictions on software providers (e.g. signed code)
  - o restricted execution environment (sandbox)
  - o correct meta data
  - o install only as intended, correct reconfiguration class
- local module store:
  - o required modules available (and not modified)
  - o sufficient free memory
- DRM (terminal part)

Software Download Infrastructure

- control access to download servers
- required modules available and unmodified
- use correct download server
- DRM (infrastructure part)

Control of Radio Emissions

Special Situations (e.g., emergency call)

Figure C-2. Reconfiguration security objectives

This section describes the reconfiguration security objectives that have to be fulfilled. Figure C-2 summarizes the reconfiguration security objectives. Two important parts are the security of the reconfiguration process and of the software download. Also radio emissions have to be controlled, and special situations as an emergency call have to be considered that could require specific handling of security issues.

C.4.1 Reconfiguration Process

The reconfiguration process is concerned with maintaining information about the current configuration and the environment, deciding whether and when to reconfigure what parts, performing the actual reconfiguration, and dealing with potential failure cases.

C.4.1.1 Reconfiguration Control

Restrictions on the reconfiguration have to be in place to ensure that only safe and working configurations are activated that are not only in-line with compliance and regulatory requirements, but that meet also end user and network preferences and expectations.

It has to be defined who is actually allowed to perform what types of reconfiguration. The manufacturer is expected to be responsible for the implementation of protection mechanisms that ensure compliance and that protect the terminal from malicious core software. But furthermore it has to be controlled which software is actually downloaded and used, when a reconfiguration takes place and to which mode. These decisions could be under control of the end user, the network operator, the communication service provider, or an independent service provider. For service providers and network operators it is essential to provide a reliable service that meets the expectations of the end users. The activation of a configuration that either does not work or that does not provide the services requested by end users should be prevented to ensure a high user satisfaction and to minimize the need for expensive customer care.

It has to be controlled who may influence which part of the reconfigurable functionality, that is who controls the reconfiguration. It has to be ensured that each party can reconfigure only those parts it is authorized to. Depending on the detailed system architecture, entities authorized to trigger a reconfiguration may have to be distinguished from those entities that are authorized to actually perform a reconfiguration.

It has to be ensured that the preferences of the user, service provider and the network operator are obeyed, i.e. that no reconfiguration can take place that is not in line. Only trusted nodes may be involved in the reconfiguration process that can be trusted to obey the preferences. However, the involved parties may have different interests: Most users will prefer the cheapest configuration that meets their requirements, while operators want to most efficiently utilize network resources and maximize revenue. Financial compensation between operators can be a motivation for one operator to impose the use of configurations that are more attractive for himself, but not for the service provider, other network operators, or the user. These diverse objectives require non-technical arrangements to define acceptable policies.

C.4.1.2 Reconfiguration Infrastructure

Additional functions will be added to the core and possibly also to the access network, a public network (Internet) or a closed network (Intranet, home network) to assist the reconfiguration (download server, download controllers, caches, reconfiguration manager). These reconfiguration support functions have to be protected from attacks themselves to ensure their secure and reliable operation. Attacks can originate from within the same administrative domain (e.g. an network operator's own network), but can originate especially from other administrative domains. When the reconfiguration process relies on supporting functions in the network, it has to be ensured that the required functions are available. Access to reconfiguration support functions has to be controlled to ensure that only authorized users entities can make use of provided services. Furthermore, it has to be ensured that the correct, trustworthy reconfiguration support functions are used. Otherwise, vicious reconfiguration support functions provided by an attacker could get access to private information and could manipulate the reconfiguration. When a user is billed for the usage of reconfiguration services, it has to be protected as well.

C.4.1.3 Reconfiguration Signaling

The reconfiguration process involves the exchange of signaling traffic between the reconfigured device and reconfiguration support nodes as well as between reconfiguration support nodes. To protect the reconfiguration process from tampering, the signaling traffic has to be protected. The communication peer entities have to be authenticated, whereby an authenticated entity can be the subscriber (user), an administrative domain or a single network element. Both the integrity and authenticity as well as the confidentiality may have to be ensured. This objective can be achieved using cryptographic means (e.g. secure communication using IPsec), or by using closed networks that cannot be accessed by unauthorized entities.

C.4.1.4 Reconfiguration Information

Different kinds of information is required to perform a reliable reconfiguration that respects the preferences and capabilities of the equipment, end user, network operator, and service provider. While it has not been decided yet in detail which information will be required, the following information is expected to be used in the reconfiguration process:

- User preferences / profile / status / context: The services and the associated policy the user is allowed to use, the user's preferences, and information on the current configuration of the user's device and his context.
- Device information: current configuration, capabilities (what parts can be reconfigured), current state as stand-by, in call, application in execution, or off, battery status, available memory, connected devices as for example headset, PDA, MP3 player, camera, inserted in a car kit with external power supply and antenna, lid open or closed in the case of a clam-shell device etc.
- Software version/meta information: On what types of devices can the software be used on, What software can be used for a specific device, which is the latest version, where can it be downloaded from. Information required for configuration management (compatibility with other software, other required software and their respective version information). What are the minimum hardware requirements to run a particular software? Which software is required to implement a certain radio interface / reconfiguration.
- Network information: The preferences of a network operator, information on available modes (for mode detection), current network status (utilization, used services, number of users/devices)

This information is required for a successful, correct reconfiguration. Therefore it has to be ensured that the information on which the reconfiguration is based is reliable (correct, unmodified), that it is available, that it cannot be changed illegitimately, and that private information is not made available to unauthorized parties. This has two implications: The information has to be protected when it is transmitted over insecure networks, and the access to and the modification of information has to be controlled.

To protect the user’s privacy, access to information that allows to track or profile the user has to be controlled. Privacy is an issue also for network operators who are reluctant to share information on their network's operational details with other network operators. Such critical information comprises for example the number, topology and configuration of nodes.

C.4.1.5 Fault Management

Although when security and configuration management mechanisms are in place that are intended to prevent the activation of a configuration that does not work properly, there should anyhow be made precautions to deal with such situations should they occur. The objective of fault management is to detect faults and to initiate or perform corrective measures.

Work done in the context of the IST TRUST project concentrated on the supervision of the radio parameters of reconfigurable terminals [4]. Radio parameters can be supervised to detect a rogue terminal that is not compliant concerning power emission or the used spectrum, or that does not obey power control commands correctly. The supervision can be performed on the terminal itself or by the network.

A configuration could be tested in the network before it is downloaded and activated on a terminal. This allows detection of reconfiguration attempts that would fail before the actual reconfiguration is attempted. Unnecessary resource consumption at the radio interface and power consumption at the terminal would be prevented, and unnecessary user interactions avoided.

C.4.2 Software Download

C.4.2.1 Terminal Side

Dynamic software download is a key technology for reconfiguration. Malicious software could invalidate properties required for type approval or assured in a statement of conformance, but it could also lead to other types of harm. For example, it could circumvent other security mechanisms required for secure network access to a cellular network or a company's Intranet, or it could send a user's private data to unauthorized parties or make the device simply unusable. The device could also manipulated to behave against the user's interest, for example by calling premium rate services in the background, or by implementing a surveillance function (bug).

To prevent harm from potentially malicious software, two basic approaches can be taken:

- *Sandbox Method*
  In this method, downloaded software runs in a restricted, controlled execution environment (sandbox). Software executing in the sandbox can access only functionality

that is considered to be safe; thus, a misbehaving program cannot cause harm. This approach is taken for example for Java MIDlets [8].

- *Trust-Based Method*
  In a trust-based approach, only software from trusted providers is accepted. A Common solutions is expected to be based on signed code (or signed content in general) where the software provider signs a software package using a digital signature (e.g. RSA/PKCS#1 or DSA). The digital signature allows the terminal to verify the identity of the software provider and the integrity of the received software package independently from the download server the package has been loaded from. So the software can be flexibly downloaded from caches and download servers not controlled by the software provider. Public-key certificates issued by a certification authority assert a binding between a subject and its public key (e.g. X.509/PKIX). Signed code allows the receiver to verify the identity of the provider and the integrity of the received software package independently from the download server the package has been loaded from. The 3GPP 23.057 MExE standard requires that core software may be installed only when it has been authorized, i.e. signed, by the manufacturer of the device [1].

These two approaches can be combined: Although the software is executed in a controlled execution environment, it is either accepted only when it originates from trusted sources/providers, or it is granted receives in this case increased permissions to access restricted functionality when it originates from a trusted provider. For example, MIDP 2.0 supports trusted applications and privileged domains so that only trusted applications can access sensitive APIs. Mechanisms are defined to sign and authenticate applications using a X.509 public-key infrastructure [9].

Signed content involves a trust relationship between the provider and the recipient. For a reconfiguration class, either only content from a trusted provider is accepted, or the content is associated with a different protection domain dependent on the trustworthiness of its provider. The trust relationship has to be reflected by data on the receiving client so that it can verify the certificate and the provider's signature and whether it is trusted for the respective content type. It has to be defined - depending on the reconfiguration class - whether the user, a service provider, or the hardware manufacturer can determine the trusted providers. This decision influences where the correspondent data can be stored and whether it can be modified and by whom. When only software provided by the hardware manufacturer or a provider authorized by the hardware manufacturer is trusted, then the cryptographic material and policy information has to be stored on the reconfigurable device by the hardware manufacturer, and it has to be ensured that it cannot be changed by the end user or a service provider.

From a security perspective, it would be sufficient when the terminal can verify a loaded software module. So when manufacturer-specific software is downloaded, proprietary security mechanisms could be used. This approach is not preferred however for the following reasons: Proprietary solutions could be suspected to be badly designed and implemented as they will probably not be made public and can therefore not been reviewed publicly. As standardized solutions are needed for the secure download of user applications or other generic content, the required functionality has to be implemented anyway. When it is furthermore required that a configuration and the involved software shall can be checked in the network, for example by a reconfiguration manager, before the actual reconfiguration is performed, it is mandatory that all security and configuration management operations can be performed or simulated also in the network as part of a virtual configuration procedure. In practice, this requires an open, standardized method as otherwise each manufacturer's and terminal type's proprietary mechanisms would have to be implemented in the network.

The local storage in the terminal for reconfiguration modules needs protection, too: The required modules must be available in the correct version, and sufficiently free memory must be available when the communication system depends on dynamic software download. Adding, removing, and updating of software modules has to be controlled. Also the available storage capacity for different kinds of content could have to be controlled to ensure that sufficient storage is available for dynamically downloaded reconfiguration modules. Otherwise, it could occur that other types of content (MP3 files, pictures, voice memos) occupy all the memory.

To limit illegitimate usage of software, digital rights management may be required. When software is not provided free of charge, it has to be ensured that software can be used only when it has been paid for, and that it cannot be copied or forwarded to other users illegitimately.

C.4.2.2 Software Download Infrastructure

The download process has to be protected to prevent illegitimate triggering of a software download, removal or modification of required software on the reconfigurable device or on the download server, and illegitimate access to download servers. These requirements can be met using common communication security mechanisms (authentication and access control of communication partners, authenticity, integrity, confidentiality of communication traffic).

It can be required that read access to a download server is restricted, for example depending on the identity of users, the service provider of a user, or the currently visited network. Whether access is controlled and who is authorized to access a download server depends on the business model and on who operates the download server and thereby where the download server is placed. Write access to a download server will in all cases have to be controlled to ensure that required software is in fact available and that it cannot be modified without permission.

Furthermore, it may be required — especially from the perspective of the service provider — to control from which download servers certain types of content can be loaded from. The download of software for very critical reconfiguration classes as for example the radio interface or security-relevant modules could be restricted to download servers controlled by the service provider, while software for other, less critical reconfiguration classes as MIDlets could be downloaded from arbitrary places.

Dependent on the business model, special billing for download as well as digital rights management will be required (copy protection, illegitimate use). However it is expected that infrastructure already available for generic content download will be reused. The network part of Digital Rights Management has to be protected as well as it has to issue licenses to use software and to interact with billing.

C.4.3 Control of Radio Emission

When radio parameters can be reconfigured, the radio emission has to be controlled to ensure that no other users within the same or at another radio communication system are disturbed and that the user's safety is not endangered. Also limitations from a compliance perspective have to be obeyed to ensure that a device emits only radio signals permitted by its statement of conformance or its type approval. It has to be clarified who takes the responsibility to ensure that no illegitimate radio emissions occur. Appropriate approaches depend on the reconfiguration scenario:

- When software that modifies the radio properties is provided or authorized only by the hardware manufacturer, the device can implement checks to ensure that only such radio software is installed and activated that has been authorized by the manufacturer. In this case, the hardware and software manufacturer is the same manufacturer, so he can control the radio emissions that can occur on his devices.
- The situation is different when radio software is provided by independent software manufacturers. This scenario is in particular important when an open, standardized radio platform is used. In the case considered here, the whole radio configuration originates from a single software provider. Radio hardware and radio software could be approved independently so that each authorized radio software could be used on each authorized radio hardware. But in this case, the responsibility for the case that a device is misbehaving is not clear. Another, less flexible approach would be that each combination of hardware and software has to be authorized. Also in this case, it is not clear whether the hardware manufacturer or the software manufacturer, both of them, or an independent "testing house" should be responsible.
- The situation is even more complicated when radio software modules are provided by several providers, and a single radio configuration uses radio software modules originating from several, different providers. It would be possible to define dynamically a single radio configuration involving software modules originating from several providers. In this case, possibly also the responsibility for the overall configuration and for a single radio software module could have to be distinguished. The entity that defines the overall radio configuration could be made responsible for the correctness of that radio configuration. But also here, the respective responsibilities of the hardware manufacturer, the entity defining the overall configuration, and the providers of software modules are not clear. An important aspect for a technical solution would be how dynamically configurations are defined. When statically, pre-defined and pre-verified configurations are not suitable, the verification of a candidate configuration would have to be done online.

When all radio software originates from a trusted source, control of radio emissions can be based on a trust-based radio software download where a reconfigurable radio terminal accepts only such radio software for which it can verify that it originates from a trusted provider and that it has not been manipulated. A possible approach for an open radio platform that executes radio software modules from several software providers could be a tightly controlled supervision function that analyses relevant properties of the radio emissions (as power, frequency, bandwidth, modulation) and compares them with reference data. If a discrepancy between actual and permitted radio emission is detected, the radio would be deactivated and corrective measures would be triggered and performed. The supervision function can be both terminal and network based. In particular, it is possible to capture relevant data at several places and to merge and analyze those together. When the supervision is done on the terminal, it might also be required that external parties as a network operator, service provider, or a regulatory body can verify that downloaded radio software and its execution environment are really controlled as expected.

The security checks whether radio software may be installed and activated have ultimately to be done on the reconfigurable device itself. But they can be based on offline information as for example a digital signature of a trusted provider, or on online information where a trusted server checks a configuration and asserts its validity before the terminal activates it. Moessner, Gultchev and Tafazolli describe a reconfiguration management architecture where an online service, which is called "reconfiguration control part", is responsible to evaluate and approve intended configurations using a virtual configuration process and to assure standards compliance [6].

C.4.4 Special Situations

Some specific situations could probably require a special handling of the security issues, and they should be kept in mind when developing a security architecture. When for example a generic radio boot protocol would be used or when an emergency call is initiated, the access to reconfiguration facilities as a reconfiguration manager or a download server could be required also when a user and the network cannot authenticate each other and protect the radio interface. Whether a specific handling of security is required for some situations will be investigated in the following project phases when the security of the SCOUT reconfiguration architecture is analyzed.

C.5 Standards Relevant for Reconfiguration Security

In the area of mobile communications, standards with relevance for reconfiguration already exist or are appearing. Here, the most relevant ones are listed:

- 3GPP 33.102 Security Architecture
- 3GPP User Equipment Management (UEM), see feasibility study 3GPP32.803
- SyncML Device Management
- OMA Download
- WAP ServiceLoad and ServiceIndication
- Java Mobile Information Device Profile MIDP, JSR-37 Version 1.0 and JSR-118 Version 2.0
- 3GPP 23.057 Mobile Execution Environment (MExE)

The security architecture of 3GPP mobile communication system is described in [2]. Inter alia, the protection of the access link as well as of signalling traffic within and between administrative domains are covered. User equipment management and SyncML device management could be used to query the current configuration of a mobile device, to change parameters, and to install or update software. OMA Download supports download of generic content, including Digital Rights Management. WAP ServiceLoad and ServiceIndication could be used to trigger a download from the network. Java MIDP is a Java variant for limited devices as mobile phones. It allows a user to download and execute Java applications to his mobile phone. The recommended practice for GSM/UMTS compliant devices of version 2.0 (JSR-118) supports also manufacturer- and operator-signed Java applications. The 3GPP MExE standard defines execution environments for mobile devices. Security domains for the manufacturer, the operator, and third party and the associated permissions are defined. Core software download is permitted only for the manufacturer domain.

C.6 Summary

This contribution summarizes reconfiguration threats and derived security objectives. They describe the issues that security has to deal with in the context of reconfiguration. Figure C-2 gives an overview on these security objectives. They will be mapped on the SCOUT reconfiguration architecture in the following phase of the SCOUT project to investigate the security issues specific to the SCOUT reconfiguration architecture and to identify required security features.

More elaborate description of reconfiguration security threats and objectives can be found in the SCOUT deliverable D4.1.1 [5]. It gives also an overview on information security in general and on important security technology relevant for reconfiguration.

Acknowledgement

This work has been performed in the framework of the IST project IST-2001-34091 SCOUT, which is partly funded by the European Union. The authors would like to acknowledge the contributions of their colleagues from Siemens AG, France Télécom — R&D, Centre Suisse d’Electronique et de Microtechnique S.A., King‘s College London, Motorola SA, Panasonic European Laboratories GmbH, Regulierungsbehörde für Telekommunikation und Post, Telefonica Investigacion Y Desarrollo S.A. Unipersonal, Toshiba Research Europe Ltd., TTI Norte S.L., University of Bristol, University of Southampton, University of Portsmouth, Siemens Mobile Communications S.p.A., 3G.com Technologies Ltd., Motorola Ltd., DoCoMo Communications Laboratories Europe GmbH.

C.7 References for Appendix C

[1] 3GPP TS23.057-500: Mobile Execution Environment (MExE) — Functional Description (Release 5), Version 5.0.0, March 2002

[2] 3GPP TS33.102-500: 3G Security — Security Architecture (Release 5), Version 5.0.0, June 2002.

[3] Kate Cook and Carlos Martinez, „Future Scenarios: Developing end user and operator requirements for software reconfigurable radio“, IST Summit 2001, Barcelona 10.09. -12.09.01.

[4] IST-1999-12070 TRUST, Deliverable D4.3 “Report on Assessments of Novel Solutions on System Aspects of Reconfigurable Terminals and Recommendation for standardisation ”, WP4, 2001.

[5] IST-2001-24091 SCOUT Deliverable D4.1.1 “Requirements on Network and Security Architecture and Traffic Management Schemes for Download Traffic based on IP Principles in Cellular and Ad Hoc Networks”, Oct. 2002.

[6] Mitola III, J., “Software Radio Architecture:Object Oriented Approaches to Wireless Systems Engineering”, Wiley, 2002.

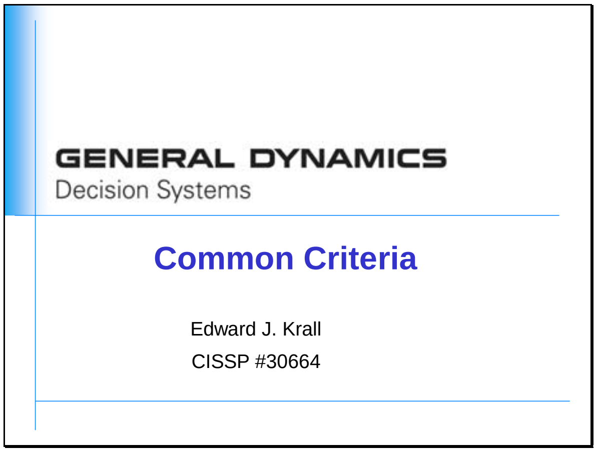
[7] K. Moessner, S. Gultchev, R. Tafazolli: Software Defined Radio Reconfiguration Management, IEEE Personal Indoor and Mobile Radio Conference (PIMRC), 2001.

[8] Sun Micros.: “Mobile Information Device Profile”, JSR-37, Java2 Platform, Micro Edition, 1.0, Sep. 2000.

[9] Sun Micros.: “Mobile Information Device Profile, v2.0”, JSR-118, JCP Public Draft Specification, Java2 Platform, Micro Edition, 2002.

[10] Walter Tuttlebee, “ Software Defined Radio: Origin, Drivers and international perspectives”, Wiley, 2002.

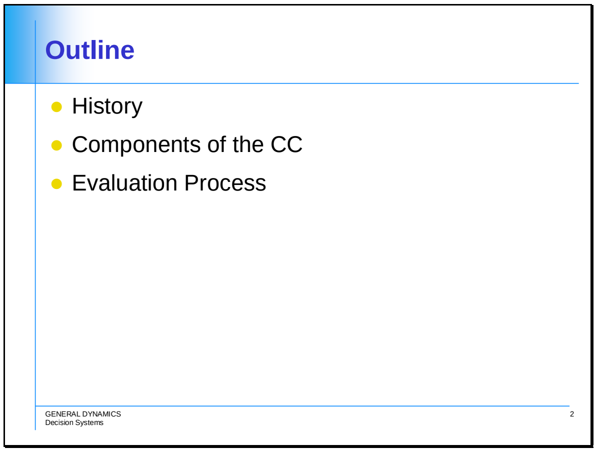
Appendix D: Overview of Common Criteria and Protection Profiles



GENERAL DYNAMICS
Decision Systems

Common Criteria

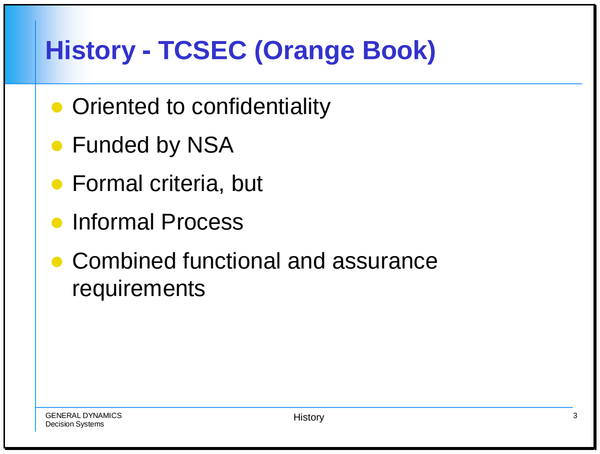
Edward J. Krall
CISSP #30664



Outline

- History
- Components of the CC
- Evaluation Process

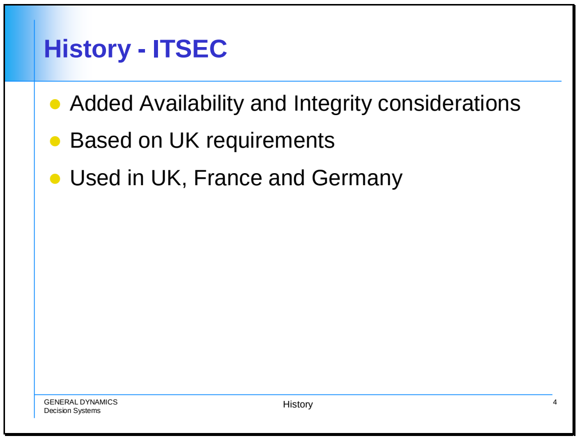
GENERAL DYNAMICS
Decision Systems 2



History - TCSEC (Orange Book)

- Oriented to confidentiality
- Funded by NSA
- Formal criteria, but
- Informal Process
- Combined functional and assurance requirements

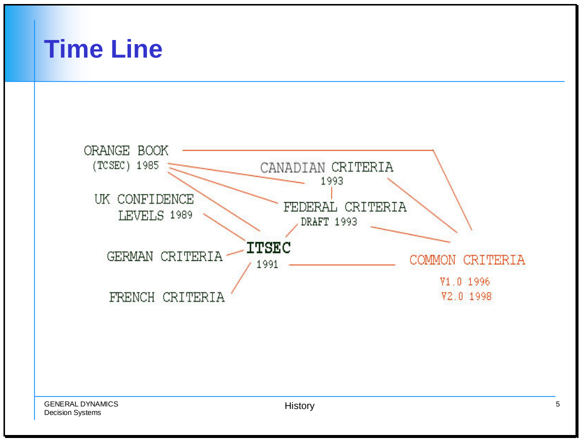
GENERAL DYNAMICS
Decision Systems History 3



History - ITSEC

- Added Availability and Integrity considerations
- Based on UK requirements
- Used in UK, France and Germany

GENERAL DYNAMICS
Decision Systems History 4



Time Line

ORANGE BOOK (TCSEC) 1985

CANADIAN CRITERIA 1993

UK CONFIDENCE LEVELS 1989

FEDERAL CRITERIA DRAFT 1993

GERMAN CRITERIA

ITSEC 1991

COMMON CRITERIA

V1.0 1996

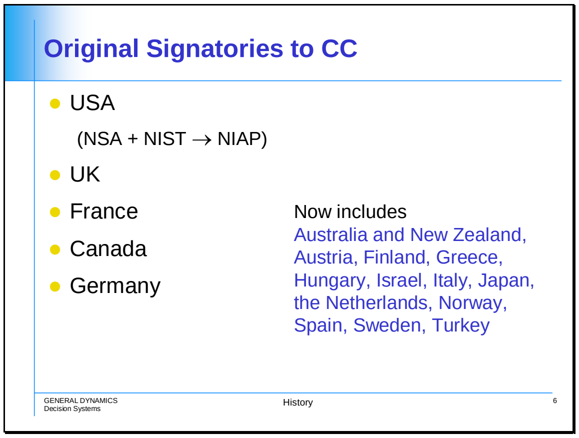
V2.0 1998

FRENCH CRITERIA

GENERAL DYNAMICS
Decision Systems

History

5



Original Signatories to CC

- USA

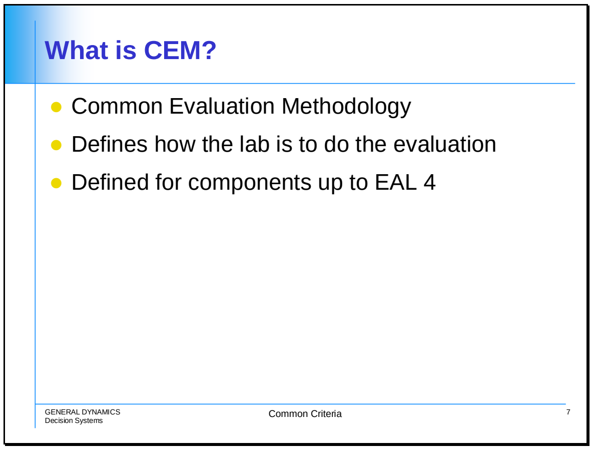
  (NSA + NIST → NIAP)
- UK
- France
- Canada
- Germany

Now includes
Australia and New Zealand, Austria, Finland, Greece, Hungary, Israel, Italy, Japan, the Netherlands, Norway, Spain, Sweden, Turkey

GENERAL DYNAMICS
Decision Systems

History

6



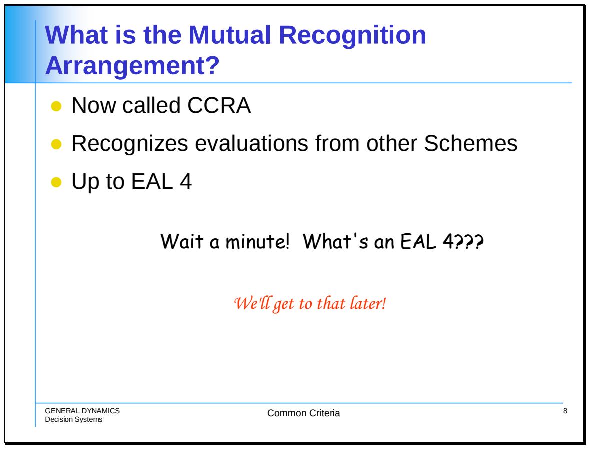
What is CEM?

- Common Evaluation Methodology
- Defines how the lab is to do the evaluation
- Defined for components up to EAL 4

GENERAL DYNAMICS
Decision Systems

Common Criteria

7



What is the Mutual Recognition Arrangement?

- Now called CCRA
- Recognizes evaluations from other Schemes
- Up to EAL 4

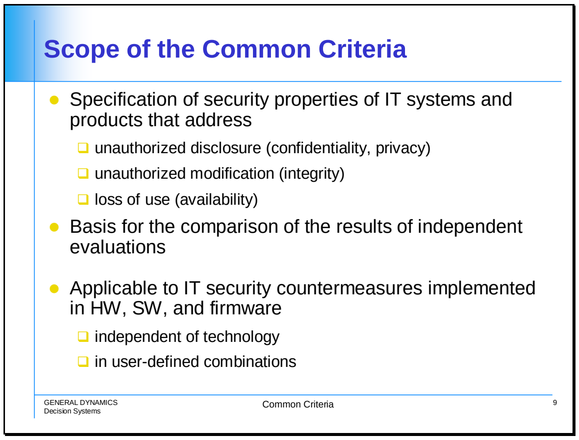
Wait a minute! What's an EAL 4???

We'll get to that later!

GENERAL DYNAMICS
Decision Systems

Common Criteria

8



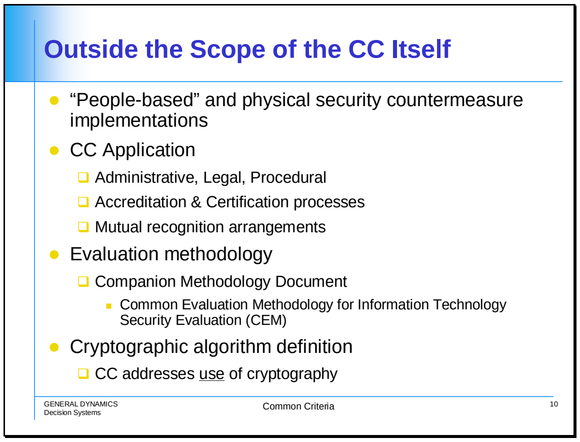
Scope of the Common Criteria

- Specification of security properties of IT systems and products that address
  - ❑ unauthorized disclosure (confidentiality, privacy)
  - ❑ unauthorized modification (integrity)
  - ❑ loss of use (availability)
- Basis for the comparison of the results of independent evaluations
- Applicable to IT security countermeasures implemented in HW, SW, and firmware
  - ❑ independent of technology
  - ❑ in user-defined combinations

GENERAL DYNAMICS
Decision Systems

Common Criteria

9



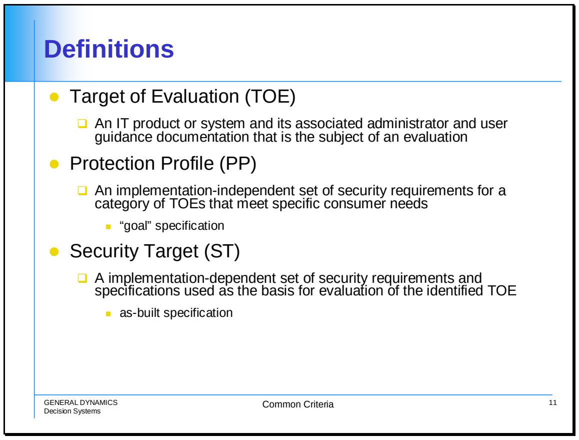
Outside the Scope of the CC Itself

- "People-based" and physical security countermeasure implementations
- CC Application
  - ❑ Administrative, Legal, Procedural
  - ❑ Accreditation & Certification processes
  - ❑ Mutual recognition arrangements
- Evaluation methodology
  - ❑ Companion Methodology Document
    - Common Evaluation Methodology for Information Technology Security Evaluation (CEM)
- Cryptographic algorithm definition
  - ❑ CC addresses <u>use</u> of cryptography

GENERAL DYNAMICS
Decision Systems

Common Criteria

10

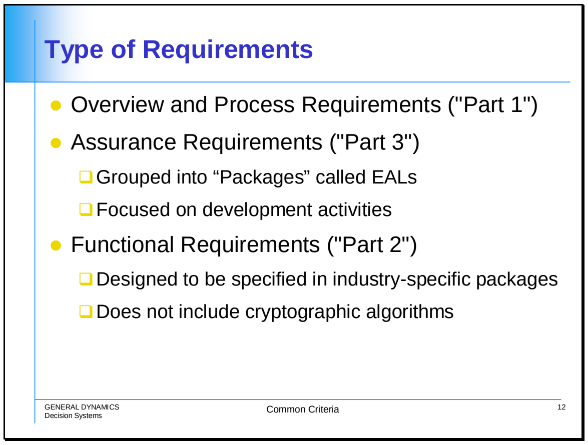


Definitions

- Target of Evaluation (TOE)
  - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation
- Protection Profile (PP)
  - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs
    - “goal” specification
- Security Target (ST)
  - A implementation-dependent set of security requirements and specifications used as the basis for evaluation of the identified TOE
    - as-built specification

GENERAL DYNAMICS
Decision Systems

Common Criteria 11

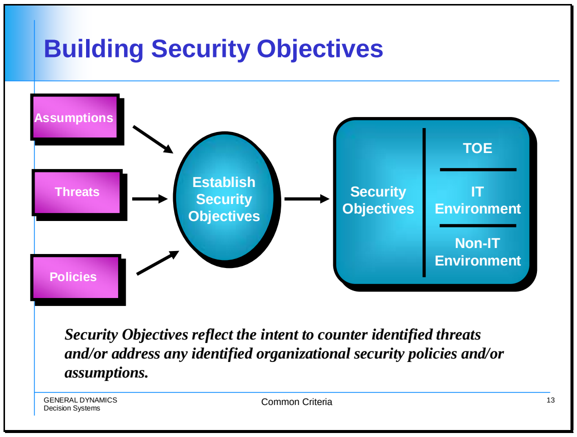


Type of Requirements

- Overview and Process Requirements ("Part 1")
- Assurance Requirements ("Part 3")
  - Grouped into “Packages” called EALs
  - Focused on development activities
- Functional Requirements ("Part 2")
  - Designed to be specified in industry-specific packages
  - Does not include cryptographic algorithms

GENERAL DYNAMICS
Decision Systems

Common Criteria 12

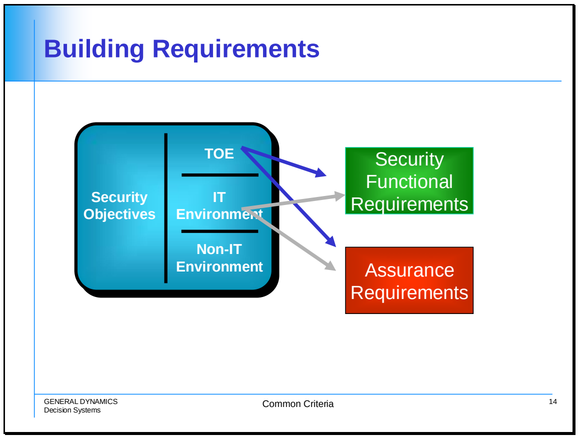


Building Security Objectives

Security Objectives reflect the intent to counter identified threats and/or address any identified organizational security policies and/or assumptions.

GENERAL DYNAMICS
Decision Systems

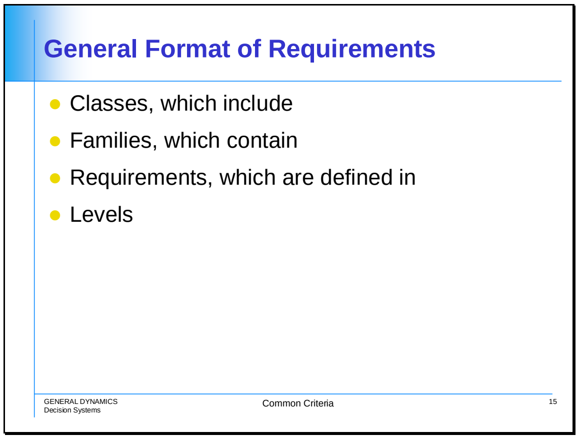
Common Criteria 13



Building Requirements

GENERAL DYNAMICS
Decision Systems

Common Criteria 14

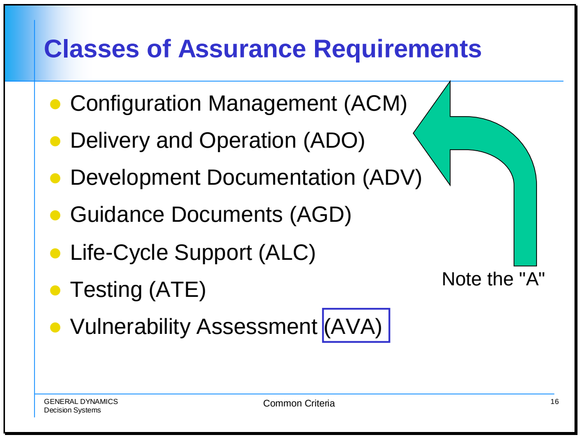


General Format of Requirements

- Classes, which include
- Families, which contain
- Requirements, which are defined in
- Levels

GENERAL DYNAMICS
Decision Systems

Common Criteria 15



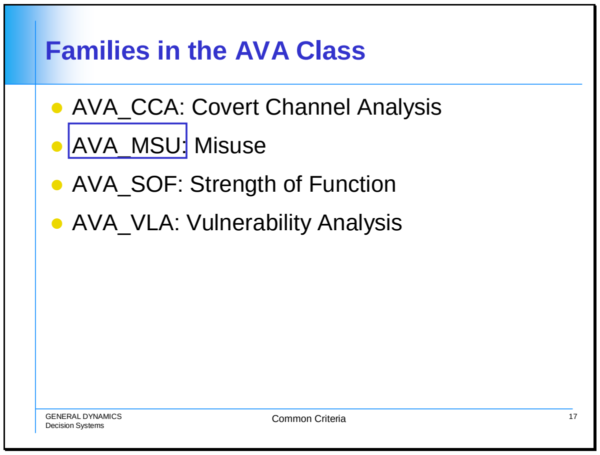
Classes of Assurance Requirements

- Configuration Management (ACM)
- Delivery and Operation (ADO)
- Development Documentation (ADV)
- Guidance Documents (AGD)
- Life-Cycle Support (ALC)
- Testing (ATE)
- Vulnerability Assessment (AVA)

Note the "A"

GENERAL DYNAMICS
Decision Systems

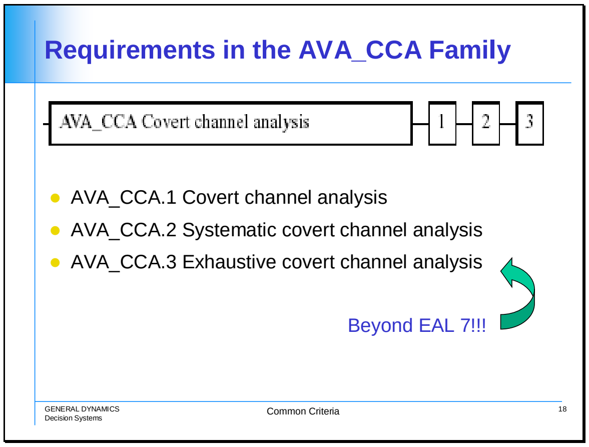
Common Criteria 16



Families in the AVA Class

- AVA_CCA: Covert Channel Analysis
- AVA_MSU: Misuse
- AVA_SOF: Strength of Function
- AVA_VLA: Vulnerability Analysis

GENERAL DYNAMICS
Decision Systems
Common Criteria 17



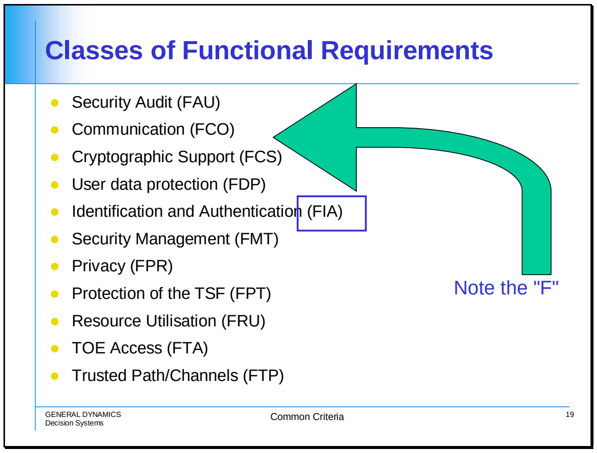
Requirements in the AVA_CCA Family

AVA_CCA Covert channel analysis 1 2 3

- AVA_CCA.1 Covert channel analysis
- AVA_CCA.2 Systematic covert channel analysis
- AVA_CCA.3 Exhaustive covert channel analysis

Beyond EAL 7!!!

GENERAL DYNAMICS
Decision Systems
Common Criteria 18

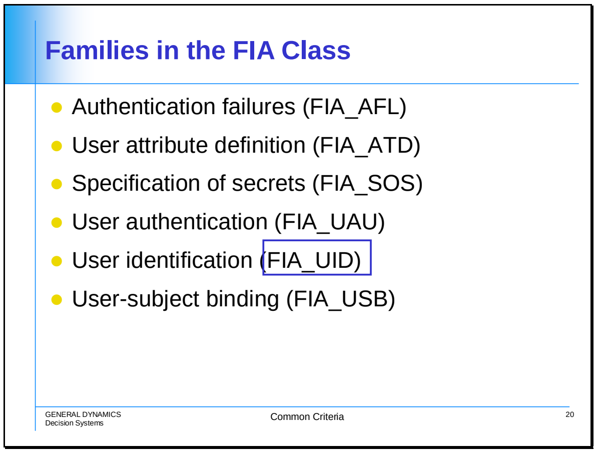


Classes of Functional Requirements

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic Support (FCS)
- User data protection (FDP)
- Identification and Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the TSF (FPT)
- Resource Utilisation (FRU)
- TOE Access (FTA)
- Trusted Path/Channels (FTP)

Note the "F"

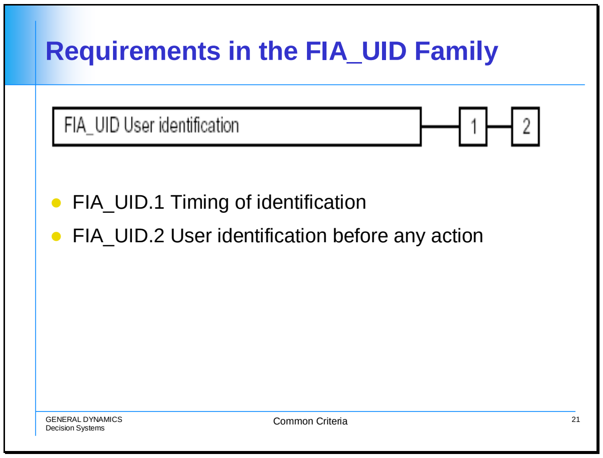
GENERAL DYNAMICS
Decision Systems
Common Criteria 19



Families in the FIA Class

- Authentication failures (FIA_AFL)
- User attribute definition (FIA_ATD)
- Specification of secrets (FIA_SOS)
- User authentication (FIA_UAU)
- User identification (FIA_UID)
- User-subject binding (FIA_USB)

GENERAL DYNAMICS
Decision Systems
Common Criteria 20

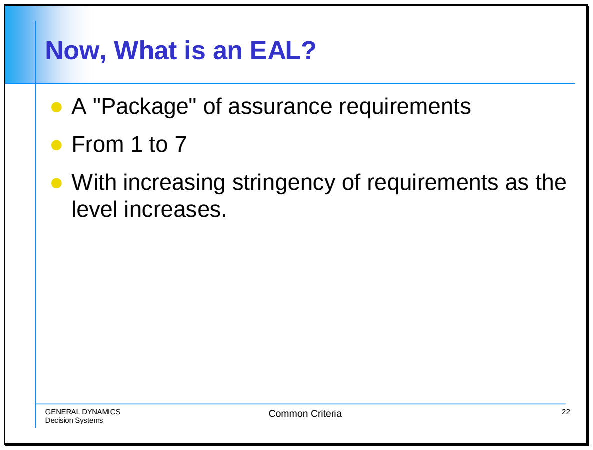


Requirements in the FIA_UID Family

FIA_UID User identification 1 2

- FIA_UID.1 Timing of identification
- FIA_UID.2 User identification before any action

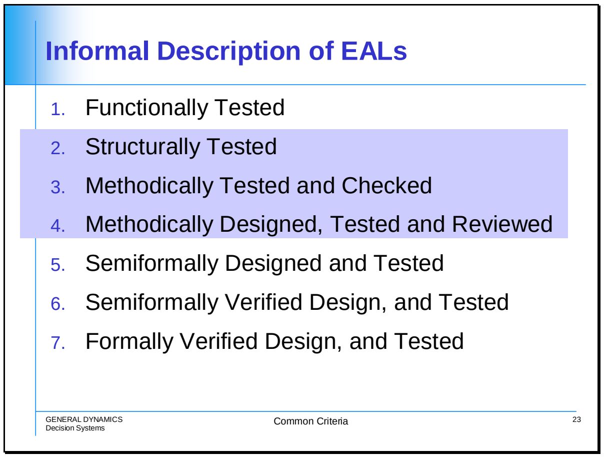
GENERAL DYNAMICS
Decision Systems
Common Criteria 21



Now, What is an EAL?

- A "Package" of assurance requirements
- From 1 to 7
- With increasing stringency of requirements as the level increases.

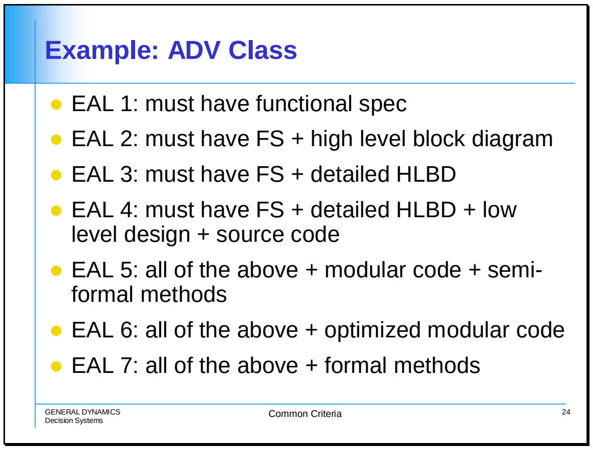
GENERAL DYNAMICS
Decision Systems
Common Criteria 22



Informal Description of EALs

1. Functionally Tested
2. Structurally Tested
3. Methodically Tested and Checked
4. Methodically Designed, Tested and Reviewed
5. Semiformally Designed and Tested
6. Semiformally Verified Design, and Tested
7. Formally Verified Design, and Tested

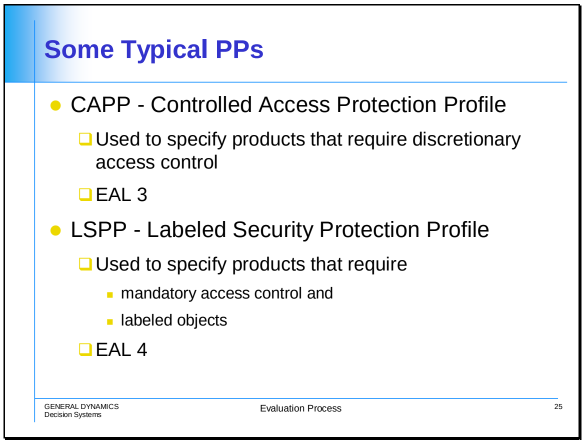
GENERAL DYNAMICS
Decision Systems
Common Criteria
23



Example: ADV Class

- EAL 1: must have functional spec
- EAL 2: must have FS + high level block diagram
- EAL 3: must have FS + detailed HLBD
- EAL 4: must have FS + detailed HLBD + low level design + source code
- EAL 5: all of the above + modular code + semi-formal methods
- EAL 6: all of the above + optimized modular code
- EAL 7: all of the above + formal methods

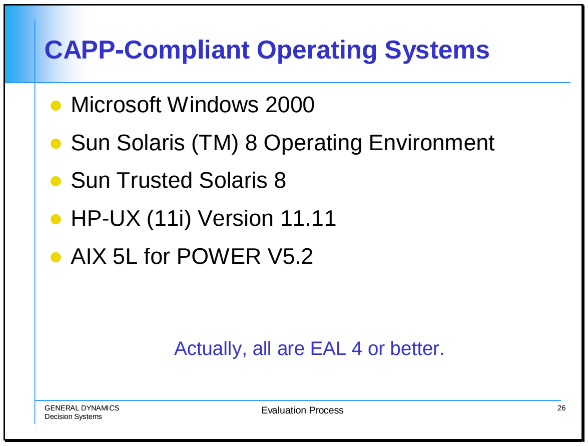
GENERAL DYNAMICS
Decision Systems
Common Criteria
24



Some Typical PPs

- CAPP - Controlled Access Protection Profile
  - Used to specify products that require discretionary access control
  - EAL 3
- LSPP - Labeled Security Protection Profile
  - Used to specify products that require
    - mandatory access control and
    - labeled objects
  - EAL 4

GENERAL DYNAMICS
Decision Systems
Evaluation Process
25

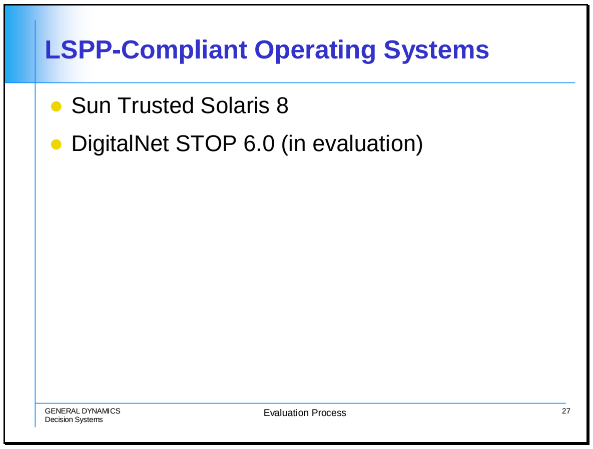


CAPP-Compliant Operating Systems

- Microsoft Windows 2000
- Sun Solaris (TM) 8 Operating Environment
- Sun Trusted Solaris 8
- HP-UX (11i) Version 11.11
- AIX 5L for POWER V5.2

Actually, all are EAL 4 or better.

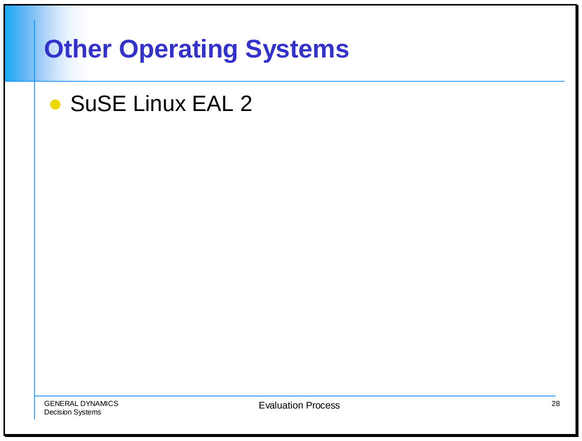
GENERAL DYNAMICS
Decision Systems
Evaluation Process
26



LSPP-Compliant Operating Systems

- Sun Trusted Solaris 8
- DigitalNet STOP 6.0 (in evaluation)

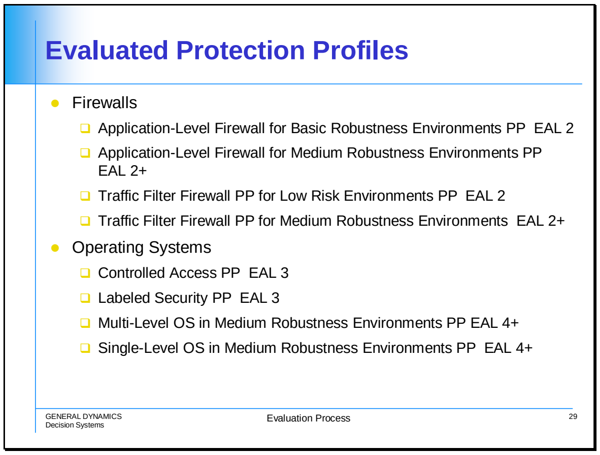
GENERAL DYNAMICS
Decision Systems
Evaluation Process
27



Other Operating Systems

- SuSE Linux EAL 2

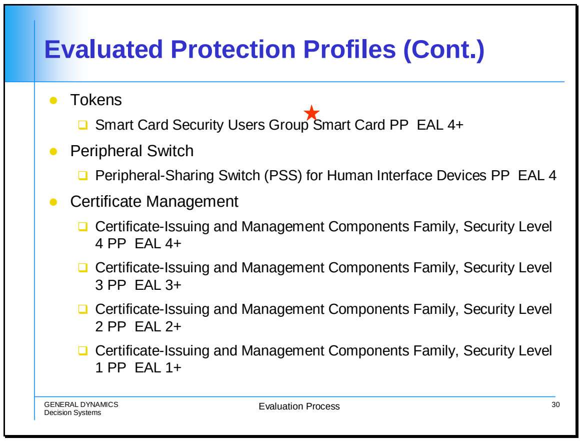
GENERAL DYNAMICS
Decision Systems
Evaluation Process
28



Evaluated Protection Profiles

- Firewalls
  - ❑ Application-Level Firewall for Basic Robustness Environments PP EAL 2
  - ❑ Application-Level Firewall for Medium Robustness Environments PP EAL 2+
  - ❑ Traffic Filter Firewall PP for Low Risk Environments PP EAL 2
  - ❑ Traffic Filter Firewall PP for Medium Robustness Environments EAL 2+
- Operating Systems
  - ❑ Controlled Access PP EAL 3
  - ❑ Labeled Security PP EAL 3
  - ❑ Multi-Level OS in Medium Robustness Environments PP EAL 4+
  - ❑ Single-Level OS in Medium Robustness Environments PP EAL 4+

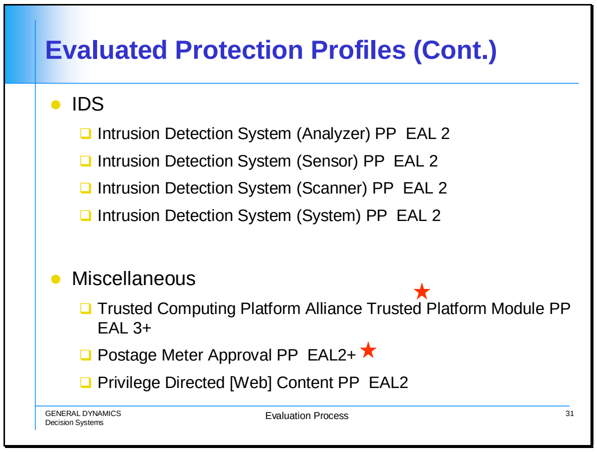
GENERAL DYNAMICS
Decision Systems
Evaluation Process
29



Evaluated Protection Profiles (Cont.)

- Tokens
  - ❑ Smart Card Security Users Group ★ Smart Card PP EAL 4+
- Peripheral Switch
  - ❑ Peripheral-Sharing Switch (PSS) for Human Interface Devices PP EAL 4
- Certificate Management
  - ❑ Certificate-Issuing and Management Components Family, Security Level 4 PP EAL 4+
  - ❑ Certificate-Issuing and Management Components Family, Security Level 3 PP EAL 3+
  - ❑ Certificate-Issuing and Management Components Family, Security Level 2 PP EAL 2+
  - ❑ Certificate-Issuing and Management Components Family, Security Level 1 PP EAL 1+

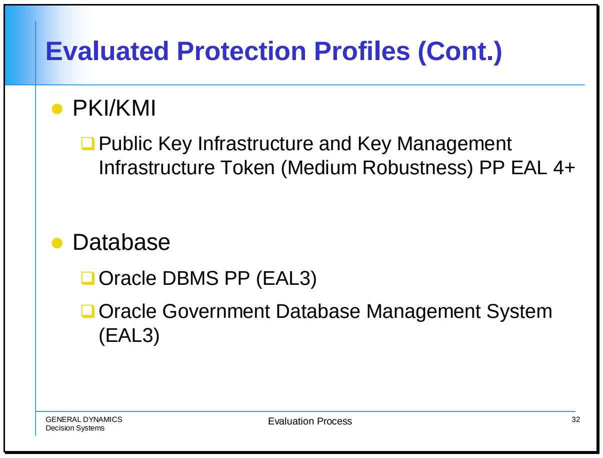
GENERAL DYNAMICS
Decision Systems
Evaluation Process
30



Evaluated Protection Profiles (Cont.)

- IDS
  - ❑ Intrusion Detection System (Analyzer) PP EAL 2
  - ❑ Intrusion Detection System (Sensor) PP EAL 2
  - ❑ Intrusion Detection System (Scanner) PP EAL 2
  - ❑ Intrusion Detection System (System) PP EAL 2
- Miscellaneous
  - ❑ Trusted Computing Platform Alliance Trusted ★ Platform Module PP EAL 3+
  - ❑ Postage Meter Approval PP EAL2+ ★
  - ❑ Privilege Directed [Web] Content PP EAL2

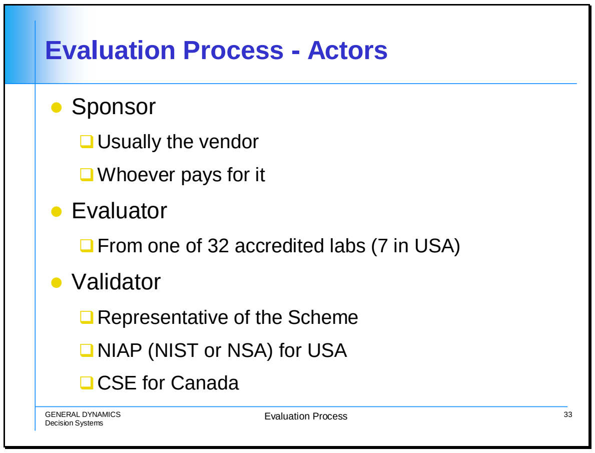
GENERAL DYNAMICS
Decision Systems
Evaluation Process
31



Evaluated Protection Profiles (Cont.)

- PKI/KMI
  - ❑ Public Key Infrastructure and Key Management Infrastructure Token (Medium Robustness) PP EAL 4+
- Database
  - ❑ Oracle DBMS PP (EAL3)
  - ❑ Oracle Government Database Management System (EAL3)

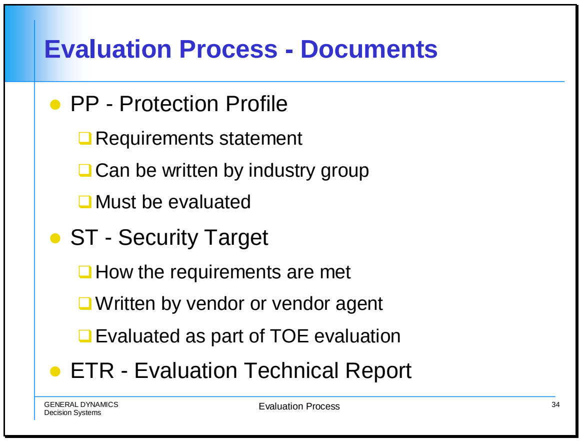
GENERAL DYNAMICS
Decision Systems
Evaluation Process
32



Evaluation Process - Actors

- Sponsor
  - ❑ Usually the vendor
  - ❑ Whoever pays for it
- Evaluator
  - ❑ From one of 32 accredited labs (7 in USA)
- Validator
  - ❑ Representative of the Scheme
  - ❑ NIAP (NIST or NSA) for USA
  - ❑ CSE for Canada

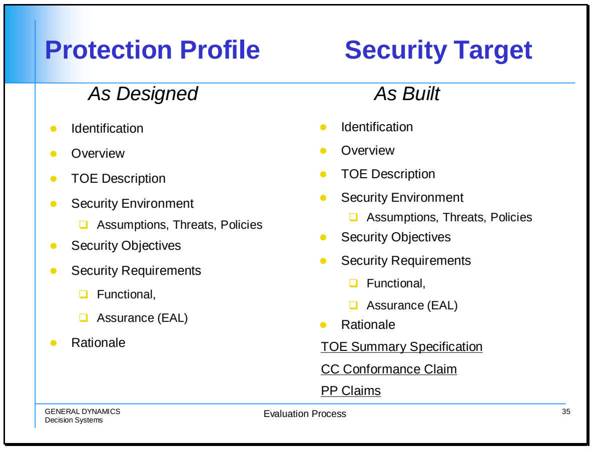
GENERAL DYNAMICS
Decision Systems
Evaluation Process
33



Evaluation Process - Documents

- PP - Protection Profile
  - ❑ Requirements statement
  - ❑ Can be written by industry group
  - ❑ Must be evaluated
- ST - Security Target
  - ❑ How the requirements are met
  - ❑ Written by vendor or vendor agent
  - ❑ Evaluated as part of TOE evaluation
- ETR - Evaluation Technical Report

GENERAL DYNAMICS
Decision Systems
Evaluation Process
34



Protection Profile

As Designed

- Identification
- Overview
- TOE Description
- Security Environment
  - ❑ Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - ❑ Functional,
  - ❑ Assurance (EAL)
- Rationale

Security Target

As Built

- Identification
- Overview
- TOE Description
- Security Environment
  - ❑ Assumptions, Threats, Policies
- Security Objectives
- Security Requirements
  - ❑ Functional,
  - ❑ Assurance (EAL)
- Rationale

TOE Summary Specification

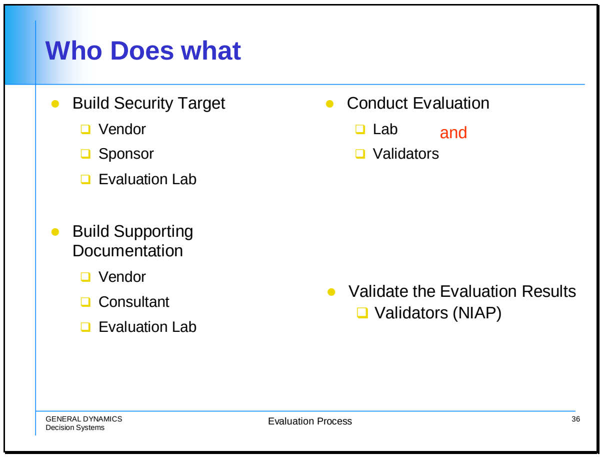
CC Conformance Claim

PP Claims

GENERAL DYNAMICS
Decision Systems

Evaluation Process

35



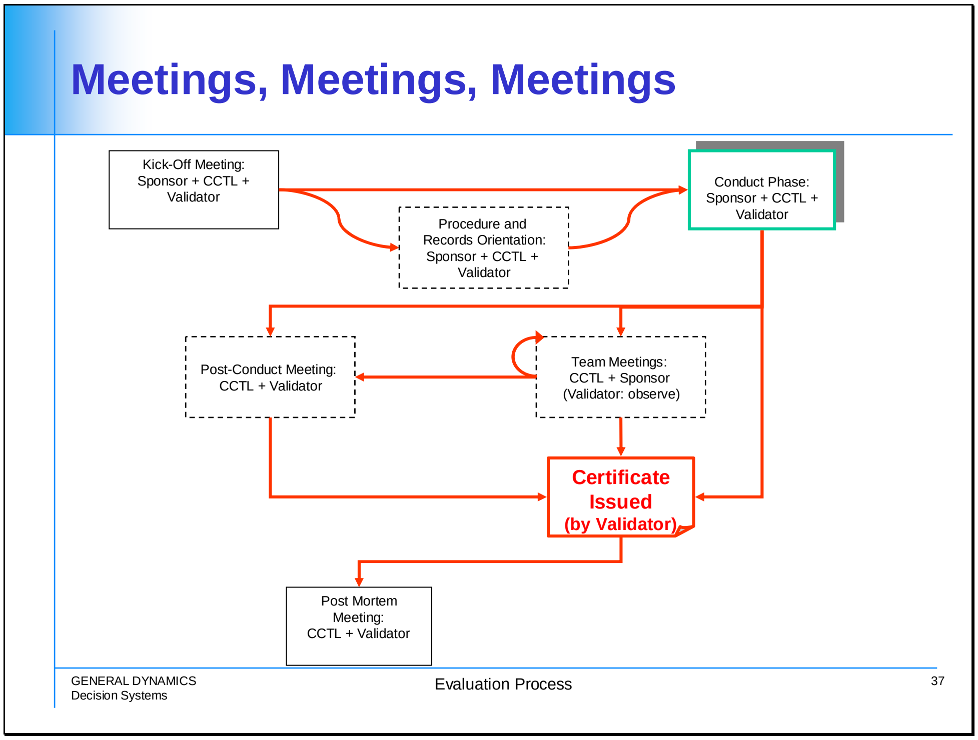
Who Does what

- Build Security Target
  - ❑ Vendor
  - ❑ Sponsor
  - ❑ Evaluation Lab
- Build Supporting Documentation
  - ❑ Vendor
  - ❑ Consultant
  - ❑ Evaluation Lab
- Conduct Evaluation
  - ❑ Lab and
  - ❑ Validators
- Validate the Evaluation Results
  - ❑ Validators (NIAP)

GENERAL DYNAMICS
Decision Systems

Evaluation Process

36



Meetings, Meetings, Meetings

Kick-Off Meeting: Sponsor + CCTL + Validator

Procedure and Records Orientation: Sponsor + CCTL + Validator

Conduct Phase: Sponsor + CCTL + Validator

Post-Conduct Meeting: CCTL + Validator

Team Meetings: CCTL + Sponsor (Validator: observe)

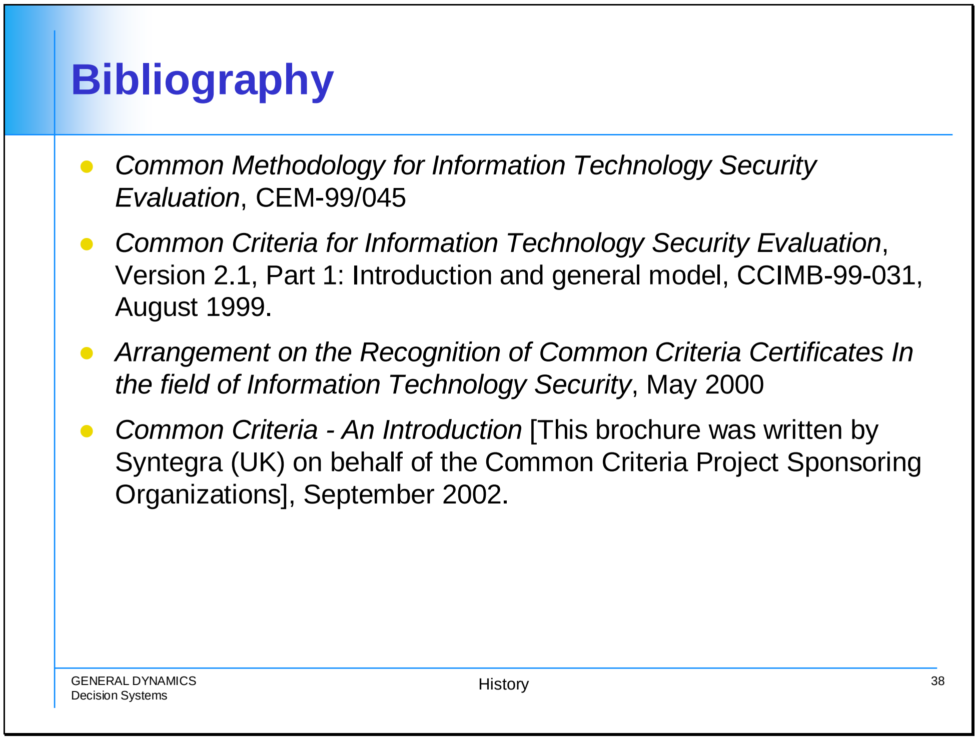
Certificate Issued (by Validator)

Post Mortem Meeting: CCTL + Validator

GENERAL DYNAMICS
Decision Systems

Evaluation Process

37



Bibliography

- *Common Methodology for Information Technology Security Evaluation*, CEM-99/045
- *Common Criteria for Information Technology Security Evaluation*, Version 2.1, Part 1: Introduction and general model, CCIMB-99-031, August 1999.
- *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, May 2000
- *Common Criteria - An Introduction* [This brochure was written by Syntegra (UK) on behalf of the Common Criteria Project Sponsoring Organizations], September 2002.

GENERAL DYNAMICS
Decision Systems

History

38

Appendix E: Terminology Defined in IETF RFC 2119

The following words, which are defined in Internet Engineering Task Force RFC 2119, are used by many standards organizations. They are also used in this document with the meanings as defined below. Note that the force of these words is modified by the requirement level of the document in which they are used.

1. **MUST**: This word, or the terms **REQUIRED** or **SHALL**, mean that the definition is an absolute requirement of the specification.
2. **MUST NOT**: This phrase, or the phrase **SHALL NOT**, mean that the definition is an absolute prohibition of the specification.
3. **SHOULD**: This word, or the adjective **RECOMMENDED**, mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT**: This phrase, or the phrase **NOT RECOMMENDED**, mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. **MAY**: This word, or the adjective **OPTIONAL**, means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product, whereas another vendor may omit the same item. An implementation that does not include a particular option MUST be prepared to interoperate with another implementation that does include the option, although perhaps with reduced functionality. Similarly, an implementation that does include a particular option MUST be prepared to interoperate with another implementation that does not include the option (except, of course, for the feature the option provides.)

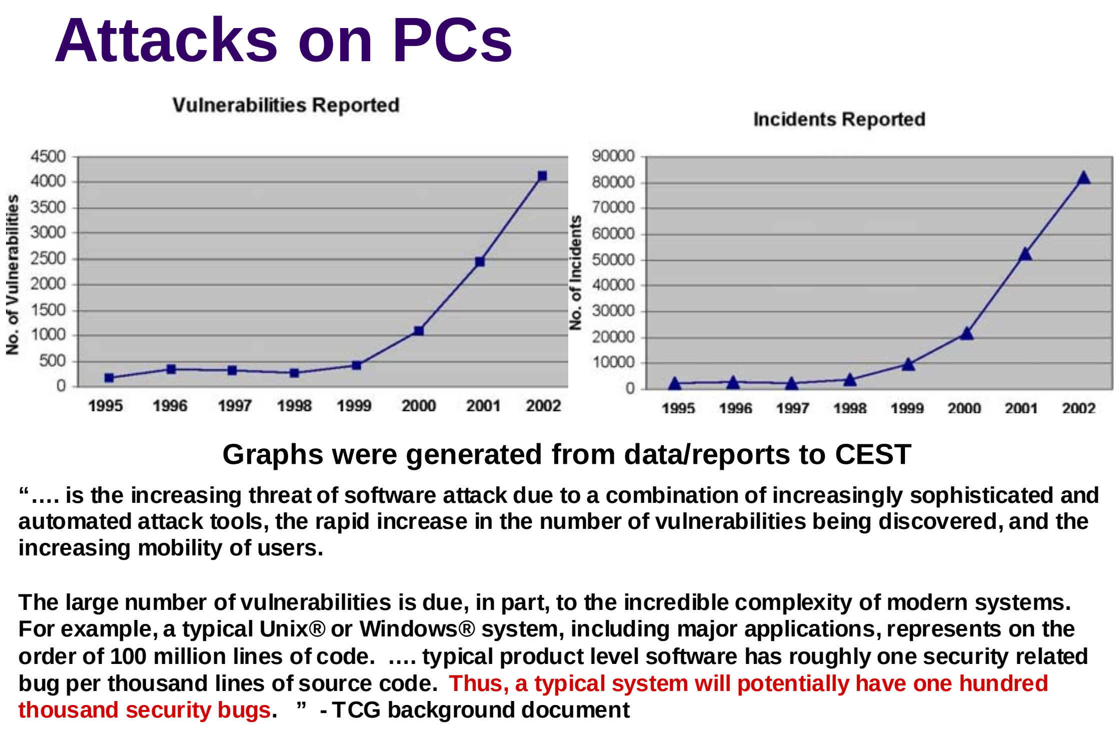
E.1 Guidance in the Use of These Imperatives

Imperatives of the type defined in this memo must be used with care and sparingly. In particular, they MUST be used only where it is actually required for interoperation or to limit behavior that has potential for causing harm (e.g., limiting retransmissions) For example, they must not be used to try to impose a particular method on implementers where the method is not required for interoperability.

E.2 Security Considerations

These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements because most implementers will not have had the benefit of the experience and discussion that produced the specification.

Appendix F: Security Attacks on Personal Computers



Graphs were generated from data/reports to CEST

"…. is the increasing threat of software attack due to a combination of increasingly sophisticated and automated attack tools, the rapid increase in the number of vulnerabilities being discovered, and the increasing mobility of users.

The large number of vulnerabilities is due, in part, to the incredible complexity of modern systems. For example, a typical Unix® or Windows® system, including major applications, represents on the order of 100 million lines of code. …. typical product level software has roughly one security related bug per thousand lines of source code. Thus, a typical system will potentially have one hundred thousand security bugs. " - TCG background document