ETSI TR 103 087 V1.2.1 (2017-11)

Reconfigurable Radio Systems (RRS);
Security related use cases and threats

Reference
RTR/RRS-0313

Keywords
radio, safety, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

The present document presents a security threat analysis of RRS networks and devices for a set of specific use cases and operational scenarios defined in ETSI TC RRS.

It is recommended to consider [i.1], [i.2], [i.3], [i.5], [i.6], [i.7], [i.8] and [i.18] for further information on the framework related to the solutions in the present document.

1 Scope

The present document provides an analysis of the risk of security attacks on the operation of reconfigurable radio systems. It identifies which security threats can disrupt RRS networks and devices or can induce negative impacts on other radio communication services operating in the same radio spectrum. The present document also identifies stakeholder and assets, which can be potentially impacted by the security threats.

The present document extends the set of use cases addressed over those covered by ETSI TR 103 087 (V1.1.1) [i.30] to cover the following:

- Remote attestation of the Reconfigurable Equipment status (installed RA and DoC).
- Configuration enforcement of reconfigurable equipment.
- Distribution and enforcement of mobility policies.
- Long-term management of devices (in particular orphaned devices).
- Secure device root of trust.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Recommendation ITU-T E.408: "Security in Telecommunications and Information Technology. An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications. Telecommunication networks security requirements".

[i.2] L. B. Michael, M. J. Mihaljevic, S. Haruyama and R. Kohno: "A framework for secure download for software-defined radio", IEEE Communications Magazine, July 2002.

[i.3] A. N. Mody, R. Reddy, T. Kiernan and T.X. Brown: "Security in cognitive radio networks: An example using the commercial IEEE 802.22 standard", Military Communications Conference, 2009. MILCOM 2009. IEEE, vol., no., pp.1-7, 18-21 Oct. 2009, Boston, MA, USA.

[i.4] Document Id: WINNF-08-P-0013: "Wireless Innovation Forum's Security Working Group. Securing Software Reconfigurable Communications Devices".

[i.5] ETSI TR 103 062: "Reconfigurable Radio Systems (RRS); Use Cases and Scenarios for Software Defined Radio (SDR) Reference Architecture for Mobile Device".

[i.6] ETSI TR 102 907: "Reconfigurable Radio Systems (RRS); Use Cases for Operation in White Space Frequency Bands".

[i.7] ETSI TR 103 063: "Reconfigurable Radio Systems (RRS); Use Cases for Reconfigurable Radio Systems operating in IMT bands and GSM bands for intra-operator scenarios".

[i.8] ETSI TR 102 944: "Reconfigurable Radio Systems (RRS); Use Cases for Baseband Interfaces for Unified Radio Applications of Mobile Device".

[i.9] ETSI TS 102 165-1 (V4.2.3): "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.10] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.11] ETSI EN 302 969: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Requirements for Mobile Devices".

[i.12] ETSI TS 103 436: "Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios".

[i.13] ETSI EN 303 095: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices".

[i.14] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC.

[i.15] Directive 2014/35/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of electrical equipment designed for use within certain voltage limits Text with EEA relevance.

[i.16] Directive 2014/30/EU of the European Parliament and of the Council of 26 February 2014 on the harmonisation of the laws of the Member States relating to electromagnetic compatibility (recast) (Text with EEA relevance).

[i.17] Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation (EEC) No 339/93 (Text with EEA relevance).

NOTE: Available at http://eur-lex.europa.eu/.

[i.18] ETSI TR 102 967: "Reconfigurable Radio Systems (RRS); Use Cases for dynamic equipment reconfiguration".

[i.19] ETSI EN 303 146-2: "Reconfigurable Radio Systems (RRS); Mobile Device (MD) information models and protocols; Part 2: Reconfigurable Radio Frequency Interface (RRFI)".

[i.20] ETSI TS 103 146-3: "Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols Part 3: Unified Radio Application Interface (URAI)".

[i.21] Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

[i.22] ETSI GS NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.23] ETSI TS 103 146-4: " Reconfigurable Radio Systems (RRS); Mobile Device Information Models and Protocols; Part 4: Radio Programming Interface (RPI)".

[i.24] Open Mobile Alliance™ OMA-ERP-DM-V1_3: "OMA Device Management".

NOTE: Available at http://www.openmobilealliance.org/.

[i.25] Open Mobile Alliance™ OMA-ERP-LightweightM2M-V1_0: "OMA LightweightM2M (LWM2M)".

NOTE: Available at http://www.openmobilealliance.org/.

[i.26] GSM Association RCC.14 : "Service Provider Device Configuration".

[i.27] ETSI TR 103 502: "Reconfigurable Radio Systems (RRS); Applicability of RRS with existing Radio Access Technologies and core networks Security aspects".

[i.28] Trusted Computing Group: "Trusted Platform Module Library, Part 1: Architecture, Family '2.0'".

[i.29] Trusted Computing Group: "TPM Main, Part 1, Design Principles".

NOTE: Available at https://trustedcomputinggroup.org/.

[i.30] ETSI TR 103 087 (V1.1.1): " Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems".

[i.31] IEEE 802.11™: "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.32] Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

assigned frequency band: frequency band or sub-band within which the device is authorized to operate and to perform the intended function of the equipment

National Regulatory Authority (NRA): body or bodies charged by a Member State with any of the regulatory tasks assigned in this Directive and the Specific Directives (Framework Directive 2002/21/EC [i.21])

radio system: system capable to communicate some user information by using electromagnetic waves

NOTE: Radio system is typically designed to use certain radio frequency band(s) and it includes agreed schemes for multiple access, modulation, channel and data coding as well as control protocols for all radio layers needed to maintain user data links between adjacent radio devices.

RE Configuration Policy: machine-readable document that is generated by the RE manufacturer or its representative (such as the Conformity Contact Entity) (such as the Conformity Contact Entity), and which contains instructions that are relevant for the RE to maintain compliance to the RED (for example, valid hardware and software combinations)

NOTE: Security objectives regarding to the DoC should be understood as applying both to the DoC and the RE Configuration Policy. Procedures that involve decision making based on the DoC implicitly use the RE Configuration Policy.

Reconfigurable Radio System (RRS): radio system using reconfigurable radio technology

security threat: potential violation of security

NOTE: Examples of security threats are loss or disclosure of information or modification/destruction of assets. A security threat can be intentional like a deliberate attack or unintentional due to an internal failure or malfunctions.

use case: description of a system from a user's perspective

NOTE 1: Use cases treat a system as a black box, and the interactions with the system, including system responses, are perceived as from outside the system. Use cases typically avoid technical jargon, preferring instead the language of the end user or domain expert.

NOTE 2: Use cases should not be confused with the features/requirements of the system under consideration. A use case may be related to one or more features/requirements; a feature/requirement may be related to one or more use cases.

NOTE 3: A brief use case consists of a few sentences summarizing the use case.

user: user of the Mobile Network

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

3GPP	Third Generation Partnership Project
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASF	Administrator Security Function
CA	Certificate Authority
CCE	Conformity Contact Entity
CE	Conformité Européenne
CIAAA	Confidentiality, Integrity, Authentication, Availability, and Accounting
CM	Configuration Manager
CoAP	Constrained Application Protocol
ComSec	Communication Security
CPU	Central Processing Unit
CR	Cognitive Radio
CSL	Communication Service Layer
CSP	Communication Service Provider
DAA	Download Authorization Authority
DM	Device Management
DMA	Direct Memory Access
DoC	Declaration of Conformity
DTLS	Datagram Transport Layer Security
EK	Endorsement Key
EU	European Union
GBA	Generic Bootstrapping Architecture
GNSS	Global Navigation Satellite System
GS	Group Specification
GSM	Global System for Mobile Communications
GSMA	Global System for Mobile Communications Association
HAL	Hardware Abstraction Layer
HMAC	keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	HardWare
IMEI	International Mobile Equipment Identity
IP	Internet Protocol
IR	Intermediate Representation
IT	Information Technology
JSON	JavaScript Object Notation
JTAG	Joint Test Action Group
LTE	Long Term Evolution
LWM2M	LightWeight Machine to Machine
M2M	Machine to Machine
MAC	Medium Access Control
MCC	Mobile Country Code
MD	Mobile Device
MDRC	Mobile Device Reconfiguration Class
MNC	Mobile Network Code
MO	Management Object
MURI	MUltiRadio Interface
NFV	Network Function Virtualisation

NRA	National Regulatory Authority
OBEX	OBject EXchange
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OS	Operating System
OSI	Open System Interconnection
PCR	Platform Configuration Register
PHY	PHYsical
PKC	Public Key Certificate
PKI	Public Key Infrastructure
QA	Quality Assurance
RA	Radio Application
RAP	Radio Application Package
RAT	Radio Access Technology
RC	Radio Controller
RCF	Radio Controller Framework
RE	Reconfigurable Equipment
RECP	Reconfigurable Equipment Configuration Policy
RED	Radio Equipment Directive
RF	Radio Frequency
RPI	Radio Programming Interface
RPOE	Radio Platform Operating Environment
RRFI	Reconfigurable Radio Frequency Interface
RRS	Reconfigurable Radio System
RRS-CP	RRS Configuration Provider
RVM	Radio Virtual Machine
SAE	System Architecture Evolution
SCA	Software Communication Architecture
SCADA	Supervisory Control And Data Acquisition
SCC	Standards Coordination Committee
SCP	Software/Content Provider
SD	Software Distributor
SDR	Software Defined Radio
SDRD	Software Defined and Reconfigurable Devices
SFB	Standard Functional Block
SHA	Secure Hash Algorithm
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPA	Service Provider Application
SPDC	Service Provider Device Configuration
SW	Software
SWIR	Software Intermediate Representation
TAD	Transfer of Authority Document
TLS	Transport Layer Security
TLV	Type-Length-Value
TOE	Target Of Evaluation
TPM	Trusted Platform Module
TR	Technical Report
TRNG	True Random Number Generator
TVRA	Threat Vulnerability Risk Analysis
UA	User Application
UDFB	User Defined Functional Block
UDP	User Datagram Protocol
UML	Unified Model Language
URA	Unified Radio Application
URAI	Unified Radio Application Interface
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Unique Reference Number
USB	Universal SErial Bus

VNFCI	Virtual Network Function Component Instance
WAP	Wireless Application Protocol
XACML	eXtensible Access Control Markup Language
XML	eXtensible Markup Language

4 Method of analysis

The approach to security analysis given in ETSI TS 102 165-1 [i.9] is a multi-step process that is intended to identify, in its first steps, system objectives and the target of evaluation - in other words to clearly identify what is the thing being analysed in order to identify where its points of attack are. The method applied in the present document is derived from that described in ETSI TS 102 165-1 [i.9] in order to provide the rationale to identify and design the security countermeasures for RRS by application of a systematic method, and to allow users to visualize the relationship of objectives, requirements, system design and system vulnerabilities.

NOTE: The TVRA method defined in ETSI TS 102 165-1 [i.9] is under review to extend the treatment of motivation and of multi-point attacks (e.g. as used in distributed denial of service attacks). The revisions do not impact the analysis given in the present document.

In order to assist the reader a short overview of the role and purpose of the TVRA method is given, although for complete details the reader is advised to consult the reference document. The depth of the TVRA changes as the system design becomes more detailed. A TVRA working from the system objectives will identify at a very coarse level the required security functionality to ensure that the objectives can be met without damage to the system. The structure of activities in development of a TVRA is shown in figure 1. The process is shown as recursive wherein in any change to any aspect of the system or its environment requires the process to restarted.

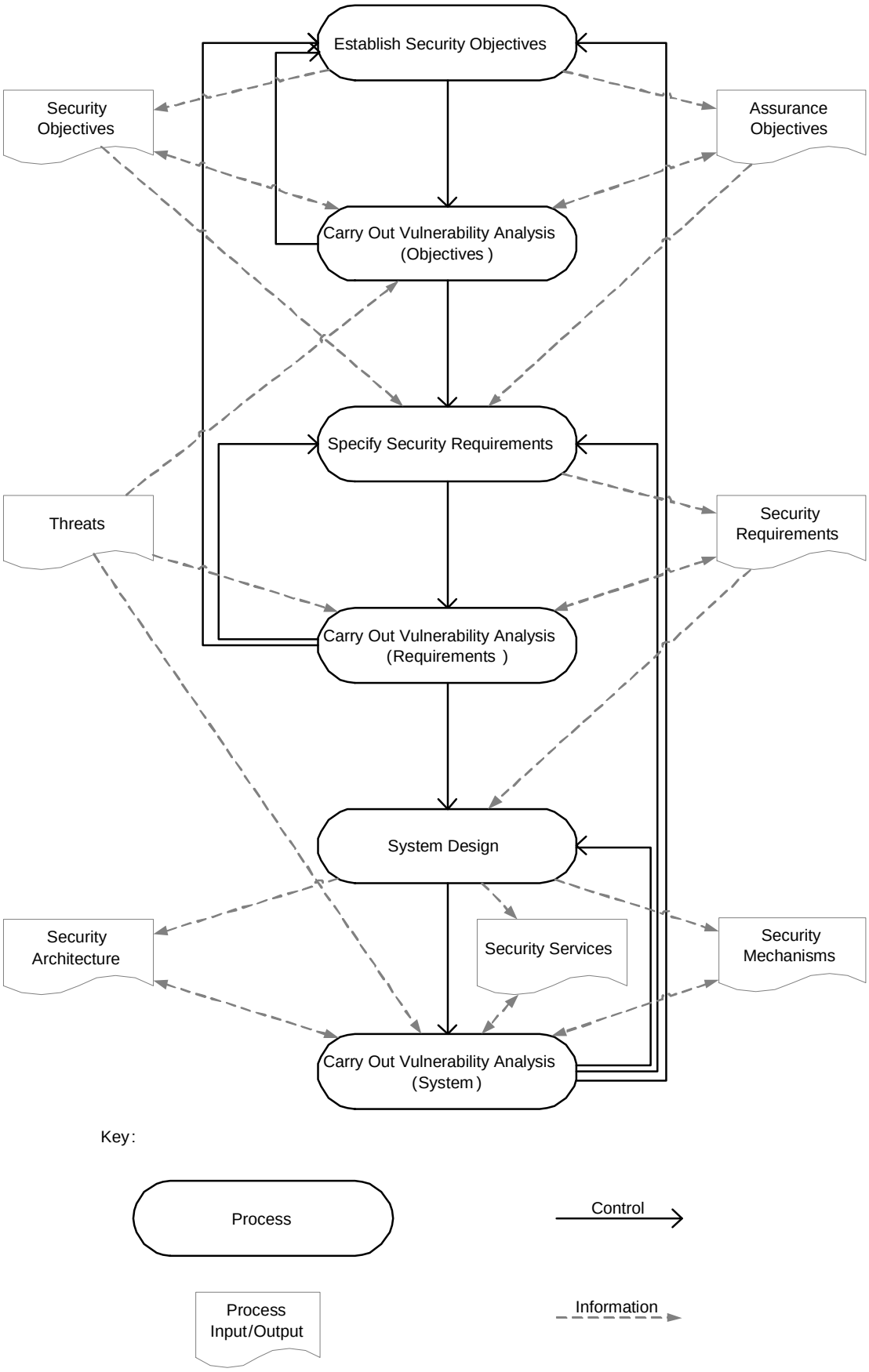

Figure 1: Structure of security analysis and development (from ETSI TS 102 165-1 [i.9])

The purpose of the TVRA is to determine how open to attack the system, or components of the system are. The TVRA method models a system consisting of assets. An asset may be physical, human or logical. **Assets** in the model may have **Weaknesses** that may be attacked by **Threats**. A **Threat** is enacted by a **Threat Agent**, and may lead to an **Unwanted Incident** breaking certain pre-defined security objectives. A **Vulnerability** is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**. When applied, **Countermeasures** protect against **Threats** to **Vulnerabilities** and reduce the **Risk**.

The TVRA method process consists of the following steps:

1) Identification of the Target of Evaluation (TOE) resulting in a high level description of the main assets of the TOE and the TOE environment and a specification of the goal, purpose and scope of the TVRA.

NOTE 1: For the present document the ToE is defined in clause 7.

2) Identification of the objectives resulting in a high level statement of the security aims and issues to be resolved.

NOTE 2: For the present document the objectives and the resultant high level statement of security provisions for RRS in the context of the ToE can be found in clause 5.

3) Identification of the functional security requirements, derived from the objectives from step 2.

4) Inventory of the assets as refinements of the high level asset descriptions from step 1 and additional assets as a result of steps 2 and 3.

5) Identification and classification of the vulnerabilities in the system, the threats that can exploit them, and the unwanted incidents that may result.

6) Quantifying the occurrence likelihood and impact of the threats.

7) Establishment of the risks.

8) Identification of countermeasures framework (conceptual) resulting in a list of alternative security services and capabilities needed to reduce the risk.

NOTE 3: The output of steps 3 through 7 are presented in clauses 6 and 7 with the conceptual framework given at the end of clause 7.

9) Countermeasure cost-benefit analysis (including security requirements cost-benefit analysis depending on the scope and purpose of the TVRA) to identify the best fit security services and capabilities amongst alternatives from step 8. The cost-benefit analysis should take account of the impact on each of standards design, implementation, operation, regulatory impact and market acceptance

NOTE 4: An indicative cost benefit analysis for a selected set of measures is given in ETSI TS 103 436 [i.12], clause A.1.

10) Specification of detailed requirements for the security services and capabilities from step 9.

NOTE 5: For RRS the output of step 10 is to be found in ETSI TS 103 436 [i.12].

The application of countermeasures adds assets to the system and may create new vulnerabilities, indicating that the TVRA will need to be undertaken again, and the method should be repeated until all the risks have been reduced to an acceptable level. Furthermore, by allowing the analysis to be rerun when attack likelihood changes, the risk to the system may be re-evaluated as knowledge of new or revised attacks becomes available.

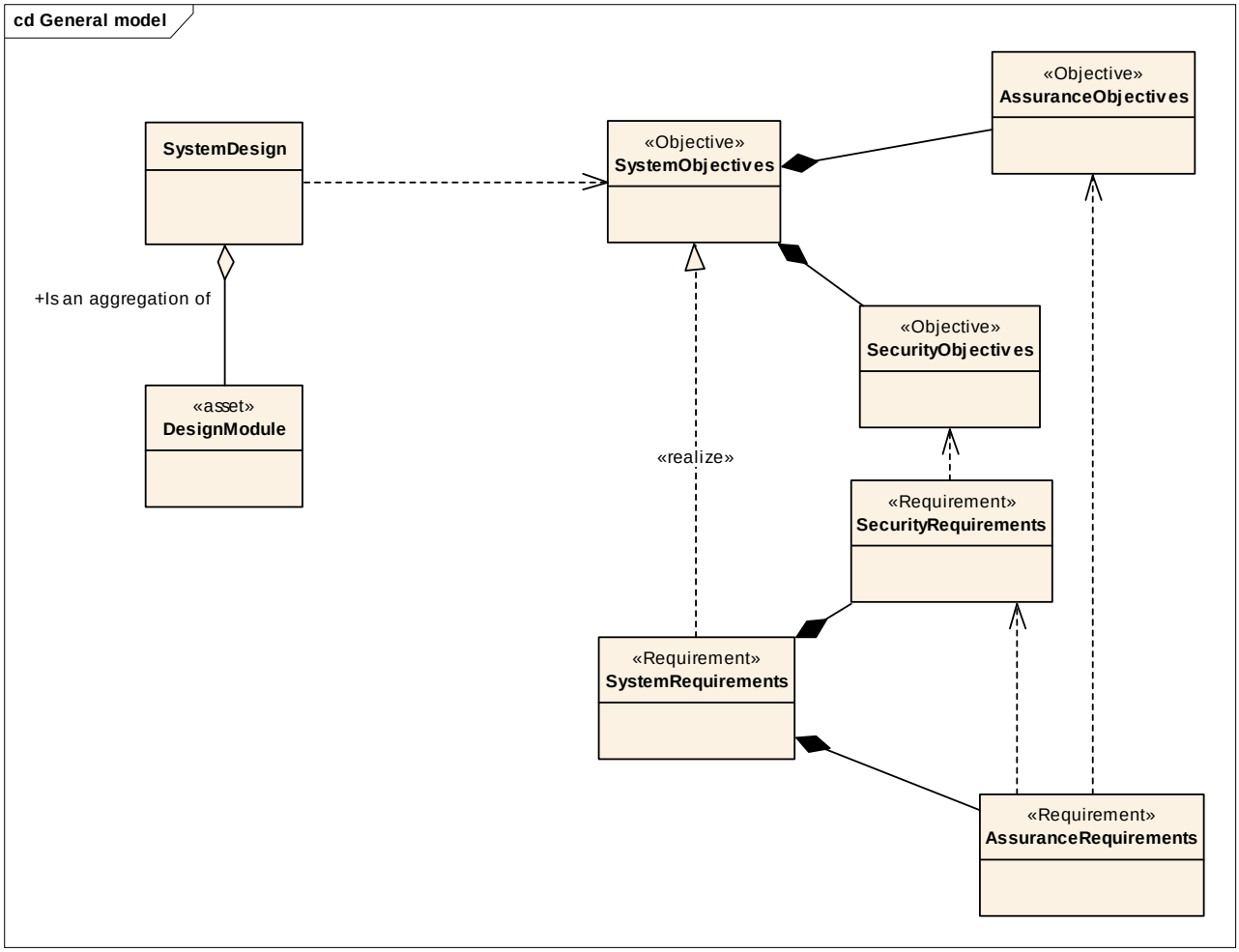

Figure 2: Relationship between system design, objectives and requirements

For most systems the development of system requirements goes far beyond just security and one concern for TVRA is to ensure that the system design is itself robust and therefore has fully documented requirements across all its aspects.

A TVRA requires that both the system being examined (with its catalogued objectives and requirements) and the assets of the system and how it fits to its environment are clearly identified. In the context of TVRA the key relationship is that between a vulnerability and an asset and this is a weighted relationship with the weighting being defined as the risk to the asset due to the associated vulnerability.

A pictorial view of the asset-threat-weakness-vulnerability-countermeasure relationship to system design is given in figure 3.

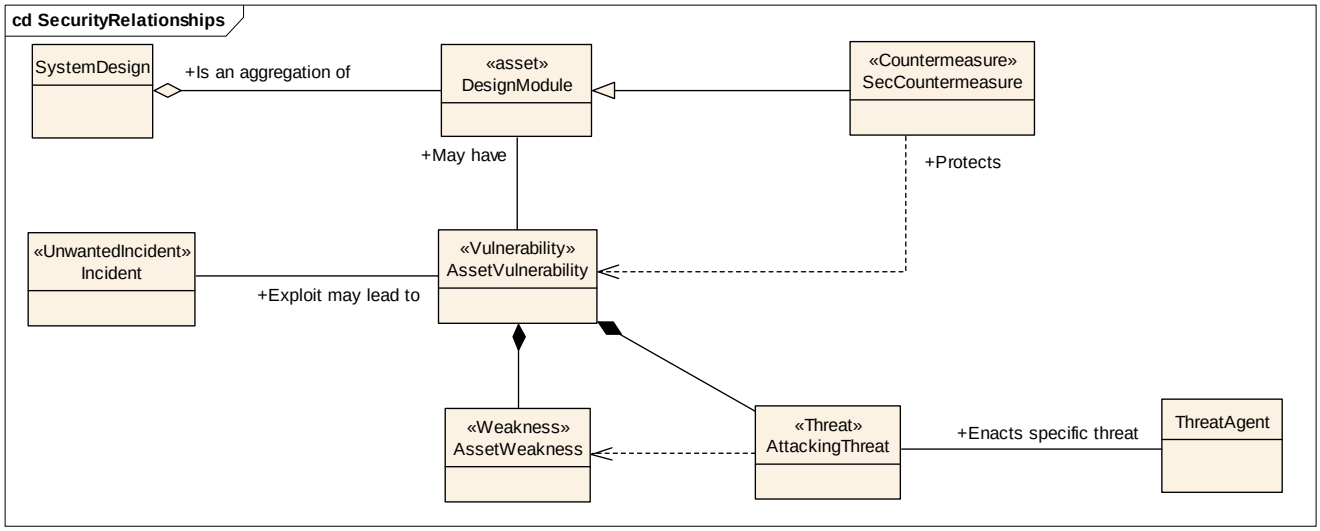

Figure 3: Generic security TVRA model

One of the purposes of security design is to minimize the probability of any instance of the class "unwanted incident" being instantiated. It should be noted that whilst some countermeasures may themselves become system assets, and as such have their own vulnerabilities, many instances of countermeasures will be considered as policies, system guidelines and, if captured early enough, system redesign.

The data types pertaining to the model in figure 3 are given in figure 4. Essentially threats can be classified as one of 5 types:

- Interception.
- Manipulation.
- Denial of service.
- Repudiation of sending.
- Repudiation of receiving.

Similarly, security objectives can be classified as one of 5 types (commonly referred to as "CIAAA" types):

- Confidentiality.
- Integrity.
- Availability.
- Authenticity.
- Accountability.

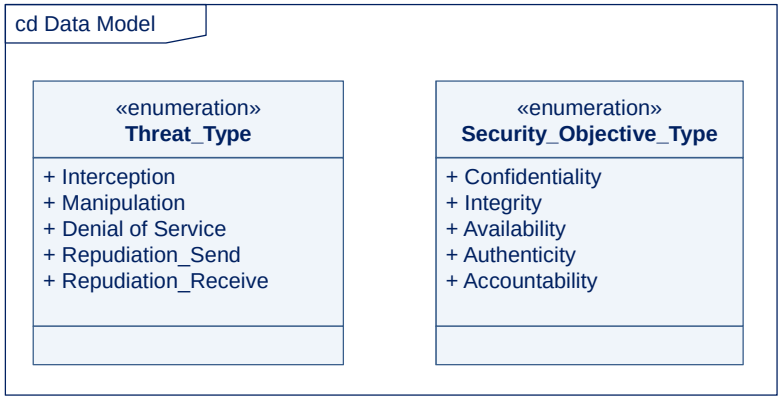

Figure 4: Data types pertaining to security relationship model

5 Security objectives

5.1 Overview

One of the challenges for a successful commercial deployment of Software Defined Radio (SDR) and Cognitive Radio (CR) technologies on top of Reconfigurable Radio Systems (RRS), is to provide an adequate level of security. While SDR and CR based systems should guarantee the same level of security of conventional wireless communication systems, they may also present new vulnerabilities or security threats, and so does RRS. To an external observer, able to only observe the radio interface (the wireless link), a radio equipment should not be detectable as being reconfigurable and thus RRS devices should not be distinguishable from non-RRS devices at this level of observation.

ETSI TR 187 011 [i.10] identifies means to define objectives and requirements in security standards and makes the following distinctions that have to be noted:

- An objective is the expression of what a security system should be able to do in very broad terms whereas a requirement is a more detailed specification of how an objective is achieved. Objectives may be considered to be desires rather than mandates. Security requirements are derived from the security objectives and, in order to make this process simpler, requirements can be further subdivided into functional requirements and detailed requirements.

- Functional security requirements identify the major functions to be used to realize the security objectives. They are specified at a level which gives an indication of the broad behaviour expected of the asset, generally from the user's perspective. Detailed security requirements, as their name implies, specify a much lower-level of behaviour which would, for example, be measurable at a communications interface. Figure 5 shows how functional requirements can be extracted from existing specifications and from other input and that they are combined to achieve the security objectives of the target system. Each functional requirement is realized by a number of implementation requirements.

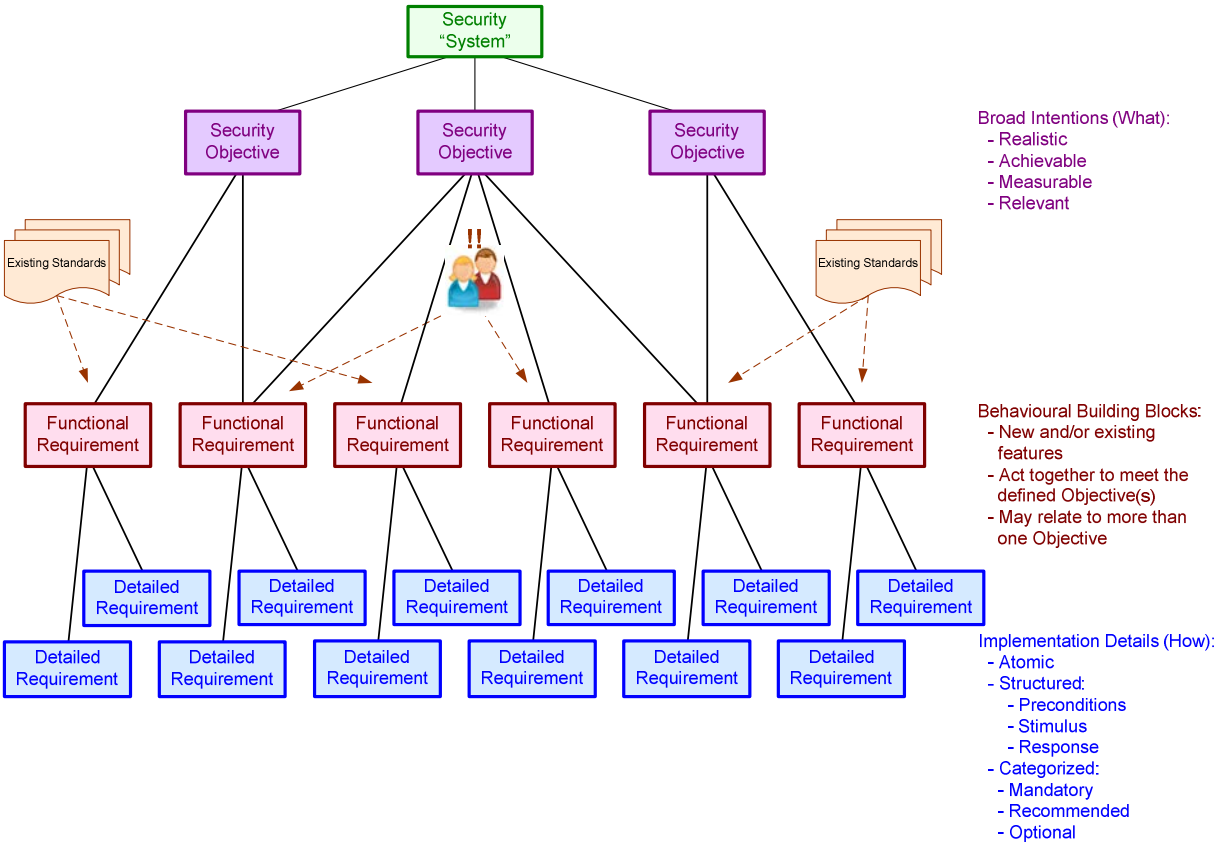

Figure 5: Security objectives and requirements (from ETSI TR 187 011 [i.10])

Each objective is identified against the affected stakeholders or system assets, an indication of the level of system intervention required to meet the objective is given.

The following technical objectives for telecommunications services security in the context of RRS hold:

- Prevention of masquerade:
  - being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and Bob cannot pretend to be Alice;
  - applies to both masquerade of the user and of the system or service.
- Ensure availability of the telecommunications services:
  - the service is to be accessible and usable on demand by an authorized entity.
- Maintain privacy of communication:
  - where the parties to a call communicate across public networks mechanisms should exist to prevent eavesdropping;
  - the only delivery points for communication have to be the legitimate parties to the call.

The ComSec attributes of a particular radio configuration belong to the radio configuration, the role of RRS in loading and operating a particular radio configuration is to assure the user and operator that the system complies with the base requirements of the technology that the RRS configured radio is being deployed as. Thus if the RRS device is configured as a GSM-900 MHz device it has to comply to the security and system requirements of GSM-900 MHz in addition to any constraints implied by the RRS nature of the device.

NOTE: The security provisions of many RATs (e.g. GSM, LTE, SAE and IEEE 802.11 [i.31])) lie at layers 2 and 3 of the OSI protocol stack and do not directly relate to the physical radio properties addressed by RRS at layer 1.

Typical objectives for telecommunication systems include:

1) *Controlled Access to resources:* the system should ensure that unauthorized actors are prevented from gaining access to information or resources of the network or devices.

2) *Service availability:* the system should be able to provide the required communication services as described in specific service level agreements.

3) *Protection of confidentiality:* the system should provide capabilities to ensure the confidentiality of stored and communicated data.

4) *Protection of system integrity:* the systems should be able to guarantee the integrity of system and its components.

5) *Protection of data integrity:* the system should be able to guarantee the integrity of stored and communicated data.

6) *Compliance to regulatory framework:* the system should be able to guarantee the compliance to the regulations active in the area, where the system operates.

7) *Accountability:* the system should ensure that an entity cannot deny the responsibility for any of its performed actions. In this context, accountability is used as a synonym of Non-Repudiation.

8) *Verification of identities:* a telecommunication network should provide capabilities to establish and verify the claimed identity of any actor in the telecommunication network.

5.2 Assumptions and assertions of RRS

In determining the objectives, a number of assumptions are made that refine the scope of the threat analysis and the domain of application of any countermeasures. The following assumptions are made:

- The RRS platform does not define the content of DoC attestations but may add an RE Configuration Policy as an annex to (or companion of) the DoC for the RE to determine compliance of a hardware and software combination.

- The RRS platform does not define the radio application but only defines how it is installed, updated, and how it interfaces to the RE.

NOTE: The radio application is itself defined using an intermediate machine independent set of ConfigCodes (defined in ETSI TS 103 146-4 [i.23]) that are generated from a Software Intermediate Representation (SWIR) of the intended application. An overview of the RA build process is presented in ETSI TS 103 146-4 [i.23].

- The RRS platform and the standards defining it do not define how the DoC is issued, this aspect is governed by the regulatory framework (Directive 2014/53/EU [i.14]).

- For purposes of the detail requirements definition of security processes there is assumed to be a lower and upper bound on the performance of the RE (e.g. processor instructions per time period, memory capacity, memory access rate).

- The point of observation and control for verification of the RRS platform operating as a valid RE is identical to that for a non-RRS platform operating as a valid RE, e.g. a GSM-900 radio should not be distinguishable in any conformance test as being an RRS or non-RRS implementation.

  It is considered that at least the following models apply for reconfiguration of the RE:

  - The RE manufacturer updates the device using the RRS capability to add functionality over the lifetime of the RE (this is somewhat analogous to a software developer extending the functionality of an application or operating system).

  - The user is offered limited control over the configuration of its device, e.g. by being able to choose whether to install an RA implementing a specific RAT in a controlled environment; this may in the future evolve into a model whereby the end user of the radio chooses to extend the functionality of the RE by installing a Radio Application of their choice from a public store.

- Whilst there will be a communications network with associated network roles involved in the distribution of RRS apps and who will support REs that are RRS enabled it is assumed that the packaging of the app and the knowledge that a terminal is an RRS-RE is transparent and the network has only got a passive role in the RRS platform.

5.3 Objectives arising from RED analysis

A detail analysis of the Radio Equipment Directive is given in annex A of the present document. The objectives stated below have been extracted from this analysis:

- The RRS framework should ensure measures are provided to prevent installation of malicious RAPs.
- The RRS framework should ensure measures are provided to prevent modification of an RAP after installation.

NOTE 1: One motivation is that the RRS framework should maintain compliance of the RE to the RED [i.14] (e.g. regarding spectrum usage, health and safety, access to emergency services)

- The RRS framework should provide means to verify the legitimacy of the Declaration of Conformity (DoC) and CE marking.

NOTE 2: This includes the DoC in complete for as well as the combination of the simplified DoC with the referenced complete DoC. These assets are essential to market surveillance and traceability as detailed in clause 7.4.3.

- The RRS platform should provide means to be able to uniquely identify the master copy of the DoC.
- Where CE marking and DoC are provided for display of the radio equipment by means of user interaction the RRS platform should provide means to assure that the marking is resistant to tampering.

NOTE 3: Where conformity assessment is carried through annex IV, Module H of the RED [i.14], the CE marking plays a critical role in traceability.

- The RRS platform should provide means to validate data used to describe the installation requirements of the RAP (the RAP metadata) against the capabilities of the RE and prohibit installations where a mismatch is identified.

NOTE 4: The assumption is that the set of capabilities offered by the RE (as one of the MDRC variants) is a superset of the capabilities required by a RA with a validated DoC.

5.4 Objectives arising from ComSec analysis

Communications Security (ComSec) is that part of the security domain that deals with the security of a communications channel. The identification of a communications channel in ToE#1 between the RadioApp Store and the RRS-enabled RE is one such channel. The channel itself has a number of characteristics, identified in ToE#1, that open it to attack and for which the following security objectives apply:

- Confidentiality:
  - The RRS platform should provide means to ensure that the content of communication between the RadioApp Store and the RE are protected from exposure to unauthorized 3rd parties.
- Integrity:
  - The RRS platform should provide means to verify that the content of communication between the RadioApp Store and RE has not been manipulated prior to processing at receipt.
- Authenticity:
  - The RRS platform should provide means for the RadioApp Store to verify the identity of the RE.
  - The RRS platform should provide means for the RE to verify the identity of the RadioApp Store.

- Availability:
  - The RRS platform should provide means to detect and prevent denial of access to the communications channel between the RadioApp Store and the RE.

5.5 Objectives arising from the analysis of the RAP as ToE#2

The following objectives have been identified from the analysis of ToE#2:

- Integrity:
  - The RRS platform should provide means to verify that the RAP has not been modified between having been made available by the RAP originator and having been downloaded on the RE.
- Authenticity:
  - The RRS platform should provide means for the RE to verify the source of the content supplied via the RadioApp Store.
- Accountability:
  - The RRS platform should allow for a manufacturer to determine whether they did or did not install a given Radio Application on the device, in more details:
    - The RRS platform should provide means to prevent the RadioApp Store denying provision of an App to the RE.
    - The RRS platform should provide means to prevent the RE denying receipt of an RA from the RadioApp Store.
    - The RRS platform should provide means to prevent the RE denying installation of an RA from the RadioApp Store.

5.6 Objectives arising from the analysis of the DoC as ToE#3

The following objectives have been identified from the analysis of ToE#3:

- Confidentiality:
  - The RRS platform should prevent an unauthorized third-party from determining that the DoC is being updated.
  - The RRS platform should prevent an unauthorized third-party from determining that the complete DoC is being retrieved from a simplified DoC over the network.
- Integrity:
  - The RRS platform should provide means to prevent modification of the DoC apart from installation and update, in particular at rest.
  - When the DoC is being updated, or the complete DoC is being retrieved, the RRS platform should allow integrity protection of said DoC while it is in-transit between the relevant entities in the network and components on the device.
  - The RRS platform should prevent an unauthorized third-party to delete, install or otherwise alter a DoC on the RE.
  - When there is only a digital DoC and no paper DoC provided with the RE, the RRS platform should provide means towards tamper-resistance of the DoC at rest on the RE.
- Availability:
  - When the complete DoC is requested over the network based on a simplified DoC residing on the RE, the RRS platform should provide means towards the availability of complete DoC to the RE.

- Authenticity:
  - When the DoC is being updated, or the complete DoC is being retrieved, the RRS platform should allow for identification and authentication of relevant entities in the network and components on the device.
  - The RRS platform should allow for authentication of content (DoC) to the relevant component on the device.
  - When there is only a digital DoC and no paper DoC provided with the RE, the system should implement measure to ensure that the digital DoC provides at least the same level of confidence than the DoC in Paper form.
- Accountability:
  - The RRS platform should allow for the traceability of devices that have received an updated DoC.
  - The RRS platform system should provide means to prove reception and installation of a DoC by a device.
  - The RRS platform should allow for binding the DoC to the device that receives it.
  - The RRS platform should allow for verifying that the presented DoC is bound to the device.

6 Stakeholders and assets

6.1 Use cases

6.1.1 Introduction

The general set of use cases for RRS are defined in [i.17]. The extension of those use cases for the purpose of security introduces one critical actor, the adversary. The technical approach of developing use cases with UML identifies a set of actors and are shown diagrammatically in figures 6, 7 and 8 for the RRS case, and examined in text in table 1. Whilst all actors are stakeholders not all stakeholders are actors as some never interact directly with the system, even though they have the right to care how the system behaves.

Table 1: Summary of use cases

Actor	Use case	Notes
Developer	Develop radio app	The primary developer of the Radio App.
	Make app available	The developer, once authorized, transfers the app to the app-store in order to allow it be distributed.
Rogue developer	Develop malicious radio app	This actor is a specialization of the developer (shares the same attributes but with a rather different intent).
RE Manufacturer	Endorse App	The RE manufacturer may choose to endorse the app as valid with their hardware.
	Make app available	Similar to the RadioApp Store actor but under the control of the RE manufacturer.
	Install app	This is a special case of the RE manufacturer "pushing" an app to the RE.
DoC responsible party	Prepare DoC for combination of Radio App and RE	From the Directive 2014/53/EU [i.14] it is clear that a single entity is responsible for the DoC addressing the Radio App and RE combination. This actor may be a specialization of the RE manufacturer actor.
	Update DoC	

Actor	Use case	Notes
Regulator	Police DoC	The DoC has to be attached to the device and if checked the regulator (or their agents) have to be able to verify that the DoC exists and to determine that it covers the operational RF modes of the RE.
	Display DoC	The DoC residing on the RE may be complete or simplified.
RadioApp Store	Make app available	The RadioApp Store (repository from which apps can be sourced) is to simply make the app available. In consideration of the regulated environment for which apps are provided the RadioApp Store should ensure apps are only made available from authorized entities and to authorized entities.
Root of Trust	null	The root of trust is the entity/actor that provides the trust for the RRS system. It is modelled as a specialization of a number of other actors as the actual entity/actor that takes this role will be context dependent.

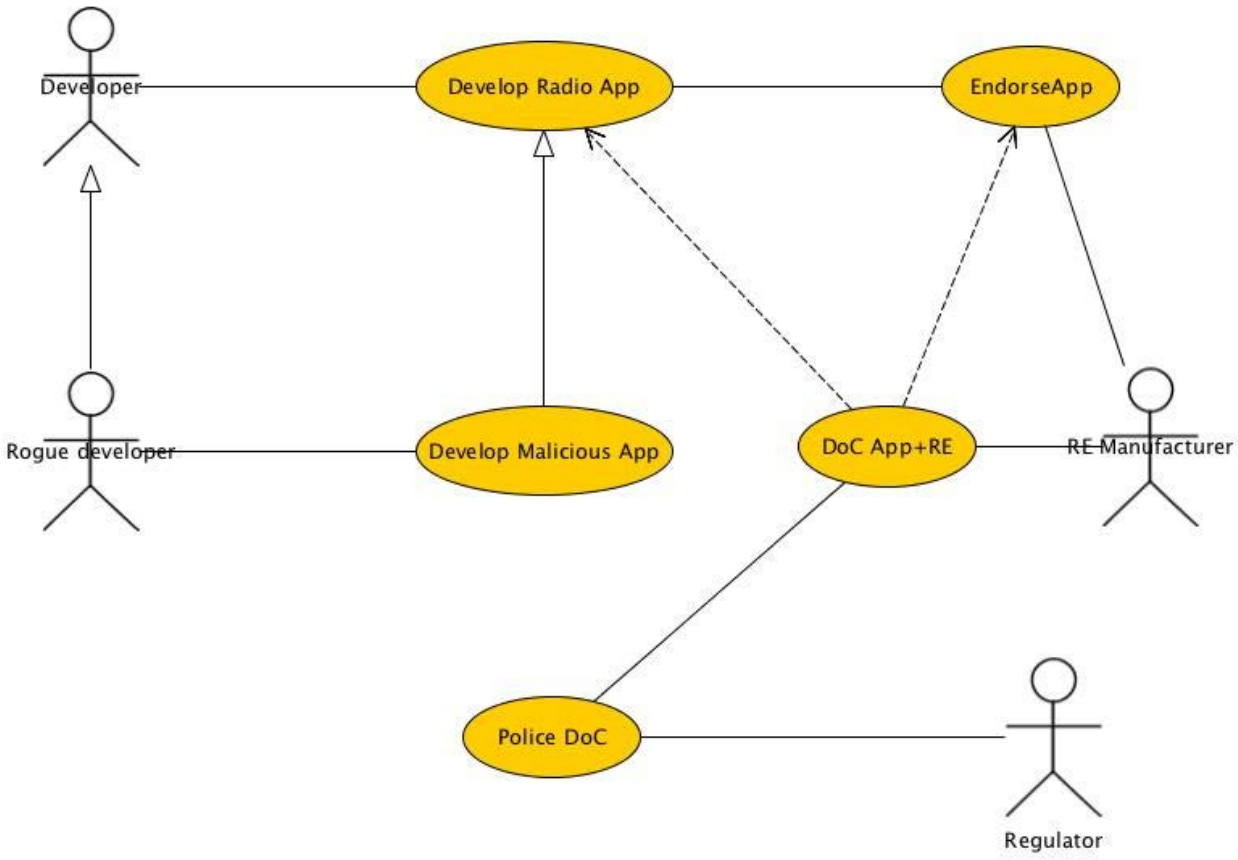

Figure 6: Simplified use case diagram for Radio App development and deployment

The use case diagram can be extended on the assumption that the model of deployment follows that of existing commercial RadioApp Stores by the addition of actors for the RadioApp Store and the communications network operators. However, it is noted that whilst there will be a communications network with associated network roles involved in the distribution of RRS apps and who will support REs that are RRS enabled it is assumed that the packaging of the app and the knowledge that a terminal is an RRS-RE is transparent.

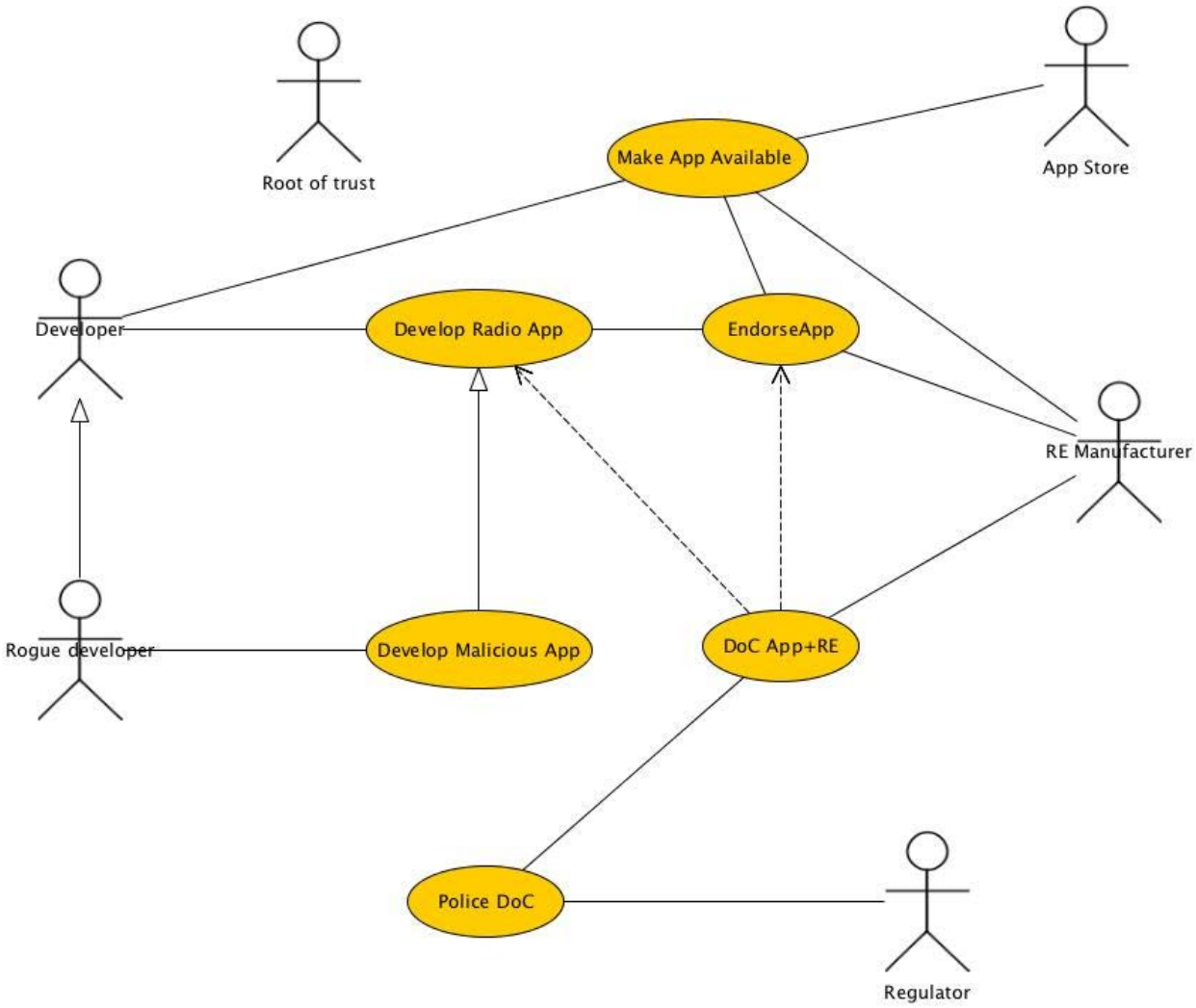

Figure 7: Extended use case interaction diagram

For the last stage of this analysis the use cases are further extended to consider both the RE user and the concept of a root of trust as shown in figure 8.

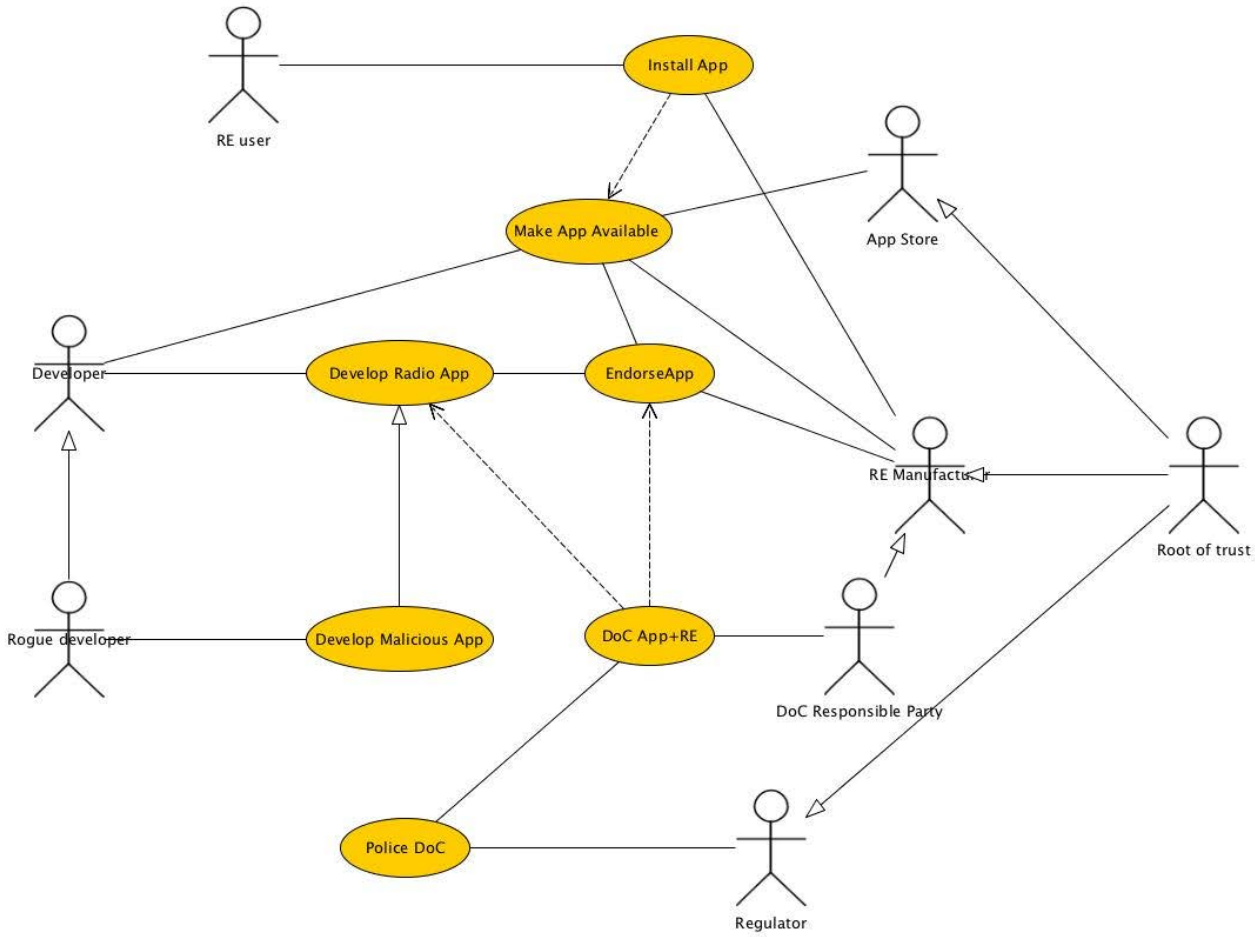

Figure 8: Further extension of use case interactions

6.1.2 Timing dependencies between use cases

In order to comply with the RED [i.14] and in particular to address the core requirement to have a single identifiable point of responsibility the following requirements apply to the ordering of actions (where the use cases represent classes of actions):

- An RA can only be made available if the DoC for the combination of RA and hardware (i.e. the Reconfigurable Equipment) has been made available.

NOTE 1: There is an implied trust relationship if this true, the user of the RA trusts that the installation of the RA will result in a device that complies with the RED through the availability of a valid DoC for the combination.

- In order to prevent malicious RA being made available the RE manufacturer has to formally endorse the RA and this step has to be done before formalizing the DoC for the combination of RE and RA.

NOTE 2: The implied resulting trust model is that the end-user trusts that the RE manufacturer will not allow malicious RA to be endorsed.

NOTE 3: The term "malicious apps" covers both RA and RAP designed with the intend to harm, and otherwise legitimate RA and RAP used in a non-legitimate context (e.g. a user forcing the installation of an RA that is not compatible with the user's RE).

6.2 Assets

6.2.1 Mobile Device Reconfiguration Classes

Using the definition of Mobile Device Reconfiguration Classes (MDRC) introduced in ETSI EN 302 969 [i.11] the asset base is MDRC dependent when considered from a security perspective, i.e. each MDRC presents a different security model to any other MDRC.

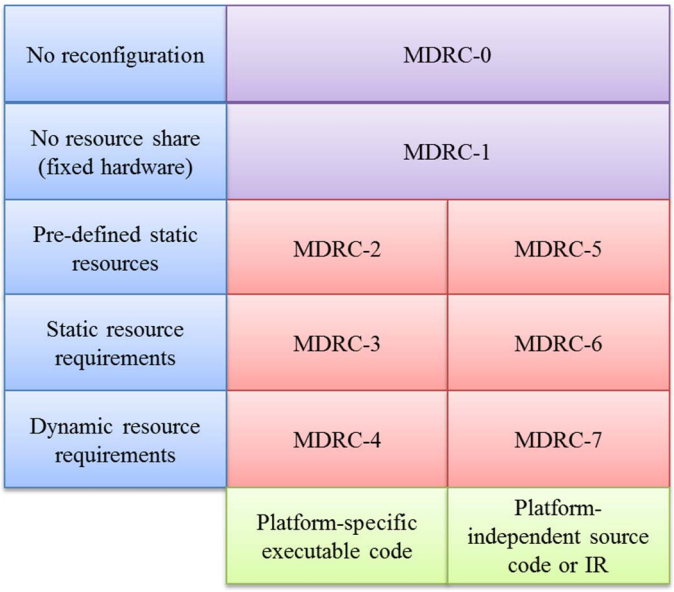

Figure 9: Definition of MDRCs according to reconfiguration capabilities from ETSI EN 302 969 [i.11]

A reconfigurable MD belongs to a defined class according to the reconfiguration capabilities, which are determined by the type of Resource requirements and the form of the Radio Application Package. Reconfigurable MD classes are defined as follows:

- MDRC-0: No MD reconfiguration is possible:
  - In the scope of the present document this has no connectivity to RadioApp Stores or ability to load Radio Apps (more generally Radio Application Packages (RAPs)).
- MDRC-1: Radio Applications use different fixed Resources:
  - No support of RAP within the RRS framework.
- MDRC-2: Radio Applications use pre-defined static Resources, MDRC-3: Radio Applications have static Resource requirements, MDRC-4: Radio Applications have dynamic Resource requirements:
  - As these modes are platform specific they need to be treated slightly differently from MDRC-5/6/7.
- MDRC-5: Radio Applications use pre-defined static Resources, on-device compilation of Software Radio Components, MDRC-6: Radio Applications have static Resource requirements, on-device compilation of Software Radio Components, MDRC-7: Radio Applications have dynamic Resource requirements, on-device compilation of Software Radio Components:
  - These classes have the closest mapping to the virtualized deployment environments for Network Functions Virtualisation (NFV) where the hardware is fully abstracted.

The definition of MDRCs described above can be summarized as shown in table 2.

Table 2: Summary of MDRCs

	Multi-radio system	Resource Share (among Radio Applications)	Resource Manager	Multi-tasking	Resource Measurement	Resource Allocation
MDRC-0	No	No	No	No	Design-time	Design-time
MDRC-1	Yes	No	No	No	Design-time	Design-time
MDRC-2 MDRC-5	Yes	No (note 1)	Yes (note 2)	Yes (note 3)	Design-time	Design-time
					Design-time /Install-time	Design-time /Install-time
MDRC-3 MDRC-6	Yes	Yes	Yes	Yes	Design-time	Run-time
					Design-time /Install-time	
MDRC-4 MDRC-7	Yes	Yes	Yes	Yes	Design-time	Run-time
					Design-time /Install-time	

NOTE 1: Resource share can exist among Radio Access Technologies (RATs) in a given Radio Application.
NOTE 2: This is for a fixed Resource allocation only. Resource management and Resource allocation among RATs (in a single RA) are pre-determined in a static manner by Radio Application provider.
NOTE 3: Multi-tasking in this case is for multiple RATs within a single Radio Application.

For each MDRC a different set of reference points is made visible in the overall model as identified in ETSI EN 303 095 [i.13].

Table 3: Required Components of the Reconfigurable Mobile Device Architecture in function of the Mobile Device Reconfiguration Class from ETSI EN 303 095 [i.13]

Mobile Device Reconfiguration Class	Required CSL Entities	Required RCF Entities	Required Interfaces
MDRC-0	None	None	None
MDRC-1	Administrator, Mobility Policy Manager, Networking Stack, Monitor	Configuration Manager, Radio Connection Manager, Flow Controller	MURI
MDRC-2, MDRC-5	Administrator, Mobility Policy Manager, Networking Stack, Monitor	Configuration Manager, Radio Connection Manager, Multi-Radio Controller, Flow Controller	MURI, URAI, RRFI
MDRC-3, MDRC-6	Administrator, Mobility Policy Manager, Networking Stack, Monitor	Configuration Manager, Radio Connection Manager, Multi-Radio Controller, Flow Controller	MURI, URAI, RRFI
MDRC-4, MDRC-7	Administrator, Mobility Policy Manager, Networking Stack, Monitor	Configuration Manager, Radio Connection Manager, Multi-Radio Controller, Resource Manager, Flow Controller	MURI, URAI, RRFI

The security concerns escalate in proportion (in most cases) to the number of exposed interfaces and assets. Thus MDRC-0 does not raise concerns, whereas MDRC-1 only exposes the Radio Control Framework through the MURI, and all other variants access all of the open interfaces within the RE.

6.2.2 Radio Application operating environment

Figure 10 provides an informative and simplified overview of the components and functions involved in the installation and execution of Radio Applications across the Application Processor and the Radio Computer, as described in ETSI EN 303 095 [i.13]. Depending on the design choices, not all elements may be present. Elements in blue boxes are specific to RRS and those marked with blue circles may be provided as online services prior to the installation phase on the RE.

NOTE 1: When the compiler or the back-end compiler are provided as online services, the RE only sees the compilation result, which is the RAP on the RadioApp Store. The RE does not communicate with the compiler or back-end compiler provided as online services, the RadioApp Store does.

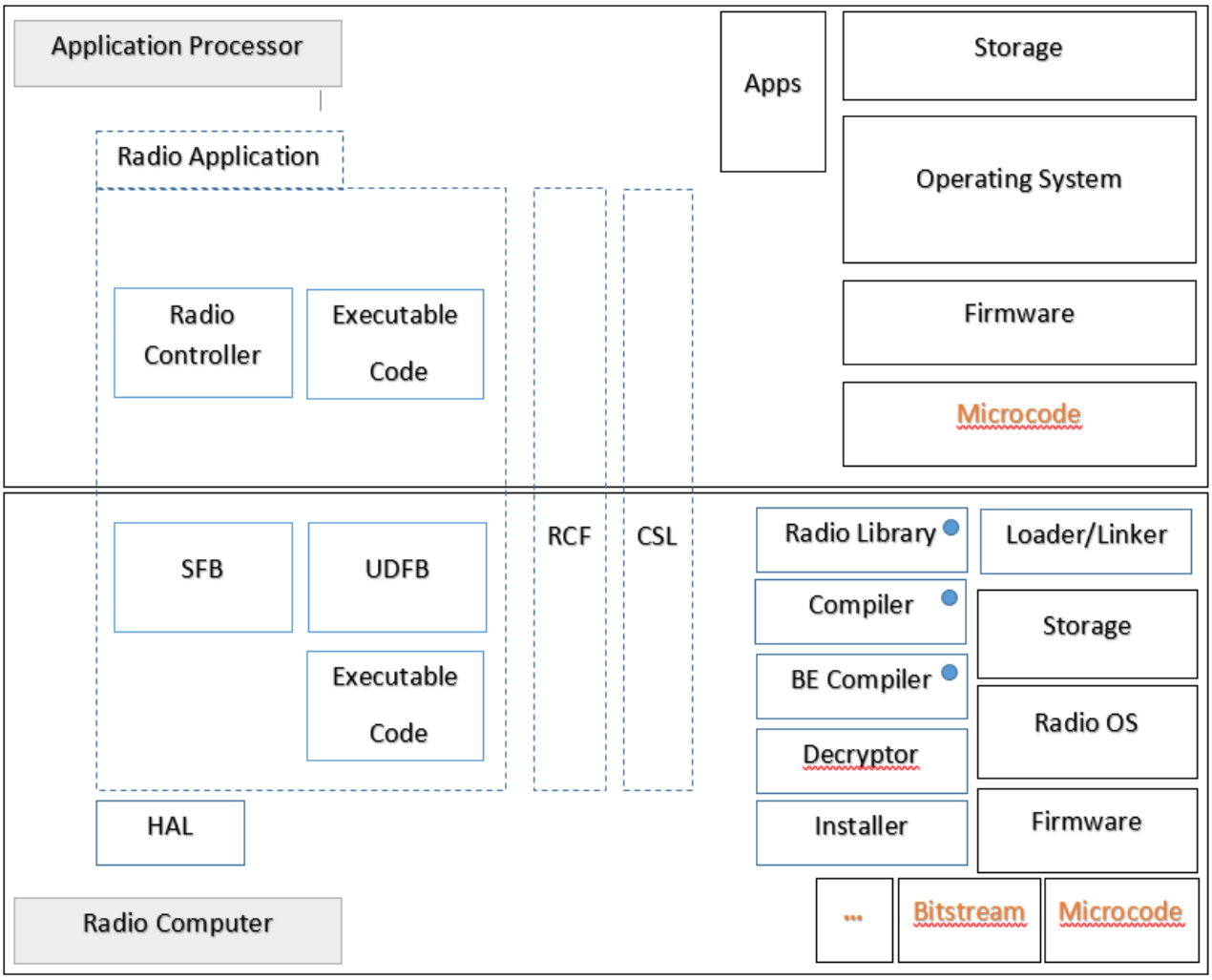

Figure 10: Overview of RRS and operating environment components over the Application Processor and the Radio Computer

As exemplified the Radio Application, the CSL, and the RCF may span the Application Processor and the Radio Computer. In addition, the RE may support different types of URA codes meaning that some URA may run directly on the Radio OS as executable codes while others may run as an RVM configured by configcodes (this possibility is not illustrated).

NOTE 2: The RVM is not a virtual execution environment, but rather an abstract machine that is configured by configcodes into an RA.

NOTE 3: The Radio Application interfaces with the Radio Platform via the RRFI [i.19] and with the RCF via the URAI [i.20].

Table 4 provides an overview of the possible locations of the compilers and the Radio Library, depending on the MDRC and design choice. The blue dots illustrate the situation where everything is compiled online, while the black dots illustrate the situation where UDFBs are compiled on the RE. As the design choice moves towards platform-independent source code/IR MDRC and dynamic linking, the number of components related to security critical processes on the RE (installation, runtime) increases.

Table 4: Compilers and Radio Library locations

	MDRC-2, MDRC-3, MDRC-4			MDRC-5, MDRC-6, MDRC-7		
Component\Phase	**Design**	**Install**	**Runtime**	**Design**	**Install**	**Runtime**
Compiler	•					
Platform-independent source code, static						
Compiler				•	•	
Radio Library				•	•	
Platform-independent source code, dynamic						
Compiler				•	•	
Radio Library				•		••
Intermediate Representation, static						
Front-End Compiler				••		
Back-End Compiler				•	•	
Radio Library				•	•	
Intermediate Representation, dynamic						
Front-End Compiler				••		
Back-End Compiler				•	•	
Radio Library				•	•	••

6.2.3 Radio Application and Radio Application Package

The RAP is the delivery unit of RA from the RadioApp Store to the RE. According to ETSI EN 303 095 [i.13], the RAP consists of:

- The RA which contains RA codes made of UDFBs, SFBs, RC codes and executable codes depending on the RA design choice.
- Configuration metadata for the RE, including:
  - The RPI which is a descriptive interface detailing how the RA is structured and its sub-components synchronized together.
  - Bindings to the HAL, when applicable.
  - Bindings to linkable libraries, when applicable.
  - Pipeline configuration.

6.2.4 Declaration of Conformity and CE marking

In the regulatory framework of the European Union, the Declaration of Conformity is a document provided with the RE in which the manufacturer declares that it has assessed compliance with all the Union Acts governing the RE. The CE marking is a simple label indicating compliance and, when applicable, the identity of the notification body.

In its digital form the DoC content can be displayed but its semantic remains opaque to the RE. However, the DoC may be complemented by an RE Configuration Policy for the RE to determine compliance of a hardware and software combination.

6.2.5 External assets

The following attributes are identified that may be manipulated by the RA through the RRS platform:

1) *Frequency band:* Frequency band or sub-band within which the device is authorized to operate and to perform the intended function of the equipment. In this context, the frequency band represents a resource, which can be used by one or more radio communication services.

2) *Radio communication service:* Radio service authorized for operation on a given frequency band with a regulatory priority.

3) *Network node:* It represents a hardware or software component of the network, which provides a specific service.

4) *RRS device:* It represents a mobile device which is implemented by means of RRS technologies and concepts.

5) *User's data:* It represents the data of a user.

NOTE: The assumption here is that the end-user (i.e. the user of the RE), when offered control over the RA configuration of the RE, has to be identifiable to the RadioApp Store sufficiently to complete the transaction. This may require commercial data (e.g. banking information if the RadioApp Store is a commercial entity).

6) *Network data:* It represents the data needed for the proper functioning of the network.

6.3 Cardinalities

Figure 11 summarizes the assumptions with regard to stakeholder and asset cardinalities in an RRS deployment.

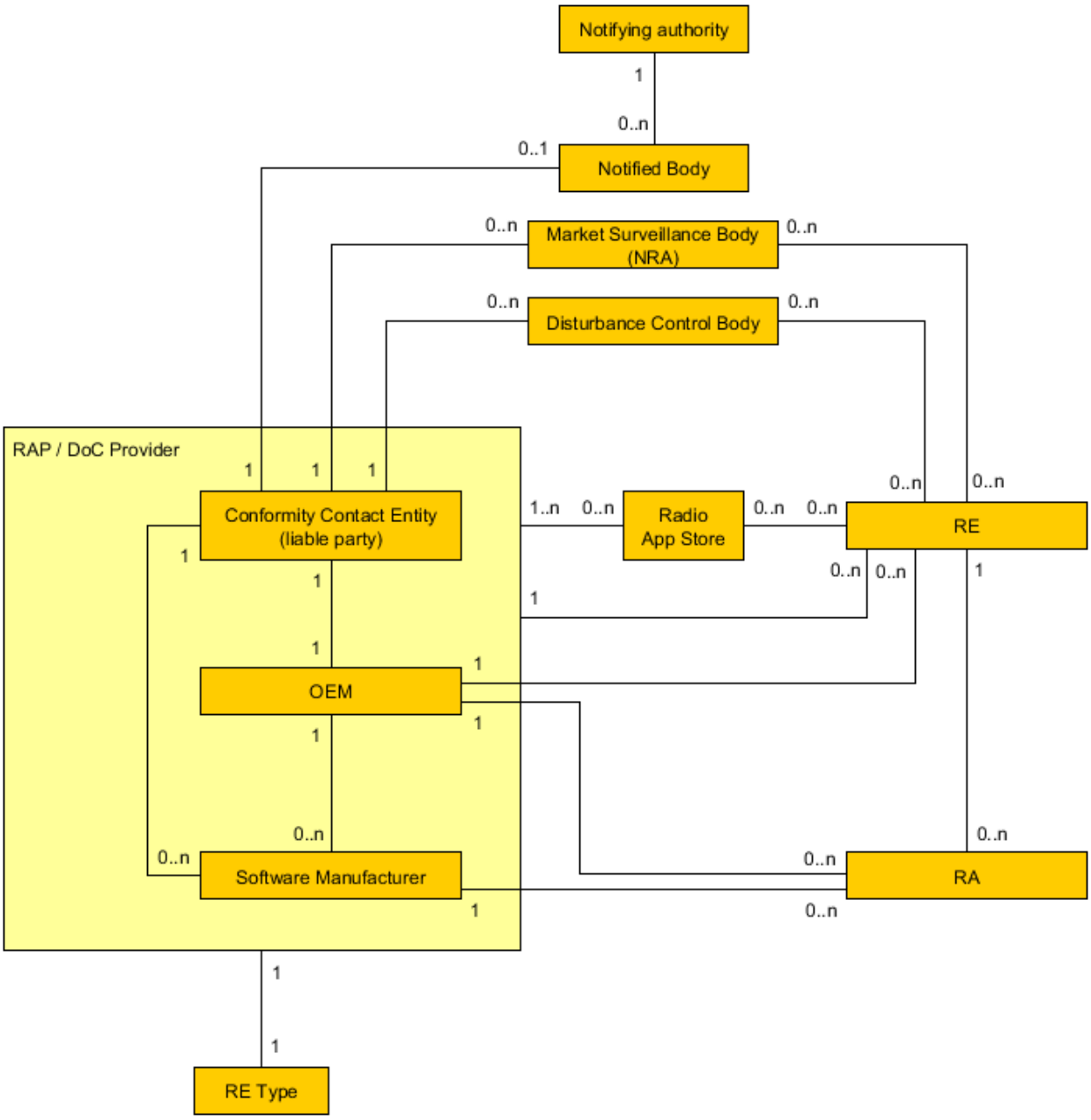

Figure 11: Cardinalities of stakeholders and assets in a hypothetical RRS deployment

These assumptions are laid as follows:

- For each RE type (product type), there is a composite RAP/DoC Provider entity which is an aggregate of the Conformity Contact Entity, the Original Equipment Manufacturer, and the Software Manufacturer.
- Within the RAP/DoC Provider, one Conformity Contact Entity takes compliance responsibility for one Original Equipment Manufacturer in relation with zero or more Software Manufacturer.
- The Original Equipment Manufacturer collaborates with zero or more Software Manufacturer for RA development, testing, and certification.
- One Software Manufacturer may develop zero or more RA.
- The Original Equipment Manufacturer may control zero or more RE, and one RE is controlled by one Original Equipment Manufacturer.
- The Original Equipment Manufacturer may test zero or more RA.
- One RE may execute zero or more RA.

NOTE: The RE user is currently not included as it is assumed they have no direct authority over the management of RA on the RE, but may be offered limited control via out-of-band means.

Regarding distribution and installation:

- Zero or more RadioApp Store may distribute RAP and DoC from one RAP/DoC Provider.
- A RadioApp Store may operate for more than one RAP/DoC Provider.
- Zero or more RE may connect to zero or more RadioApp Store.
- However, any RE is bound to one DoC Provider and one RAP provider.

Regarding market control:

- Any number of Market Surveillance and/or Disturbance Control Bodies may assess or track any number of RE.
- As a result, one Conformity Contact Entity may be contacted by zero or more Market Surveillance and/or Disturbance Control bodies.
- Within the RED [i.14], one Notifying Authority notifies zero or more Notified Bodies.
- For assessment of conformance the Conformity Contact Entity may interact with zero or one Notified Body depending on the assessment Module in use (in the context of one RE type).

7 Identification of ToE for RRS App deployment

7.1 Overview

Within RRS architecture the following stages in deployment (lifecycle) are considered and the primary assets they require in the RRS context to enable that lifecycle state are:

- Development:
  - Compilers, shadow radio platform.
- Distribution and storage:
  - Application Store and any included logical element.

- Runtime, storage:
  - Reconfigurable Equipment and its logical elements.
- Transport:
  - Network.

The Application store and the composition of the Reconfigurable Equipment architecture are defined in ETSI EN 303 095 [i.13]. For the purpose of illustrating communications between the RE and the RadioApp Store across the Network, a "Communication End-Point" element is added to both. This is a virtualized element that is modelled as a role of any other element defined for the RE.

The Network is composed of the access networks of the RadioApp Store (such as a datacentre network), of the RE (such as 3GPP-based or Wi-Fi networks), and of any in-between private or public network. The considered architecture for communication across the network is shown in simplified form in figure 12. The distribution network may include physical means such as distribution through a USB device or a direct cable connection but from the point of view of the evaluation for the present document the means of instantiating the distribution network is not considered other than to assume it is a hostile environment through which an RA has to pass prior to installation.

Figure 12: Simplified model of radio app distribution

7.2 ToE#1: communication between the RadioApp Store and the RE

7.2.1 Introduction

Following on from the model for security analysis proposed in ETSI TS 102 165-1 [i.9], and exemplified by the statements that a system, modelled as a composition of assets where **assets** in the model may have **weaknesses** that may be attacked by **threats**, and that a **threat** is enacted by a **Threat Agent**, the purpose of the ToE is to define the extent of the model of that system that vulnerabilities will be looked for.

In identifying the ToE and the various threats to it the identification of core weaknesses is key. Whilst some weaknesses will lead to system vulnerabilities the common approach in security design is to eradicate them either by redesign or by adding assets to the system to reduce the likelihood of any vulnerability being exploited. The identifiable weaknesses of RRS that can be exploited are considered below:

- RRS allows for deliberate manipulation of the device operation in the radio transmission/reception domain.

NOTE: This weakness is of itself non-negotiable - it is a fundamental design goal of RRS.

- The network path between the RadioApp Store and the Reconfigurable Equipment is comprised of at least one radio interface which broadcasts and is thus visible to any adversary.
- The communication service is provided by a "communication end-point" which is comprised of hardware and software, the latter potentially relying on an Operating System (providing e.g. a network stack).

The distribution network is assumed to be initially uncontrolled and without any means of protection an eavesdropper on the distribution path is able to access the content of a document, to modify the content of a document and to masquerade as the owner of a document. Without detailed knowledge of the exchange protocol assessment of the risk is difficult to assess with accuracy although the models from existing RadioApp Stores from commercial providers and software update providers suggest that the risk is considerable and requires to be countered.

7.2.2 Threats

ETSI TS 102 165-1 [i.9] identifies a number of threat trees and these may be extended but the core model is shown in figure 13.

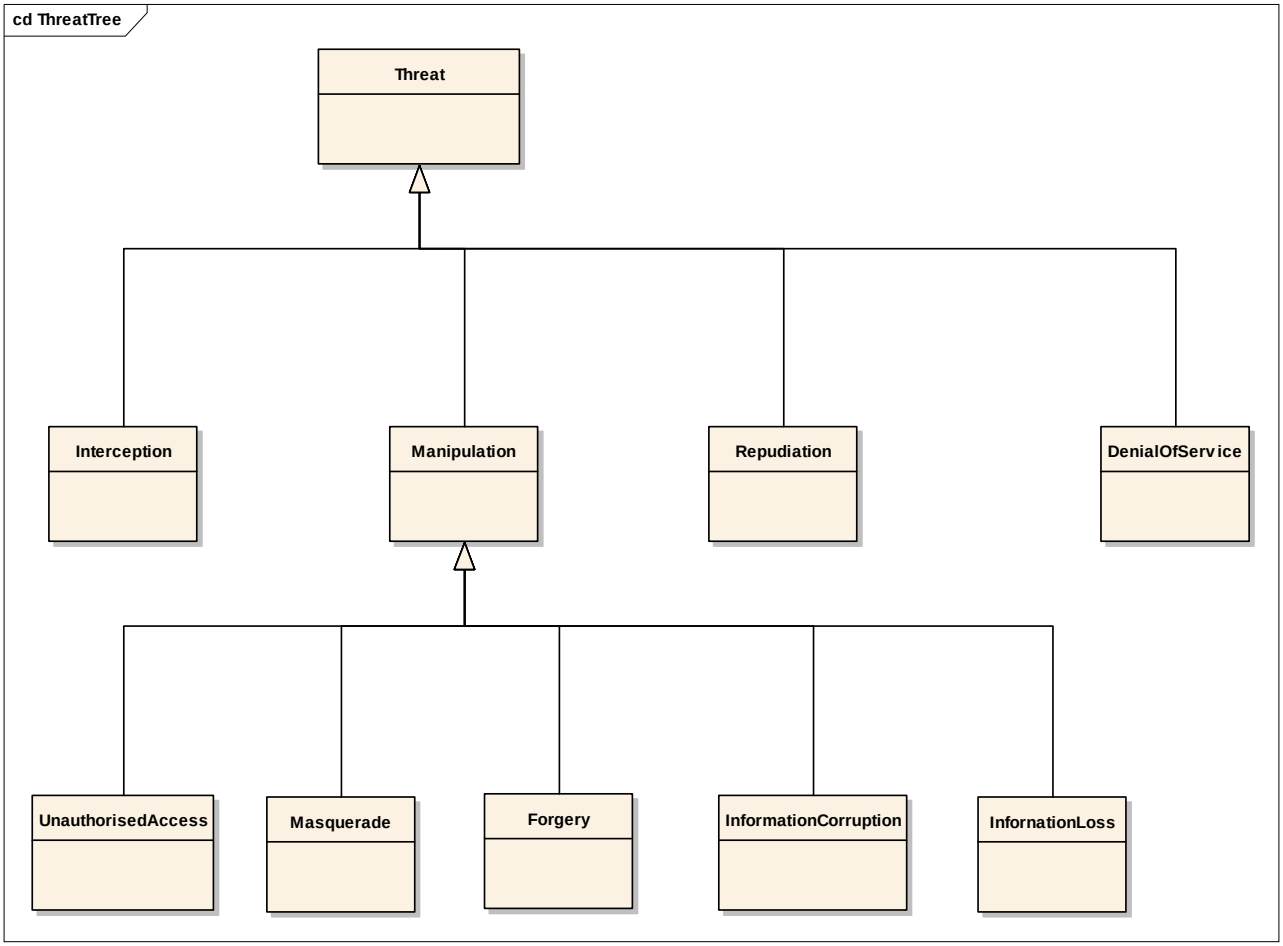

Figure 13: Threat tree (from ETSI TS 102 165-1 [i.9])

Following on from the simplified threat tree it is reasonable to identify a simplified mapping of objective classes to threat types as shown in table 5. Note that is also common to pair threats to an objective in tuples with countermeasures such as {*confidentiality*, *encryption*}.

Table 5: Threats to security objective types (from ETSI TS 102 165-1 [i.9])

Threat	Objective type				
	Confidentiality	Integrity	Availability	Authenticity	Accountability
Interception (eavesdropping)	X				
Unauthorized access	X	X		X	X
Masquerade	X	X		X	X
Forgery		X	X	X	X
Loss or corruption of information		X	X		
Repudiation		X		X	X
Denial of service			X		

Expanding the conceptual model presented in table 5 the following (see table 6) can be stated as threats to each of the classes of objective for RRS.

Table 6: Mapping of objectives for RRS

Objective class	Threat class	Notes
confidentiality	eavesdropping	Information about RAs distributed to devices (identifier, version, etc.), their status on devices (installed, activated, etc.), as well as other signalling information from the RE and the RadioApp Store is being observed. Such information, once gathered, could be used to build further attacks
	traffic analysis	Changes in traffic pattern may allow to infer ongoing activities (such as ongoing installation)
	interaction	Interacting with a RE or RadioApp Store may allow to gather data (e.g. obtain the list of installed RAs on the RE)
integrity	data modification	RAP or signalling data is modified, truncated or deleted
	spoofing	Signalling or other data (such as pushing a RAP to the RE) is injected
	compromise	A software element is compromised
availability		Exhaustion or unavailability of resources on the hosts or in the network (includes radio)
		Interferences in and to the radio environment
		Deactivation of an RA on the Reconfigurable Equipment, or of the RadioApp Store
authentication/identity	identity or credential forgery, theft	
	access control bypass	

7.2.3 Risk assessment

The assessment of risk follows the method described in ETSI TS 102 165-1 [i.9] and applies a number of metrics to assess the likelihood of an attack along any particular vector. The metrics are the following and described in detail in ETSI TS 102 165-1 [i.9]:

- Time.
- Expertise.
- Knowledge.
- Opportunity.
- Equipment.
- Asset Impact.
- Intensity.

7.3 ToE#2: Radio Application Package

7.3.1 Introduction

This ToE deals with the lifecycle of RAP throughout the system, from the development phase and storage on the RadioApp Store, to distribution towards the RE, installation, runtime (instantiation, activation and reverse operations) and finally de-installation from the RE. Impact to the radio environment are part of this ToE.

7.3.2 Lifecycle starting from the availability on the RadioApp Store

In a first approach, the Radio Market Platform is envisioned as a controlled market, where there exist two important control points:

- The RE, which decides whether or not to install an RA based on information provided by trusted sources in the network.

- The RadioApp Store, which decides which RAP are available for installation in the first place.

NOTE 1: These controls points are designed to keep honest actors honest and assume that there is a trust relationship between the manufacturer and the RE (i.e. that the RE manufacturer has put controls in place for the RE to reliably decide based on the provided information).

Although the Administrator in the CSL is the entry point for installation of RA on the RE, it is assumed that the RadioApp Store is a mandatory intermediary between the RE and the RAP provider, i.e. that there is no possibility for a RA provider to bypass the RadioApp Store and directly install a RA on the RE.

The distribution phase is separated from the installation phase because the trust relationships will likely differ for each phase (e.g. the RadioApp Store will be trusted for distribution, but the RAP provider will be trusted for installation).

The UML state diagram below provides a simplified and exemplary lifecycle for the Radio Application and Radio Application Package from the point of view of the RE. As illustrated, one state is located in the Radio Application Store (doted lines), one state is located in one of the Application Processor or Radio Computer (plain lines), while the three other states may be located on both (grey background).

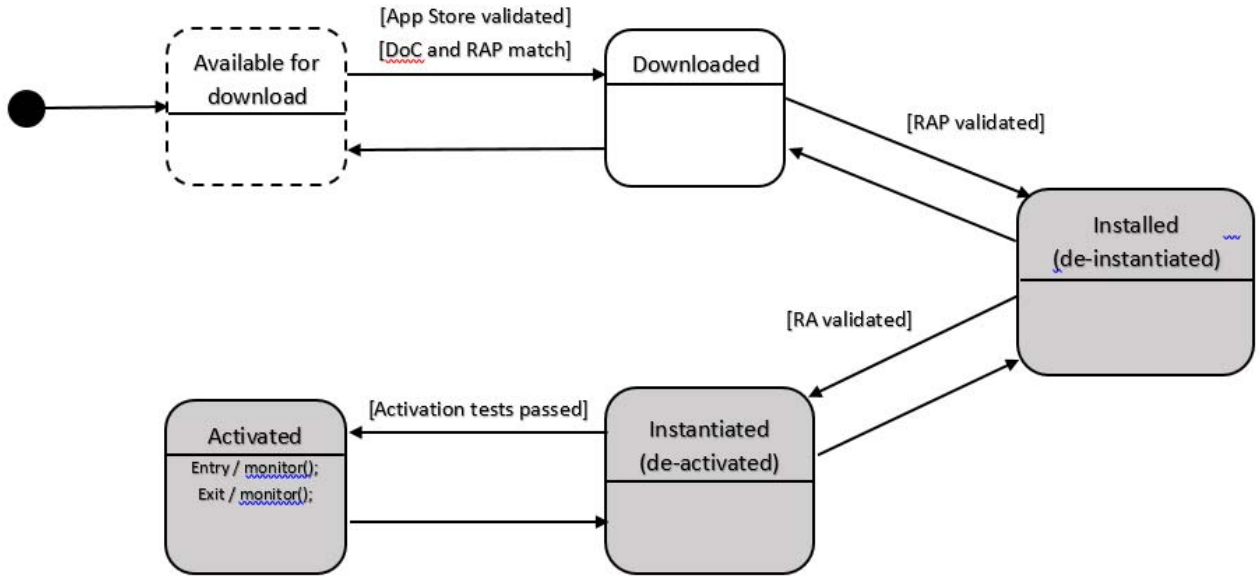

Figure 14: Simplified lifecycle for RA and RAP

A short an exemplary description of the security-related guard conditions and actions is provided below.

[RadioApp Store validated]

The Reconfigurable Equipment has successfully identified and authenticated the RadioApp Store, determined its legitimacy to distribute RAP to the RE via an authorization mechanism, and established a secure communication channel with the store. There may be a plurality of stores available to the device.

NOTE 2: The RadioApp Store may also wish to identify and authenticate for access control purposes. For example, a manufacturer (or the liable third-party) may only accept connections from RE under its responsibility, and the list of available RA may be tailored according to the device model.

Once this guard condition is met, one could expect the next step to be a determination step, in which it is identified that one or more RAP are available for the RE to download and it is decided that a non-empty set is to be installed.

[DoC and RAP match]

The Reconfigurable Equipment has obtained RAP metadata and an up-to-date DoC and RE Configuration Policy, and determined via parsing the RE Configuration Policy that the DoC applies to the RAP, i.e. that there is reasonable certainty that compliance to regulatory requirements will be maintained when instantiating the related Radio Application on the RE.

NOTE 3: This guard condition was placed before the "downloaded" state for optimization purpose. This implies that the RE trusts the RadioApp Store to provide such metadata in order to optimize the download procedure. However, the RAP metadata itself would have to be verified for compliance prior to installation.

[RAP validated]

The Reconfigurable Equipment has successfully identified and authenticated the originator of the RAP and/or the entity that has authority to install the RAP on the RE, and has determined that:

- the RAP is indeed the one that is intended to be installed and is unaltered;
- the RAP matches the RE capabilities;
- the RAP is effectively covered by the DoC relevant to the RE.

NOTE 4: In order to maintain compliance to the RED the RE does not install the RAP if any of these conditions as not been validated.

[RA validated]

The Reconfigurable Equipment has verified, for example via cryptographic means, that the integrity of the Radio Application that is about to be instantiated as well as the configuration metadata has not been compromised since installation.

[Activation tests passed]

Before the Radio Application is activated its status is checked, for example against the known expected state in which it should be.

monitor()

This is an exemplary action in which key properties of the Radio Application are measured while it is active for the purpose of detecting and reacting to improper behaviour. Example include, but are not limited to, detection of memory corruption, system call whitelisting, and control-flow integrity.

NOTE 5: Mitigations related to the instantiated and activated states are vendor-specific and not in the scope of the present document.

7.3.3 Other aspects of the lifecycle

7.3.3.1 Withdrawal of a Radio Application from the Radio Market Platform

There are cases where a Radio Application may be withdrawn from the Radio Market Platform, for example when a more recent version is available, or when it is determined that the Radio Application is not suitable for use. This may lead to the RE being instructed to uninstall and delete the Radio Application from storage.

7.3.3.2 Development and pre-distribution phase

Prior to an RA being distributed, it has to be developed and tested, in particular for compliance with the regulatory framework in which it will operate. This involves a number of actors and interactions which are detailed in clause 6.1. Annex H provides information on security challenges related to the design phase.

7.3.3.3 RE and RA lifetime

It is expected that RE will have a very long lifetimes (decades).

7.3.3.4 Identification of rogue or compromised Radio Applications

In relation to market surveillance activities and response to security events, another aspect of the lifecycle is the ability to conduct RE and installed RA inventories.

7.3.4 ToE#2 environment

As detailed in clauses 6.2.2 and 6.2.3 of the present document the RAP can be installed over several architectural components on the RE and its metadata can influence software and hardware configuration. In addition, the Radio Applications operate on the hardware and software resources provided by the RE and access the radio spectrum and network elements.

Therefore, the RA and RAP can be used as attack vectors against the RE, the radio spectrum, and the network.

7.3.5 Out-of-scope aspects of ToE#2

The Radio Market Platform is currently considered to be a controlled market.

It is assumed that RRS devices are permanently managed.

Although remote control features are identified as an essential aspect of RRS security, they are not detailed in the present document.

7.3.6 Threats

Based on the analysis of the RAP ToE the following threats have been identified to the classes of objectives for RRS.

Table 7: Threats to security objectives for RAP

Objective class	Threat class	Notes
confidentiality	not applicable	There is no confidentiality requirement beyond ComSec (RAP confidentiality is currently assumed not to be in the scope of RRS).
integrity	data modification	The RAP could be deleted, modified or replaced at rest on the RadioApp Store or on the device; It could also be deleted, modified or replaced at runtime on the device.
availability		None. For the distribution phase see threats described in ToE#1.
authentication/identity	masquerading	A third-party pretends to be the RAP originator.
	illegitimate copy	A RAP legitimately installed on a given RE is being copied to and installed on an RE that should not host it.
accountability	repudiation	A compromised RE denies installation of a given RAP; A compromised RadioApp Store denies distribution of a given (potentially malicious) RAP.
	traffic interception	A confirmation message (installation, deletion, update) is intercepted and not relayed to the final recipient.

7.4 ToE#3: Declaration of Conformity and CE marking

7.4.1 DoC characteristics

As detailed in clauses 6.1.1 and 6.2.4 of the present document, the DoC is critical in asserting the compliance of a device to the Union Acts of the EU. A RAP cannot be made available on the RadioApp Store if the corresponding DoC is not available. Details of DoC usage from a market surveillance perspective are provided in clause 7.4.3.

The characteristics of the DoC are summarized below.

DoC Form

- in paper form along with the RE;
- in digital form within the RE memory, either:
  - complete; or
  - simplified, with a pointer to the complete DoC (*internet address* in RED [i.14] terms).

NOTE 1: The term *internet address* hints that the retrieval method does not necessarily have to be via a WEB URL, although this will likely be the case (another protocol could be used).

Format

- there is neither a specific data format nor a specific presentation format to comply to for the digital representation of the DoC.

Aggregation

- there is one DoC for all compliance matters in the EU regulatory framework (i.e. radio, consumer electronics, material used in the product);
- the DoC may have, and usually has, annexes.

Availability

- the DoC is expected to be available with the product. It has become common for devices to display a DoC on screen via a menu option;
- the DoC can be available at several different locations for any given product (with the product itself, from the OEM, and from several economic and regulatory actors);
- the DoC could be requested from the RE via a remote query mechanism;
- there is only one DoC per device type.

Classification

- the portion of the DoC that is present on the RE is a fully public document.

NOTE 2: Technical annexes of the DoC can contain confidential information and usually remain with the manufacturer.

Lifecycle

- the DoC is not a static document and is bound to a specific set of hardware and software combinations (this is not incremental versioning). This is regardless of the RE manufacturer bounding the DoC to software available in the future;
- the DoC may be updated on the RE (as part of errata or reconfiguration that would justify a modification of the existing DoC), reasons to update the DoC include:
  - new software version covered by the DoC;
  - change in the scope of the DoC when a RA is installed or removed;
  - changes external to reconfiguration, such as the availability of new Harmonised Standards;
- the availability requirement of the DoC within the RED is 10 years.

The characteristics of the CE marking are as follow:

- The CE marking is normally affixed on the device plate or device package; the purpose of a physical marking is to provide some form of resistance to tampering (there is a strong expectation for this property).

- The CE marking may be provided on the device display along the DoC. For the purpose of the present report this is interpreted as "the CE marking is part of the DoC data".

7.4.2 Consequences drawn from characteristics

Consequence #1: the DoC is already aggregated prior to distribution to the RE.

Because the DoC data and representation formats are left open, it is assumed that aggregation into the DoC of various statement of compliance to Union Acts happens before the DoC is published and as such there is only one asset to protect (as opposed to an aggregate of assets). This also rules out having to manage several sources into a DoC aggregate: from the RE perspective there is only one source.

Consequence #2: the RE comes with an original DoC.

Consequence #3: the DoC in paper form should point to an up-to-date digital version.

It is assumed a DoC is initially provisioned on the RE at manufacture time, and it may be updated following a device reconfiguration. This means that the DoC in paper form, if available, should provide an internet address to its up-to-date digital version.

In case the RE is unable to connect to a network, it may not be possible to resolve the complete DoC from the simplified DoC on the device. Such situation is easily accommodated by providing the operator a short internet address or reference number for retrieval of the complete DoC via other means.

NOTE: The absence of a DoC in digital form make it impossible to implement RA updates.

Consequence #4: there exists a DoC master copy, which is identifiable as such.

Since there can be copies of the DoC among various market actors, it is necessary to identify a master copy. The simplified DoC could point to this master copy, consequently a similar pointer being provided in the complete DoC would solve the master copy problem. It may not be necessary to identify a legal master and legal copies under the RED [i.14].

Consequence #5: the digital CE marking is always part of the DoC.

Consequence #6: DoC delivery to the RE is a critical process.

Considering that the DoC is a public document bound to a device for compliance purpose, it is important to make sure that all operating devices receive an updated copy of the DoC when necessary. It is of lesser importance to know who requested the DoC. As illustrated in the following clause it is essential that measures are taken on the RE to safeguard the integrity of the DoC and CE marking at rest and their availability (as displayable elements on the RE).

7.4.3 DoC usage from a market surveillance perspective

The list below summarizes the point of view of market surveillance available at the time of drafting the present report, regarding device release procedure and the use of the DoC:

- When the manufacturer produces a new device, the conformance assessment is first performed, followed by the issuance of the DoC.
- Only after the DoC is available, can the device be released on the market.
- In case the device changes after having been released on the market, conformance is assessed again and a new DoC issued if necessary (which is almost always the case since the software version will change, see RED [i.14], annex VI).
- The market surveillance authority essentially looks at the final product, as found on the market:
  - in a first step, the authority checks whether the DoC and the device match;
  - in a second step, the authority carries on the assessment and checks for compliance of the device. In case of mismatch or alleged non-compliance, the manufacturer is contacted by the authority, which seeks to determine who holds liability.

- Since the DoC is to be updated each time there is a new software version on the device, it contains its own history which allows for traceability of hardware and software combinations over time, e.g. for disturbance control against past events.

From this summary it should be clear that the portion of the DoC that is present on the RE is essential for the Market Surveillance Body to retrieve the elements of the DoC staying at the manufacturer.

7.4.4 ToE#3 environment

The DoC is to be stored on the RE and parsed for display or interpretation. It can therefore be used as an attack vector against the RE.

7.4.5 Out-of-scope aspects of ToE#3

Remote attestation of the DoC on the RE is not in the scope of the present document.

7.4.6 Threats

Based on the analysis of the DoC ToE the following threats have been identified to the classes of objectives for RRS.

Table 8: threats to security objectives for DoC

Objective class	Threat class	Notes
confidentiality	not applicable	The part of the DoC that is present on the RE is a public document.
integrity	data modification	The DoC could be deleted, modified or replaced at rest on the RadioApp Store or on the device. It could also be deleted, modified or replaced at runtime on the device.
	spoofing	The DoC could be modified prior to display on the device.
availability		For the retrieval of the complete DoC see threats relative to ToE#1.
authentication/identity	masquerading	A third-party pretends to be the DoC originator.
	illegitimate copy	An otherwise valid DoC could be copied from one device to another device (possibly of another type or counterfeit).
accountability	repudiation	A compromised device denies having the expected version of a DoC, or pretends to have another one.
	traffic interception	A confirmation message (update) is intercepted and not relayed to the final recipient.

7.5 Conceptual countermeasure framework for RRS to address ToE#1, ToE#2 and ToE#3

7.5.1 Introduction

There are in general 2 means to counter threats, the first being system redesign to eradicate underlying weaknesses, the second (chosen here) is to add features to the system in order to minimize the likelihood of a successful attack.

NOTE: The impact is not affected in general by the presence of countermeasures, rather the likelihood of an attacker to implement an attack is minimized.

7.5.2 Framework elements

The primary objectives, the ToEs, and the assessment of risk give rise to the following key elements of the framework:

- Identity management framework:
  - Required to allow for proper identification and authorization of entities.

NOTE 1: Identity does not imply of human agents but is intended to address proper identification of the class of RE, and other elements in the RRS framework (the app-store, the authorities, the RE manufacturer, etc.).

- Non-repudiation framework.

NOTE 2: The presence of rogue apps on a device should be accountable, thus evidence should be gathered across the system to ensure that the installation and or removal of any app should not be deniable.

- Package integrity verification framework (runtime and at installation).

7.5.3 Revised risk calculations

7.5.3.1 Application of identity management framework

7.5.3.1.0 Introduction

The purpose of the identity management framework is to substantially reduce the risk arising from unknown and unauthorized entities in the RRS framework. The effect is to reduce all attacks realized to "low" by lowering the likelihood of a successful attack.

NOTE: The identity management framework itself adds substantially to the number of entities in the RRS framework and may provide additional vectors of attack unless appropriate levels of care are taken in implementation, particularly of any cryptographically significant material.

7.5.3.1.1 Identities in RRS

7.5.3.1.1.1 Implicit endorsement model

The class diagram below details the hierarchy of identities required to operate an RRS platform in the implicit endorsement model. In this proposed model RAP (resp. RE) are implicitly scoped by (resp. bound to) the RAP/DoC Provider and are not necessarily globally identified.

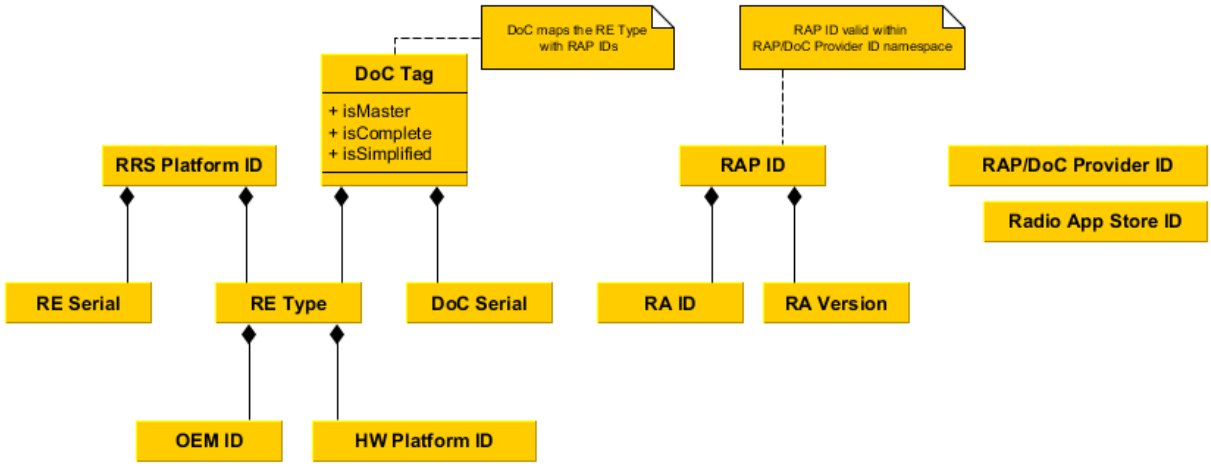

Figure 15: RRS identities in the implicit endorsement model

The essentials identities are defined as follows:

OEM ID: identifies the OEM from which the RE originates from. The OEM ID may be opaque data at the level of the RRS Platform but not at the level of device firmware management.

HW Platform ID: identifies the hardware platform and related capabilities of the RE. The separation of the OEM ID and HW Platform ID take into account the possibility that several OEM may build on the same hardware platform (eventually with variants).

RE Type: being composed of the OEM ID and the HW Platform ID, the RE Type uniquely identifies the capabilities of the RE.

RE Serial: a serial number uniquely identifying a device within the RE Type.

RRS Platform ID: identifies the set of hardware and software components on the RE that provide RRS-related functionalities. It is composed of the RE Type and the RE Serial. Thus the RRS Platform ID uniquely identifies an RE and provides information on the RE capabilities. It can therefore be used by the RadioApp Store as a reference identifier when providing DoC and RAP to the RE. Note that the RRS Platform ID cannot reasonably be a device identifier scoped by the Radio Access Technology, such as a MAC address or an IMEI, because the set of RA installed on an RE may change over time.

DoC Serial: a serial number uniquely identifying a DoC relative to the RE Type is applies to.

DoC Tag: being composed of the DoC Serial and RE Type, uniquely identifies a Declaration of Conformity as applicable to the RE. The DoC Tag is stored in the RE Configuration Policy and has attributes indicating whether the DoC is the master copy, a complete copy or a copy in a simplified version. In addition, the RE Configuration Policy of the DoC binds the DoC Tag to the list of applicable RAP ID (that is, applicable RA and their versions). The DoC Tag is not an identifier but a reference: it merely binds the DoC to the RE Type it applies to. As such, there is neither a need to register and manage the DoC Tag as an identity, nor to include it in the visible fields of the DoC.

NOTE: This means that the DoC Tag does not need to be included in the requirements set in the RED [i.14] regarding information that is to be provided in the DoC.

RA ID: uniquely identifies a given Radio Application in the context of the RAP/DoC Provider.

RAP ID: uniquely identifies a given Radio Application and its version.

RAP/DoC Provider ID: uniquely identifies the RAP/Doc Provider ID for market surveillance and disturbance control purposes (hence this ID should be globally unique), however it may be opaque data to the RE as the RE is implicitly bound to the RAP/DoC Provider. The RAP/Doc Provider ID may be a URN. In this model the RAP/DoC Provider is trusted by the RE for both the endorsement of the DoC and RAP.

RadioApp Store ID: identifies the RadioApp Store the RE should connect to. The RadioApp Store ID may be a URL.

7.5.3.1.1.2 Explicit endorsement model

In the proposed explicit endorsement model, more flexibility is given in the management of stakeholders from the RE perspective. In particular, the Software Provider is directly visible to the RE, which will locally validate the Software Provider certificate. This allows the OEM to revoke a Software Provider in a more efficient way than with the previous model. In a similar fashion, a change in the Conformity Contact Entity can easily be enforced while the OEM remains in control of the RE. This requires additional identities to be defined. The class diagram below details the hierarchy of identities required to operate an RRS platform in the Explicit endorsement model.

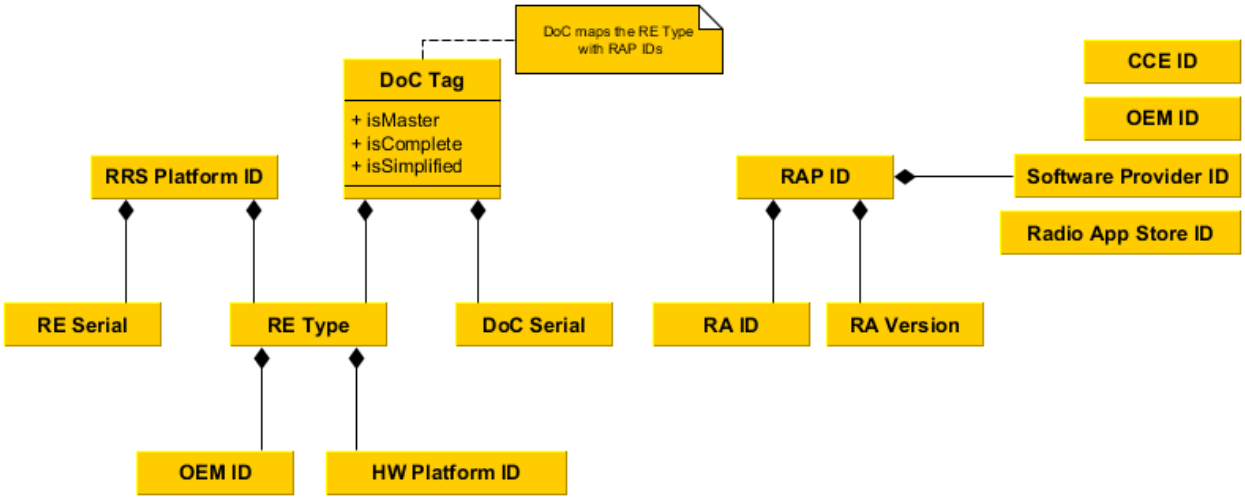

Figure 16: RRS identities in the explicit endorsement model

While other identities of the implicit endorsement model remain relevant, the RAP/DoC Provider ID is replaced by three identities:

CCE ID: identifies the Conformity Contact Entity which the RE trust for endorsement of the DoC. The CCE may also endorse RAP. The CCE ID may be a URN.

Software Provider ID: identifies the provider of an RA. The Software Provider ID may be a URN.

OEM ID: identifies the OEM for the purpose of RA endorsement.

These three identifiers should be globally unique. In this model the RAP ID is composed of the RA ID, the RA Version, and the Software Provider ID. Therefore it is also globally unique.

NOTE: It is envisioned that the identifiers for the CCE, OEM, Software Provider, RAP/DoC Provider, and RadioApp Store can be mapped to identities - or build on processes - that already exist on the market. The RAP ID is dependent on the RadioApp Store model.

7.5.3.1.1.3 Advantages of using a DoC Tag

After the DoC signature validation step in the Administrator Security Functions, the applicability of the DoC to the RE is verified in the certification step performed in the Configuration Manager. The DoC Tag greatly simplifies this process since the information would be readily available in the RE Configuration Policy and issued by a trusted source. In particular, devices of different RE Type could share the same trust anchor and intermediate certificates for validating signatures from the CCE.

If the DoC Tag cannot be included in the RE Configuration Policy, then another means is necessary to ensure that a given DoC does apply to the RE. This is because the RadioApp Store is only trusted for distribution of assets and not for their assignment and endorsement. Without the DoC Tag, if the Radio Application Store is compromised the attacker could present the RE with a DoC that is valid for another RE Type. In order to prevent this, the DoC signature step should take the RE Type into account which means that the PKI will be more complex (dedicated intermediate certificates will be required for each RE Type). In addition, management of DoC and RE Types in the manufacturer's inventory will be more complex because the association between the DoC and RE Types will be implicit instead of being explicit.

Table 9 summarizes the advantages and disadvantages in both cases.

Table 9: Effects of the presence or absence of a DoC Tag

	DoC Tag present	DoC Tag not present
Advantages	Simplified certification step	No need to extend the RE Configuration Policy
	Simplified PKI	
	Simplified asset management	
Disadvantages	Need to extend the RE Configuration Policy	More complex PKI to support the certification step
		More complex asset management for manufacturers

7.5.3.1.1.4 Entity authentication and management

As exemplified in both models care is to be given to the issuance of identities as they have to be either locally or globally unique. Additional considerations apply to the RRS Platform ID which should be hard to guess.

In order to reduce the risk of an unknown or unauthorized entity, the RRS Platform, RadioApp Store, RAP/DoC Provider, CCE, Software Provider, and OEM should be authenticated by means of a shared secret or certificate tied to their identity. The revocation of a given entity is a consequence of the revocation of their credential.

7.5.3.2 Application of non-repudiation framework

The purpose of the non-repudiation framework is to prevent denial of transmission or reception of information. Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information. This requires providing evidence of the origin of the information and being able to relate it to the information it applies to. Non-repudiation of receipt ensures that the recipient of information cannot successfully deny receiving the information. This requires providing evidence of receipt of the information and being able to relate it to the information it applies to. Both are achieved by means of digital signature based schemes applied to the identity of the source (or recipient) and the transmitted information.

7.5.3.3 Application of integrity verification framework

The purpose of the integrity verification framework is to ensure that packages introduced to the system are free from manipulation in the path from developer to end user, and that the supply chain involved in their distribution can be trusted and verified. The mechanism recommended is a digital signature based scheme that builds on the identity management framework outlined above.

7.5.4 Summary of threats introduced by countermeasures

Void.

8 Modifications applicable to the RRS architecture

8.1 Additional elements

Architectural elements supporting RRS security are defined in ETSI EN 303 095 [i.13].

Figure 17: Void

Figure 18 provides an overview of the cryptographic functions provided by the ASF as well as the Asset Endorsement Functions, and how they are arranged together in order to support the digital signature strategy providing confidentiality, integrity, and authenticity of RRS assets, and the non-repudiation strategy.

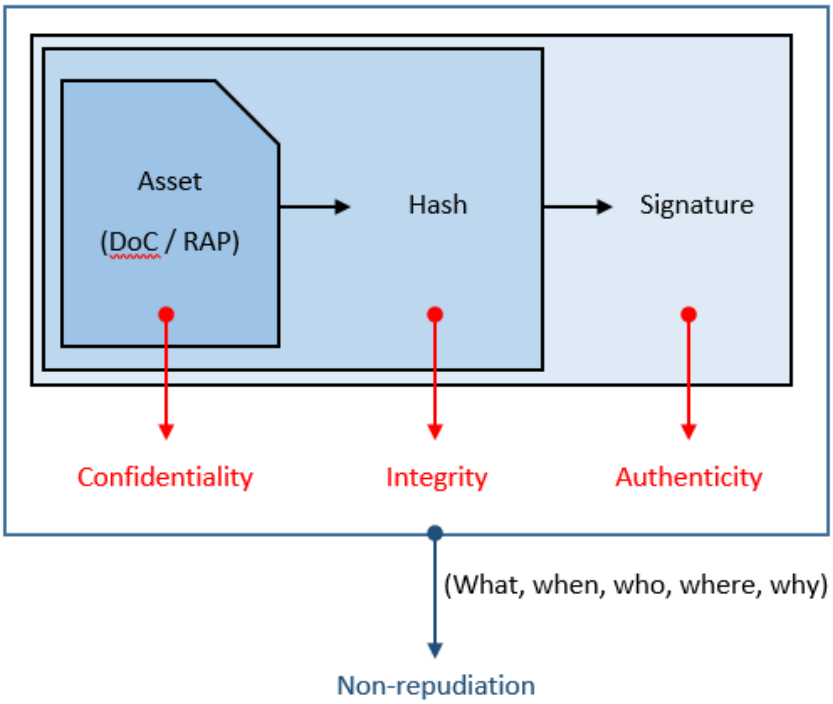

Figure 18: cryptographic functions applied to RRS assets

8.2 Additional flow diagrams

8.2.1 RAP endorsement, distribution, and validation

Figure 19 illustrates the various steps from packaging and endorsement to validation of an RAP. Once the RAP is validated the flow resumes at the certification step as defined in clause 6.1 of ETSI EN 303 095 [i.13].

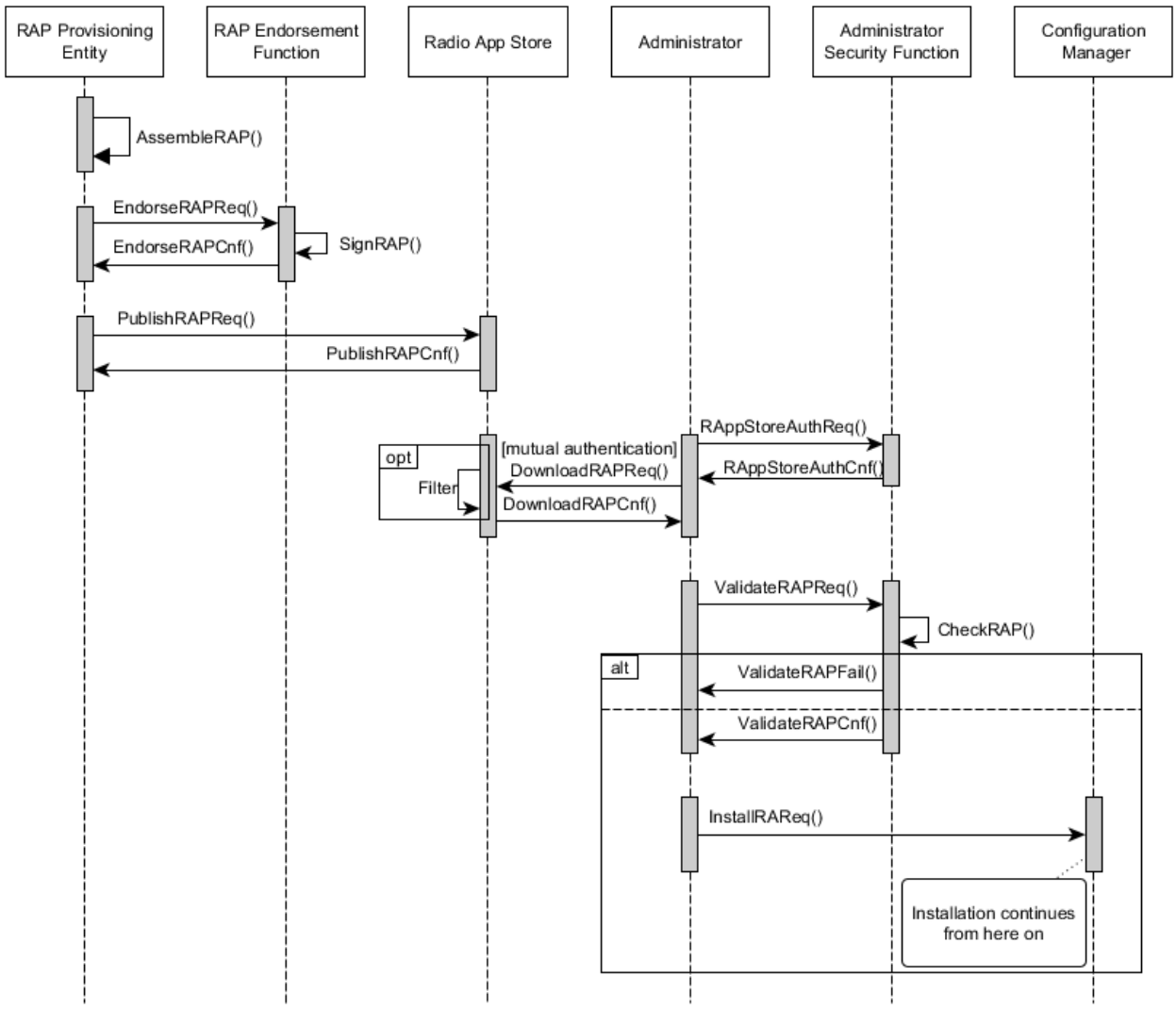

Figure 19: Flow diagram for RAP endorsement, distribution and validation

Once the RAP is assembled it is submitted to the RAP Endorsement Function for endorsement, that is to say for digital signature by relevant stakeholders (e.g. the OEM, the Software Provider, and the CCE). Following this step, it is published on the RadioApp Store. Who participates to the signing process and how it is implemented (e.g. in which order the RAP is signed) depends on the chosen business model and is therefore not detailed further.

After the RadioApp Store and the RE have mutually authenticated each other, the Radio App store may compile a restricted list of Radio Application available to the RE. The ASF verifies the origin and integrity of the RAP by validating the digital signature. In case of success the installation proceeds to the certification step by the Configuration Manager.

In order to ensure that the RE will only install valid RA, the RAP endorsement and validation mechanism is enforced in software. This requires that the Administrator and the Configuration Manager (for the certification step) be part of the RE root of trust and their trustworthiness evaluated through an assurance process.

8.2.2 DoC endorsement, distribution, and validation

The situation is very similar to the RAP case, with the exception that either the complete DoC, or the combination of the simplified and complete DoC, may be provided for endorsement and publication. For the sake of simplicity, the RadioApp Store is defined as the entity distributing both variants of the DoC, although it would be possible to have another entity distribute the complete DoC when the simplified DoC is made available via the RadioApp Store.

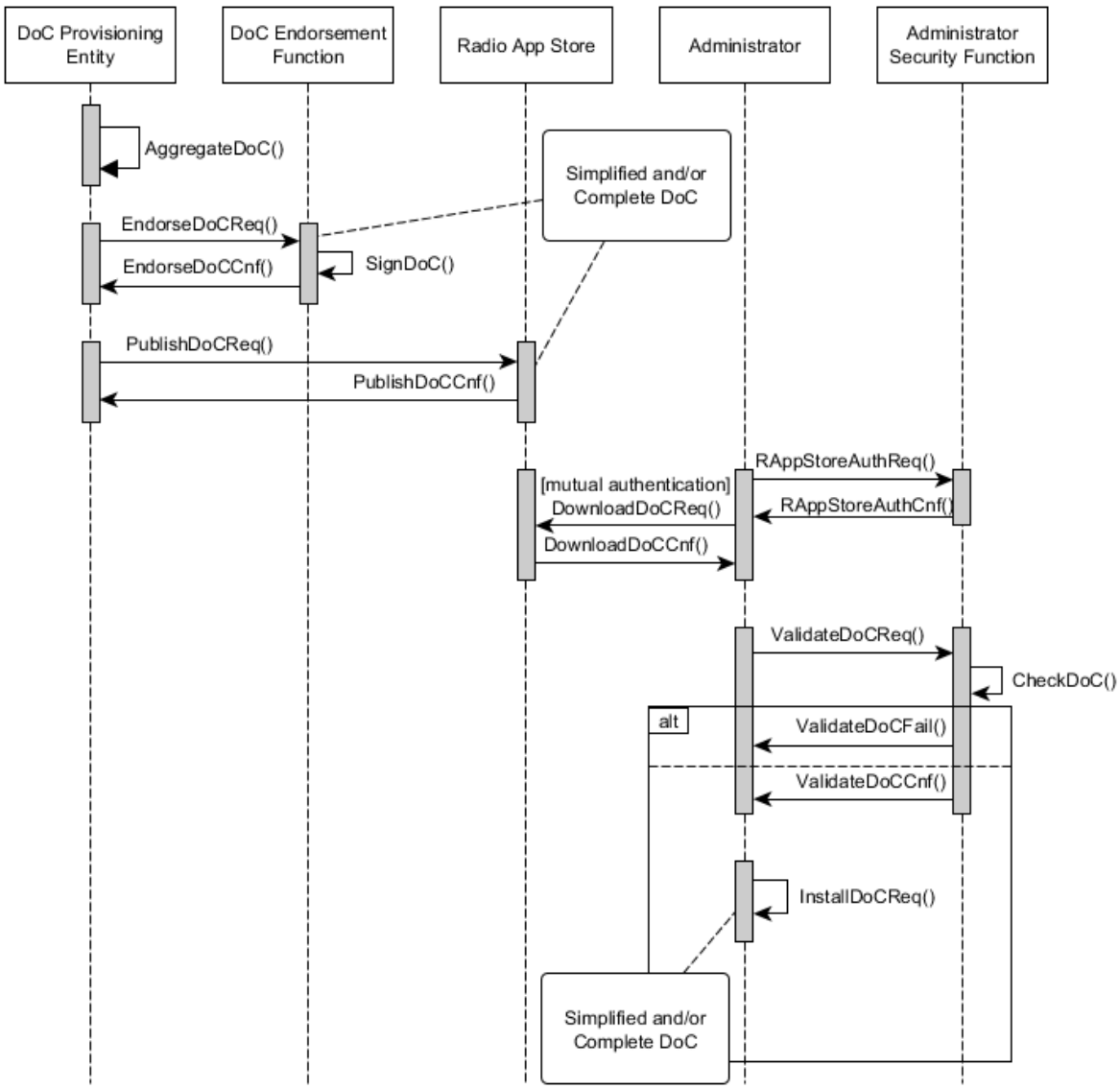

Figure 20: Flow diagram for DoC endorsement, distribution and validation

The DoC installation step does not necessarily imply a formal installation of the DoC on the device - although that is a possibility. At this point however, the DoC should be available to the RE for the compliance verification step.

Figure 21 is an exemplary flow diagram illustrating the retrieval of the complete DoC from the simplified DoC on the RE.

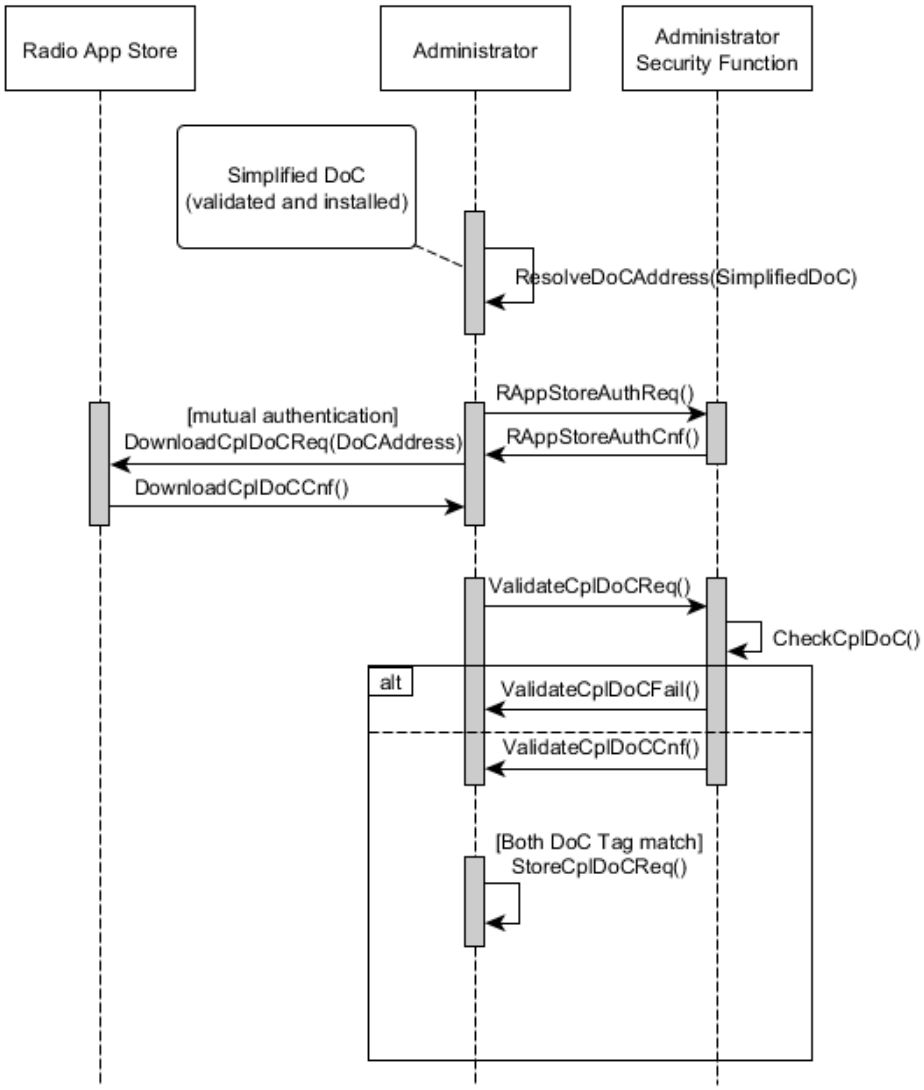

Figure 21: Flow diagram for retrieval and validation of the complete DoC from the simplified DoC

The ResolveDoCAddress() step retrieves the internet address of the complete DoC from the installed simplified DoC, as per the requirements of annex VI of the RED [i.14]. Note the guard condition verifying that both DoC Tag match. It is essential to ensure that both DoC match after their origin and integrity have been verified, otherwise there exist a risk of retrieving an incorrect DoC.

9 Remote attestation of the Reconfigurable Equipment status (installed RA and DoC)

9.1 Overview of remote attestation use case

The purpose of "remote attestation" is to allow an authorized party to verify claims about the properties of a platform based on collected evidence, and to derive decisions from those properties. Such properties include e.g. the composition of the platform (hardware components, installed software), status, and environmental information (active users, location…). While the primary purpose is to ensure proper behaviour of the target platform - by verifying that the platform has not been modified, or is running a proper set of hardware and software components - remote attestation can be leveraged for decisions that depend on the status of the platform (such as authorization and access control).

For RRS the target platform is the base hardware of the RRS platform, the RCF, the CSL, and the set of installed RA and their associated DoC and RE Configuration Policy. The Remote Attestation facility extends the capabilities of the non-repudiation framework by requesting evidence of the status and installed software on the platform. A very basic model of what remote attestation does is to request the platform to provide a manifest of its installed firmware and software and to compare that to an externally maintained list of allowed software, e.g. "diff manifest_installed known_allowed".

NOTE 1: For a generic model of remote attestation the scope of remote attestation for the purposes of the present document covers only those elements that describe radio operation. Thus applications on the RRS platform's host should not be considered in the scope of remote attestation for RRS, even though the capabilities of the host may be necessary for the purpose of remote attestation in RRS.

NOTE 2: In the context of RRS, remote attestation does not extend to information that is internal to any RAT. However a RAT may leverage the capabilities of the RRS platform when said RAT defines remote attestation procedures.

Assertion 1: Any 2 vendors installing the same set of RA will implement their RRS platform differently from each other. This in turns means that the build chain between two vendors will be different, in particular the RVM. Thus, assertions are not transferable, but may be composable.

Assertion 2: An RRS platform is designed to be mutable and the installed software base does not necessarily reflect the capability given by the DoC and the RE Configuration Policy (may be a subset, and explicitly cannot contain RAs that are not endorsed by the DoC).

NOTE 3: Attestation of the platform may also be defined locally. For the purposes of the present document it is assumed that the entities involved in remote attestation are physically as well as logically separated.

NOTE 4: The query protocol of remote attestation in the generic RRS platform is not defined in the RRS architecture.

Remote attestation entails the use of components on the target platform that are trusted for collecting, storing, and reporting evidence about the platform and its status. This is the purpose of the hardware root of trust as detailed in clause 12. For a remote attestation protocol to successfully complete it is necessary to attest the presence of such components. This is done by verifying that credentials exist, that vouch that the components are genuine, starting from the hardware root of trust and the host platform, and extending to other components that are part of the attestation hierarchy for the platform until a chain of trust exist from the root of trust to the keys that are used to attest to the platform's status (the attestation key).

Assertion 3: An RRS platform may depend on the host's hardware root of trust or possess its own as detailed in clause 12.1. A path exists from the hardware root of trust to validate the trustworthiness of the RRS platform for the purpose of remote attestation.

For remote attestation in RRS the following use cases are expected:

- Verification of compliance to the essential requirements of the RED [i.14] by the market surveillance authority.
- Verification of RRS platform status for device management purpose by the manufacturer.

- Verification of the active set of Radio Applications by the disturbance control authority.
- Verification of specific type and version of a Radio Application for access control by a mobile network operator.

NOTE 5: this last use case may be supported by the RAT itself.

9.2 Actors and relationships

9.2.1 The platform

The RRS platform is expected to record its own properties (such as firmware version, configuration and activated RAs) and key events such as:

- installation / deletion / update of the DoC, RE Configuration Policy, Radio Applications, and Mobility Policies;
- processing of configuration enforcement commands;
- processing of TAD and installation of profiles (see clause 11).

This is done via the Root of Trust for Measurement and Root of Trust for Storage, and trusted components in the attestation hierarchy such as the RRS platform firmware and the Administrator Security Function.

The information can be stored as separate properties, in a database, or as an auditable event log, as appropriate.

9.2.2 The attesting entity

This is a local entity which answers requests from a remote verifying entity, with information relevant to the requestor, along with proof of the information trustworthiness. The attesting entity enforces access control mechanisms to ensure that only authorized verifying entities can obtain and assess information pertaining to the platform. Different verifying entities may not have access to the same set of information.

The attesting entity is composed of the Root of Trust for Reporting and of components trusted for reporting in the attestation hierarchy. As such, an attestation may be the composition of atomic attestations pertaining to properties of various entities in the RRS platform. The entry point to the attesting entity is the Administrator Security Function in the CSL.

NOTE: An attesting entity could also be external to the RE and attest to composite properties of an RRS deployment by leveraging local attesting entities (for example, that all RE have an up-to-date Radio Application of a given type). While the current remote attestation framework does not forbid such advanced scenarios, the provisions for remote attesting entities are left for further study.

9.2.3 The verifying entity

The role of this entity is two-fold:

- to validate the trustworthiness of the information provided by the attesting entity - by verifying that the information is provided by a trusted platform combined with a legitimate root of trust, and that the information originates from components that are part of the attestation hierarchy (this prerequisite is assumed to be fulfilled in the considerations below);
- from the provided information, to derive a decision related to the assertion of the requestor.

The verifying authority implements access control mechanisms so that requestors can only request remote attestation they are authorized to.

For the constrained purposes of market surveillance where the master document identifying the allowed radio capability is the RE Configuration Policy, the verifying entity needs to verify the manifest of installed software against the allowed capabilities identified in the RE Configuration Policy. The verifying entity further needs to verify that the DoC that is present on the RE matches the RE Configuration Policy.

NOTE 1: To allow this to work the RE Configuration Policy has to be formatted in such a way that it is clearly able to match the manifest of installed RA and RRS platform firmware.

NOTE 2: Remote attestation for market surveillance can allow two types of decisions: firstly, that compliance testing by market surveillance can take place (there is a valid DoC on the RE and the installed RAs match), and secondly, when the combination of hardware and software is already known to be compliant, market surveillance can directly determine that an RE is compliant to the essential requirements of the RED [i.14].

For the purpose of platform status verification by the manufacturer, the verifying entity needs to verify the RE Type and the RRS firmware version. It may also need to:

- verify the manifest of installed RA against authorized RAP/DoC Provider ID or Software Provider ID (depending on the endorsement model);
- obtain and verify the integrity of the event logs;
- verify the installed TAD(s), RRS-CP Profile and RRS Configuration Profile.

For the purpose of disturbance control, the verifying entity needs to verify the RRS Platform ID, the location of the RE, and the manifest of active RA.

For the purpose of network access control, the verifying entity needs to verify the RAP ID of a specific RA.

9.2.4 The requestor

The requestor is an entity that wishes to validate high-level assertions about a target, The requestor does not execute the remote attestation protocol directly but delegates this task to the verifying entity. This assumes that there is a trust relationship between the requestor and the verifying entity.

Table 9a provides example of high-level assertions that requestors may wish to validate, depending on the use case.

Table 9a: Example high-level assertions for requestors

Use case	Example assertions
Verification of compliance	The target device possesses a valid DoC, and the installed RAs match the capabilities announced of the DoC
	The combination of hardware and software on the target device is compliant to the essential requirements of the Directive 2014/53/EU [i.14]
Verification of RRS platform status	The target device possesses a valid and up-to-date firmware
	The event logs show no attempt at compromising the RE security mechanisms
	A specific RA is not installed on any of the RE operating on the network
Disturbance control	The target device is the offending device
Network access control	The target device possesses a version of the RA that supports the capabilities that are required for operating on the network

In several of the remote attestation use cases it is not necessary to know the RRS Platform ID or even the RE type and the DoC Serial, as exemplified in clause 9.2.3. The implication is that the remote attestation protocol can by default avoid unnecessary exposure of privacy-sensitive information, unless absolutely necessary.

9.3 Considerations for remote attestation solutions in RRS

9.3.1 Relation to the non-repudiation framework

Remote attestation extends the non-repudiation framework by providing access to information on the RRS platform itself. While the non-repudiation framework can provide a historical view of past transactions on an RRS deployment and thus allow to infer the status of a given RE based on this information, remote attestation allows to connect to the RE and obtain fresh status information. Information freshness is important to support real-time decisions such as access control, and is poorly supported by the non-repudiation framework. One the other hand, the non-repudiation framework is superior in efficiency when an assertion is to be proven for a large number of RE (for example, to attest to the completion of an upgrade campaign without connecting to each device in order to obtain the evidence of the upgrade operation).

The non-repudiation framework requires careful considerations on the protection of privacy-sensitive information. Indeed, for the evidences gathered to be meaningful, information allowing the identification of the RE need to be included in the data set. There exist anonymous methods of remote attestation (see clause 9.4) which would allow the verifying entity to verify claims about an RE without the need to identify the RE.

9.3.2 Implementation

Remote attestation is typically performed by digitally signing the requested data where the digital signature's semantic is that the data originates from a source trusted to attest to the data validity. To this end the key used to perform the digital signature (the attestation key) is part of an attestation hierarchy that vouches that the attesting entity is part of a trusted platform (as detailed in clause 9.1).

The ability to attest to platform properties requires that the measured information be stored in memory locations that are protected from tampering, including deletion. As there is limited tamper-resistant memory available in a hardware root of trust, properties that can withstand deletion can be saved in a protected store outside of the hardware root of trust (see clause 12.2.5). One way to retain the ability to attest to these properties is to store them - in an ordered fashion - as leaf nodes of a Merkle tree in a protected store, and save the root node of the Merkle tree to the hardware root of trust.

Remote attestation is usually combined with public-key encryption so that the information sent can only be read by the programs that presented and requested the attestation, and not by an eavesdropper.

9.4 Direct Anonymous Attestation

Direct Anonymous Attestation is an anonymous or pseudonymous signature scheme (refer to annex K). It is used in TPM 1.2 [i.29] and TPM 2.0 [i.28] specifications. It provides a solution to convince a third-party (the verifying entity) that an attestation key comes from a TPM, without identifying the TPM. The protocol further embeds a revocation mechanism allowing the verifying party to determine whether the attestation key comes from a legitimate TPM.

Direct Anonymous Attestation addresses the limitations of other attestation schemes w.r.t. privacy:

- when the TPM uses the Endorsement Key (EK) to authenticate the attestation key, all transactions of the device become linkable to each other (through the EK);
- if a group secret is provisioned on all TPM of a given type, then anonymity is ensured by the presence of a global secret, however extraction of the secret from one TPM would render legitimate and malicious TPMs indistinguishable to verifiers as the global secret would be known to attackers;
- a privacy Certificate Authority could vouch to a verifier that an attestation key comes from a legitimate TPM (e.g. the privacy CA verifies the TPM's EK), without disclosing the EK and other identifying information to the verifier, however there are risks that the privacy CA may be compromised or collude with the verifier in order to uncover the TPM's identity.

The use of Direct Anonymous Attestation makes sense when it is not necessary to include platform identification information in the attested data.

10 Configuration enforcement of reconfigurable equipment

10.1 Introduction and scenario

The procedure described in clause 7.3.2 of the present document allows for the Reconfigurable Equipment to select and install RAs under the strict control of the DoC. However, the details of the selection process are left to market deployment - it could be user-driven, automated by the terminal, or decided by a control entity in the network. The configuration enforcement framework is a selection process whereby a network entity controls the state of the RE. It is therefore a remote control procedure.

The configuration enforcement framework can support the following use cases:

- management of radio applications;
- radio spectrum management and mobility policy management;
- RRS platform management (discovery, registration, and capability identification);
- initiation of a remote attestation procedure;
- lifecycle management of the RRS platform on the RE;
- disturbance control operations.

The disturbance control use case described in ETSI TR 102 967 [i.18], clause 6.6 is foreseen to become critical in the future and is at the core of the design - in such case, a misbehaving device can cause harm in the sense given by the RED [i.14] (see annex A of the present document). In addition to the Disturbance Control Body, other actors may use this functionality.

EXAMPLE: The RAP/DoC Provider may wish to trigger the RE so that it connects to the RadioApp Store and performs an update. This can help pushing updates in a scalable manner, without the network overhead incurred by devices regularly polling the RadioApp Store.

10.2 Scope

10.2.1 Background

The scope of the configuration enforcement framework is that of the compliance requirements set forth by the RED [i.14]. It should be noted that other control frameworks may be in place:

- on the RE, to manage aspects of the device that are not related to radio reconfigurability (for example, the update mechanism of the host Operating System, the device firmware);
- in the network e.g. for network planning.

The configuration enforcement framework is designed so that they do not overlap, with the view that it can be used in a standalone manner or as an extension of those frameworks, depending on market and regulatory requirements.

NOTE: Some of the existing reconfiguration frameworks are presented in annex I of the present document.

It is recalled that the DoC is the master document that identifies which hardware and software combination are conformant to the essential requirements of the RED, and that the RE Configuration Policy that is provided along with the DoC indicates which RAs can be installed on an RE. The configuration enforcement framework is not meant to go beyond (or override) what the DoC and the RE Configuration Policy allow.

Accordingly, the configuration enforcement framework focuses on the management of the DoC, the RE Configuration Policy, the RA, and the radio behaviour. Other aspects of the RRS Platform (RCF, CSL) are out of scope: these are expected to be handled e.g. as part of firmware management mechanisms on the host device.

The peer to the configuration enforcement entity in the network is the Administrator in the CSL.

10.2.2 Core Command set

Below is the minimal set of commands which would be required to provide basic functionalities of the configuration enforcement framework:

- Commands related to Radio Application management:
  - List installed RA.
  - Connect:
    - The Connect command triggers the RE so that it connects to the RadioApp Store and automatically update the DoC, the RE Configuration Policy, and installed RA.
- Commands related to RRS platform management:
  - Query RRS capability:
    - Using a known identifier of the device under a specific RAT - such as the IMEI - the device is queried for its RRS capability and its RRS identity.
- Commands related to disturbance control:
  - Safe mode:
    - This command instructs the RE to fall back into a safe radio configuration as defined by the manufacturer prior to the device being placed on the market.

10.2.3 Extended Command Set

Below are additional commands which would allow to extend the functionalities of the configuration enforcement framework. These are provided for reference, in order to assess the foreseeable capabilities of the framework:

- Commands related to Radio Application management:
  - Install RA, Update a given RA:
    - This command triggers the RE to connect to the RadioApp Store, download the identified RA from the RadioApp Store, and install it (or update the installed version).
  - Delete RA.
  - Update DoC.
  - Update RE Configuration Policy.
  - Snapshot and Snapshot Deletion:
    - The Snapshot command consists in saving the currently installed DoC, RE Configuration Policy, and RA, and pinning them as a restoration point, so that the radio components of the RE can be restored in a known working state.
  - Restore:
    - The Restore command resets the RE with a combination of DoC, RE Configuration Policy, and RA that was previously saved as a snapshot.
- Commands related to RRS platform management:
  - Register:
    - This is an outbound command allowing the RE to register to a well-known network entity, as an RRS capable device.

- Initiate remote attestation.

NOTE 1: This command is not part of the core set as remote attestation may have its own entry point on the RE.

- Commands related to radio spectrum management:
  - Example commands include, but are not limited to, request for activated RAT, indication of preferred RAT, indication of preferred channel to use for a given RAT, request for bandwidth throttling for a given RAT.
- Commands related to mobility policy management.
- Commands related to lifecycle management of the RRS platform:
  - The lifecycle management framework is detailed in clause 11 of the present document. Example commands include issuance of a TAD, RRS-CP Profile, or RRS Configuration Profile.
- Commands related to disturbance control and spectrum management:
  - RA Switch-off:
    - A specific Radio Application on the RE is forbidden to operate (or deactivated). Depending on the radio access technology, the command may target reception, transmission, or both capabilities. In addition, the command may have effect for a limited time, or may have permanent effect.
  - RA Switch-on:
    - A specific Radio Application on the RE is permitted to operate again. Depending on the radio access technology, the command may target reception, transmission, or both capabilities.
  - Radio front-end Switch-off:
    - The command may have effect for a limited time, or may have permanent effect.
  - Radio front-end Switch-on.

NOTE 2: On RE that only have radio capabilities, the Radio front-end Switch-on operation is not available remotely and can only be performed locally on the device. A similar situation may arise when all RA on the device are switched-off for reception.

NOTE 3: Operations related to disturbance control are very invasive and should be guarded with specific countermeasures to prevent abuse. Some of these countermeasures are administrative and legal procedures that are out of scope of the present document.

10.2.4 Actors

The following actors have been identified as users of the configuration enforcement feature:

- The Market Surveillance Body, a specialization of the National Regulatory Authority, who may leverage the querying capabilities of the configuration enforcement framework as part of the conformance assessment procedure of a given device.
- The Disturbance Control Body, a specialization of the National Regulatory Authority, who may enforce the configuration of the RE on regulatory grounds.
- The RAP/DoC Provider as an abstraction of the CCE, OEM, and Software Manufacturer, who may enforce the configuration of the RE for operational reasons.
- The Radio Network Manager, an abstract entity in the network that is responsible for radio spectrum management.

Depending on user expectations as well as operational and regulatory requirements, each actor may only have access to a subset of the available operations. An access control matrix is proposed below, that applies the separation of duty principle. In this approach, the RAP/DoC Provider is expected to cooperate with other actors when the remote attestation facility is needed.

Table 10: Exemplary access control matrix for configuration enforcement

Command	Market Surveillance Body	Disturbance Control Body	RAP/DoC Provider	Radio Network Manager
List installed RA	Allowed	Allowed	Allowed	Allowed
Connect	-	-	Allowed	-
Query RRS capability	Allowed	Allowed	Allowed	Allowed
Safe mode	-	Allowed	-	-
Install, Delete, Update RA	-	-	Allowed	-
Update DoC	-	-	Allowed	-
Snapshot, Snapshot Deletion, Restore	-	-	Allowed	-
Register	-	-	-	-
Initiate remote attestation	-	-	Allowed	-
radio spectrum management commands	-	-	-	Allowed
RA Switch-off/on	-	Allowed	-	-
Radio front-end Switch-off/on	-	Allowed	-	-
NOTE: When different actors can perform an overlapping set of operations, a mechanism might be needed to resolve conflicts.				

10.3 Technical considerations

10.3.1 RAT capabilities

Each RAT may provide a specific set of transport mechanisms to the configuration enforcement framework, or may require that a specific mechanism be provided. Assuming there is a common implementation of configuration enforcement on the RE, an extension may be necessary to support a given RAT (e.g. a plugin). One possibility to deliver this extension is via the RAP.

In addition, operational restrictions on the RAT may limit network interactions related to configuration enforcement. Namely, the availability of the Internet Protocol is not guaranteed, bandwidth may be limited, and bidirectional interaction may not be possible.

10.3.2 Access control

Considering that different actor may perform a different set of configuration operations, a mechanism is required so that the configuration enforcement client on the RE can apply specific access rules for each actor. Due to possible operational restrictions, the configuration enforcement client may not be able to challenge an actor in order to prove its identity (which would be an interactive operation).

10.3.3 Default control channel

The RRS platform allows to simultaneously host different Radio Applications supporting various Radio Access Technologies, and the set of supported RAT will change over time. Therefore, there cannot be a single, fixed RAT to be used as a reference delivery channel for the implementation of configuration enforcement (that is, to transport remote control messages and responses). This has the following consequences:

- a mechanism is needed for the RE to identify over which RAT it should expect to receive control messages (or each RA has a mechanism to receive control messages);
- similarly, a mechanism is needed for the network to identify over which RAT it can address the configuration enforcement client.

10.4 Technical implementation

10.4.1 Introduction

The worst case for distribution of command messages is taken as a baseline, namely, that the transport channel is unidirectional and that the command should fit in one message that should be a small as possible - that is, in one single application protocol data unit (APDU). The data model should therefore strictly match the command set and properties of the configuration enforcement protocol.

Since it is not possible to make any assumption regarding private extensions and fields for opaque data, these are not taken into account in the present analysis.

In case a confirmation message is needed, it may be transported over another channel.

10.4.2 Data model and data flows

It is assumed that the underlying protocol used to transport command messages provides source and destination addresses when necessary, as well as the parameters identifying the APDU as a configuration enforcement APDU and the target service access point on the receiving peer. When this information cannot be carried by the transport protocol, it may be necessary to provide it as metadata to the command message APDU.

The following parameters are expected to always be part of the APDU:

- application-level identity of the originating peer;

NOTE: For network originated command messages this is the identifier of the network entity acting on behalf of an actor identified in clause 10.2.4.

- application-level identify of the destination peer;
- command identifier.

The transactional model is that of a query-only mechanism whereby a response may be provided when the communication channel allows, or may be inferred from the behaviour of the system. These strong constraints make it possible to integrate the configuration enforcement framework in other management solutions, including those that rely on unidirectional channels (such as broadcast-only systems).

Table 11 details the origin, parameters and expected response of each command.

Table 11: high-level data model for configuration enforcement commands

Command	Origin	Parameters	Expected response	Suitable for unidirectional protocol
List installed RA	Network	None	Structured list of RAP IDs	N
Connect	Network	RadioApp Store ID (optional)	Acknowledgment	Y
Query RRS capability	Network	None	RRS Platform ID	N
Safe mode	Network	None	Acknowledgment	Y
Install, Delete	Network	RAP ID	Acknowledgement with optional success indication	Y
Update RA	Network	Installed RAP ID, replacement RAP ID	Acknowledgement with optional success indication	Y
Update DoC	Network	replacement DoC Serial	Acknowledgment	Y
Update RE Configuration Policy	Network	replacement RECP Serial	Acknowledgment	Y
Snapshot	Network	None	Snapshot ID	Y
Snapshot Deletion	Network	Snapshot ID	Acknowledgement with optional success indication	Y
Restore	Network	Snapshot ID	Acknowledgement with optional success indication	Y
Register	Device	RRS Platform ID, structured list of activated RAP ID	Acknowledgment	Y (see note)
Initiate remote attestation	Network	Depends on remote attestation protocol	Undetermined	Undetermined
radio spectrum management commands	Network	Depends on the command (not detailed in the present document)	Undetermined	Undetermined
RA Switch-off	Network	RA ID, Time span, capability	Acknowledgment	Y
RA Switch-on	Network	RA ID, capability	Acknowledgment	Y
Radio front-end Switch-off	Network	Time span	None	Y
Radio front-end Switch-on	Network	None	None	Y
NOTE: In case the registration happens on a unidirectional channel it is assumed that other RATs are installed and activated on the RE, that would allow the proper operation of the configuration enforcement framework.				

10.4.3 Delivery mechanisms in selected RAT

Several categories of mechanisms are envisioned for delivery of command messages, considering that they are mostly network-originated:

- message-based, connectionless delivery mechanisms such as point-to-point SMS (SMS-PP), Cell Broadcast Service, or SMS-based WAP Push/OMA Push;
- IP-based connection-oriented mechanisms such as an OMA Push Client acting as an HTTP server;
- IP-based connectionless mechanisms such as CoAP.

Details and security considerations relative to these delivery mechanisms are provided in [i.27].

10.5 Security objectives

Based on the previous assumptions the following security objectives are identified:

- Confidentiality:
  - The configuration enforcement framework should provide means to ensure that the command APDUs are protected from exposure to 3rd parties.

NOTE: This is mainly to prevent an adversary from leveraging information from command messages in order to better target attacks, and to protect the privacy of the device user by avoiding fingerprinting of the device over the air based on its RRS capabilities.

- Integrity:
  - The configuration enforcement framework should provide means to verify that the content of the command APDU has not been modified prior to processing at receipt.
  - The configuration enforcement framework should provide means to protect against traffic manipulation.
  - The configuration enforcement framework should ensure that malformed commands cannot compromise the proper operation of the RE.
- Authentication:
  - The configuration enforcement framework should provide means for the RE to verify the identity of a command originator, without the availability of a return channel.
  - The configuration enforcement framework should provide means for a network entity to verify the identity of the RE.
  - The configuration enforcement framework should not process control messages that have not been issued by an authorized entity.
- Accountability:
  - When the sensitivity of the command is high the configuration enforcement framework should provide means to prevent the related actor denying the transfer of such command.

Because the configuration enforcement framework is considered independently of the delivery mechanisms, no objective is set regarding availability. It should be noted that the framework depends on the availability guarantees of the transport network.

10.6 Threats

Based on the assumption for the configuration enforcement framework as well as the security objectives, the following threats have been identified.

Table 12: threats to security objectives for the configuration enforcement framework

Objective class	Threat class	Notes
confidentiality	eavesdropping	Signalling information as well as device status information could be observed and leveraged to build further attacks.
	traffic analysis	Changes in traffic patterns may allow to infer ongoing activities.
	fingerprinting & tracking	Interaction with the RE at the level of the configuration enforcement client, or eavesdropping could be used to gather information for the purpose of fingerprinting the RE (device type, device status) which, when combined with other information, may be used to uniquely identify and track the device. A consequence of illegitimate tracking is the compromise of the device user's privacy.
integrity	data modification	A command or response message is modified on the fly.
	spoofing	Illegitimate command or response messages are injected.
	malicious input	A malformed message allows an adversary to cause malfunction or take control of the RE.
	replay	A message from a legitimate entity, that was already processed, is being sent again by an adversary.
authentication/identity	masquerading	A third-party pretends to be a legitimate actor to the framework.
	unauthorized access	A specific message, sequence of messages or environmental conditions cause the authorization step to be bypassed.
accountability	repudiation	A configuration command was sent but the emitter denies the sending of the command.

11 Long-term management of reconfigurable equipment

11.1 Introduction and scenario

The reconfigurability provided by RRS will increase the long-term relevance of the underlying hardware platform since hardware accelerators and radio software libraries can be re-organized into new RATs - that is, into newer generations of current access technologies or into a completely different RAT that would nevertheless leverage the existing building block provided by the RRS platform. Devices that have been placed on the market can also be updated in order to correct design flaws of early RAT versions. This can be an advantage for operators of radio access networks who would otherwise have to support immutable legacy devices at the expense of efficiency.

Instead of reducing the lifetime of the device it is attached to, an RE may follow the lifecycle of said device when the service provided is lightly affected by technological churn, or when the device is designed to last. Example of the former case are individual (autonomous) cars, examples of the latter case are SCADA or Industrial IoT devices. Thus, it can happen than the RE remains used in the field after the commercial or institutional entity, which is responsible for the RE reconfigurability, ceases its activities.

While unmanaged devices would not have been a problem in the past (the reader is invited to consider legacy, unconnected household devices as an example), this situation is becoming less acceptable at the time the present document is being written. At the radio level, the increased usage of the radio spectrum and reliance of the economy on digital services provided over the air requires continued improvements in spectrum efficiency and thus maintainability of deployed RAs. The exposure of radio devices to local networks or the Internet has given rise to new classes of threats and the need to continuously monitor and provide security updates to devices in order to reduce the probability of security incidents - especially when such incident can have lethal or other serious consequences. This is also required for Radio Applications since they manage the first layers (typically PHY and MAC) that are part of the attack surface. Once compromised a Radio Application could be made to behave in the interest of the attacker (e.g. against the essential requirements of the RED) or be used to compromise other elements on the device.

The purpose of the long-term management framework in RRS is to avoid the case where an RE becomes orphaned, i.e. that there is no entity responsible for the management of Radio Applications on the RE.

11.2 Scope

As with the configuration enforcement framework presented in clause 10 of the present document, the lifecycle management framework focuses on the services provided by the RRS Platform located on the RE, such as the RA and the DoC. It does not cover the RRS Platform itself or other components of the device. The reasons for this are manifold:

- the framework matches the services offered by the RRS specifications;
- the interfaces provided by the RRS Platform may be well documented for third parties, whereas the internals of the RRS Platform may remain confidential. Thus, a third party taking over the management of the RE may be able to develop RAs as a Software Manufacturer would do, or issue a new DoC or RE Configuration Policy as the CCE would do, but may not access core functionalities of the RRS platform;
- the RRS Platform itself may be part of another management framework on the device, that the OEM may not wish to open even after they would stop supporting the device;
- depending on the context and the jurisdiction, it may not be legally possible to grant administrative power to an entity that is not the device owner.

NOTE: An OEM may still extend the scope of the framework to the RRS Platform by leveraging the RRS Configuration Profile (detailed below) to bind it to the RRS firmware update mechanism of the RE.

11.3 Architecture and Actors

11.3.1 Introduction

Figure 22 provides an overview of the long-term management framework.

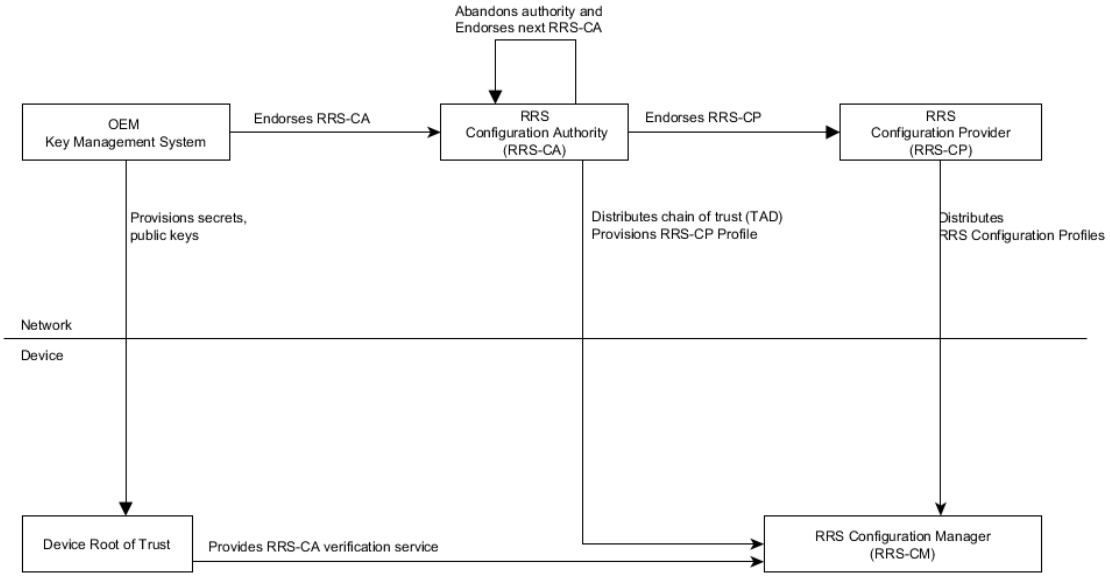

Figure 22: Overview of the long-term management framework

The long-term management framework is made of a multi-layered architecture that separates the provision of configuration parameters (handled by the RRS Configuration Provider, or RRS-CP) from the management of authoritative power (handled by the RRS Configuration Authority, or RRS-CA). The RRS-CP remains under the control of the RRS-CA and provides the RE with configuration parameters related to RRS operations, such as the RAP/DoC Provider or the URL of the RadioApp Store. These configuration parameters are handled by the RRS Configuration Manager (RRS-CM) which configures the RRS platform.

The flexibility of the framework resides in the ability of a RRS-CA to endorse a new RRS-CA, thus allowing the transfer of its authority over configuration management to a new entity in a controlled manner (by building a dynamic chain of trust), and in doing so, providing the means to avoid orphaned devices over an extended timeframe. This design matches the different roles in configuration management, with the RRS-CP role being of operational nature, while the role of the RRS-CA is that of a reference authority.

The OEM is the cornerstone of the framework, as it endorses the first RRS-CA and provisions secrets and functions in the device root of trust, allowing the RRS-CM to verify the legitimacy of the RRS-CA and RRS-CP, as well as the information provided by them. Cryptographic tools, business processes and requirements on software behaviour allow the chain of trust to remain valid even when the OEM and former RRS-CA would phase out.

The role of the RRS-CA could be hold by the Conformity Contact Entity or the RAP/DoC provider, although this is not mandatory.

NOTE: The current design does not make use of the Administrator Security Function in the CSL, as the long-term management framework configures the Administrator and the ASF. For the same reason, the RRS-CM is not mapped to the Configuration Manager in the existing RRS architecture.

11.3.2 The RRS Configuration Profile

The RRS Configuration Profile contains the necessary operational parameters allowing the RE to contact and authenticate network entities in the RRS architecture, and to authenticate actors. Examples include, but are not limited to:

- The RadioApp Store.
- Network entities and actors related to the configuration enforcement framework.
- Front-end and back-end compiler services (when the compilers are provided as online services to the RE).
- RAP/DoC Provider entity and the entities it is composed of (CCE, Software Manufacturer), except the OEM which remains an immutable entity in the framework.
- Market Surveillance Body/Disturbance Control Body.

The RRS Configuration Profile is a reference configuration document for the RE. The RE is not expected to bypass the configuration parameters present in the profile. Conceptually it can be mapped to OMA DM [i.24] Management Objects or to the XML configuration document in GSMA SPDC [i.26].

The RRS Configuration Profile is provided to the RRS-CM by the RRS-CP.

11.3.3 The RRS-CP Profile

The RRS-CP Profile contains the parameter identifying one or more RRS-CP and allowing the RE to authenticate them. The RE is not expected to connect to an RRS-CP, or to accept messages from an RRS-CP, that cannot be authenticated through the information provided by the RRS-CP Profile.

Depending on the interaction method between the RRS-CM and the RRS-CP, the RRS-CP Profile may contain a URL to the service access point of the RRS-CP.

The RRS-CP Profile is provided to the RRS-CM by the RRS-CA.

11.3.4 Transfer of Authority Document (TAD)

The Transfer of Authority Document is an electronic document that certifies that the holder (a RRS-CA) is entitled to administer the RRS parameter configuration of the RE. For the RE this translates into the RRS-CA being authorized to designate one of more RRS-CP for the RRS-CM to receive configuration parameters from.

The TAD contains at least the following information:

- Originator of the TAD (the identifier of the entity holding administrative authority at the time the TAD is issued).

- Beneficiary of the TAD (the identifier of the entity that will hold administrative authority after the TAD comes into effect).
- Date the TAD comes into effect.

NOTE: When the RE and the RRS-CA communicate with each other over an interactive channel, the identifier of the TAD beneficiary may contain a URL.

The first TAD is provided by the OEM. Subsequent TADs are provided by RRS-CAs.

11.3.5 Effective transfer of authority

The transfer of authority is formalized by the issuance of a TAD by the current RRS-CA, and electronic distribution of the TAD to the next RRS-CA as well as to the RRS-CM on the RE. This implies that the originator of the TAD abandons administrative rights over RRS parameter configuration on the RE. In effect, this is enforced by the RE.

As the authority over RRS parameter configuration is transferred from one RRS-CA to the next one, a chain of trust is progressively built from the issued TAD, with the OEM as the trust anchor. Since the premise of the long-term management framework is that an entity acting as an RRS-CA may cease their activity, it is the responsibility of the current RRS-CA as well as the RRS-CM to keep a copy of all issued TAD so that the chain of trust can be verified.

In order to simplify the implementation of the RRS-CM, the OEM bootstraps the long-term management framework by issuing the first TAD and designating itself as the first RRS-CA.

11.4 Verification of profiles and actors, profile updates

In order to verify the profiles and actors in the long-term management framework the actions detailed below are expected from the RRS-CM on the RE.

When a new RRS Configuration Profile is made available to the RE by a RRS-CP:

- The RRS-CM verifies the integrity of the RRS Configuration Profile and that it originates from the RRS-CP.
- The RRS-CM verifies that the RRS-CP is endorsed by the current RRS-CA.
- The RRS-CM installs the new RRS Configuration Profile and discards the previous one.

When a new RRS-CP Profile is made available to the RE by a RRS-CA:

- The RRS-CM verifies the integrity of the RRS-CP Profile and that it originates from the RRS-CA.
- The RRS-CM verifies that the RRS-CA is the current RRS-CA.
- The RRS-PPM installs the new RRS-CP Profile and discards the previous one.

When a new TAD is made available to the RE by the current RRS-CA:

- The RRS-CM verifies the integrity of the TAD and that is originates from the current RRS-CA.
- The RRS-CM saves the TAD and set the current RRS-CA to the identity of the beneficiary in the TAD.

During any of the above operation the RE verifies the chain of trust leading to the current RRS-CA by walking the chain backward (verifying each TAD from the previous one) until the original TAD is found and verified by the device root of trust.

NOTE: These mechanisms introduce specific threats that are detailed in clause 11.7.

11.5 Message flows

11.5.1 Transfer of authority between two RRS-CA

Figure 23 illustrates the steps of the transfer of authority.

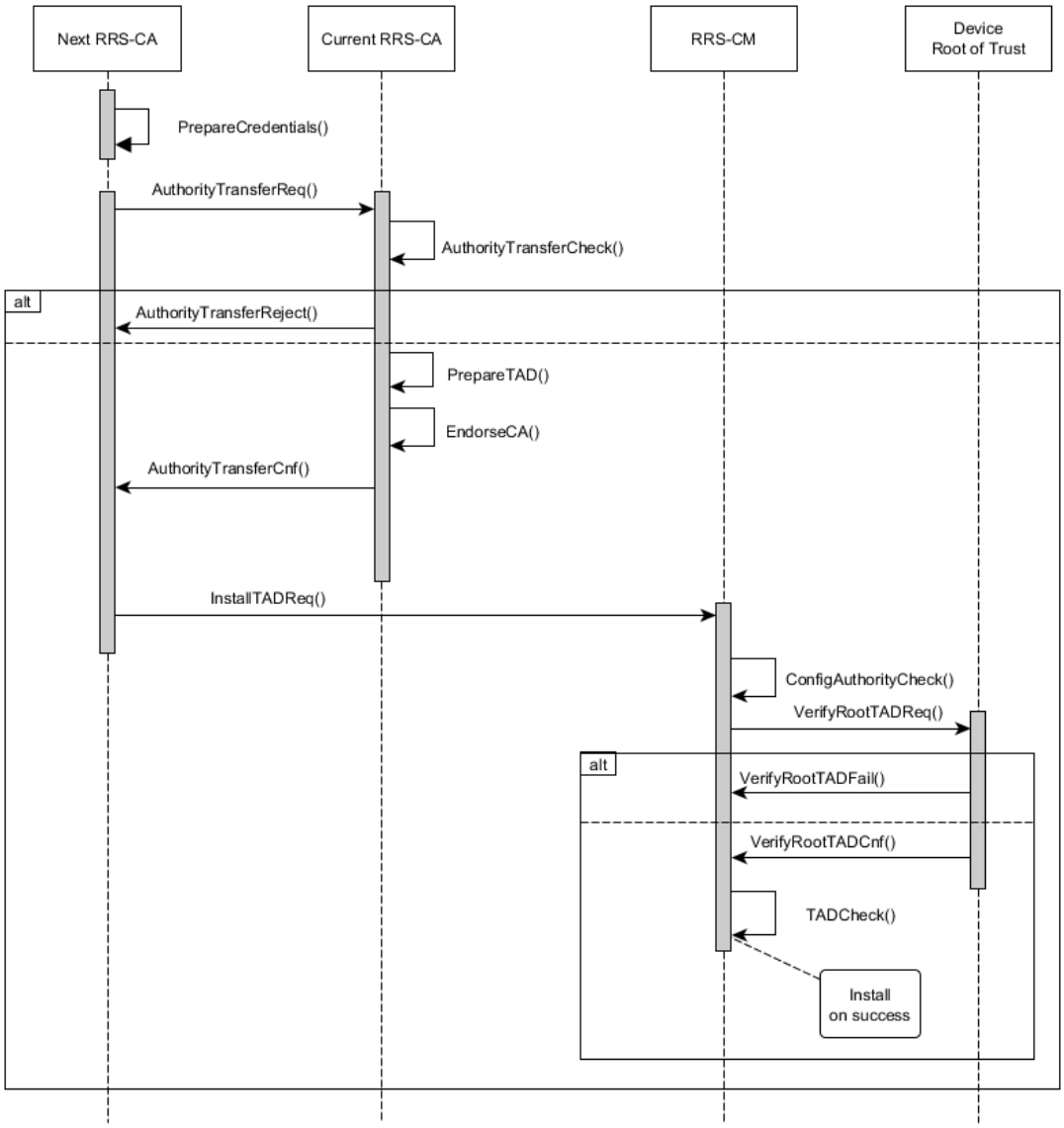

Figure 23: Flow diagram for the transfer of authority between two RRS-CA

Before requesting the transfer of authority from the current RRS-CA, the candidate RRS-CA prepares its credentials (these will be included in the TAD). The *AuthorityTransferCheck()* step illustrates the conclusion of an offline process that takes place between the two RRS-CA. Indeed, it is not expected that a transfer of authority happens easily. It should rather be viewed as the result of a market agreement, possibly involving a regulator or a market consortium.

When the transfer of authority is confirmed, the current RRS-CA generates a TAD and endorses the new RRS-CA. The new RRS-CA distributes the TAD to the RE. This does not contradict the rules detailed in clause 11.4: due to the difficulties and duration of update campaigns, the distribution task often cannot be the responsibility of the TAD originator.

When the TAD is received by the RE, the RRS-CM verifies the legitimacy of the TAD originator, followed by the TAD origin and integrity. When all checks are successful, the TAD is installed.

11.5.2 Designation of legitimate RRS-CP by the RRS-CA

Figure 24 illustrates how the RRS-CA designates a RRS-CP as legitimate.

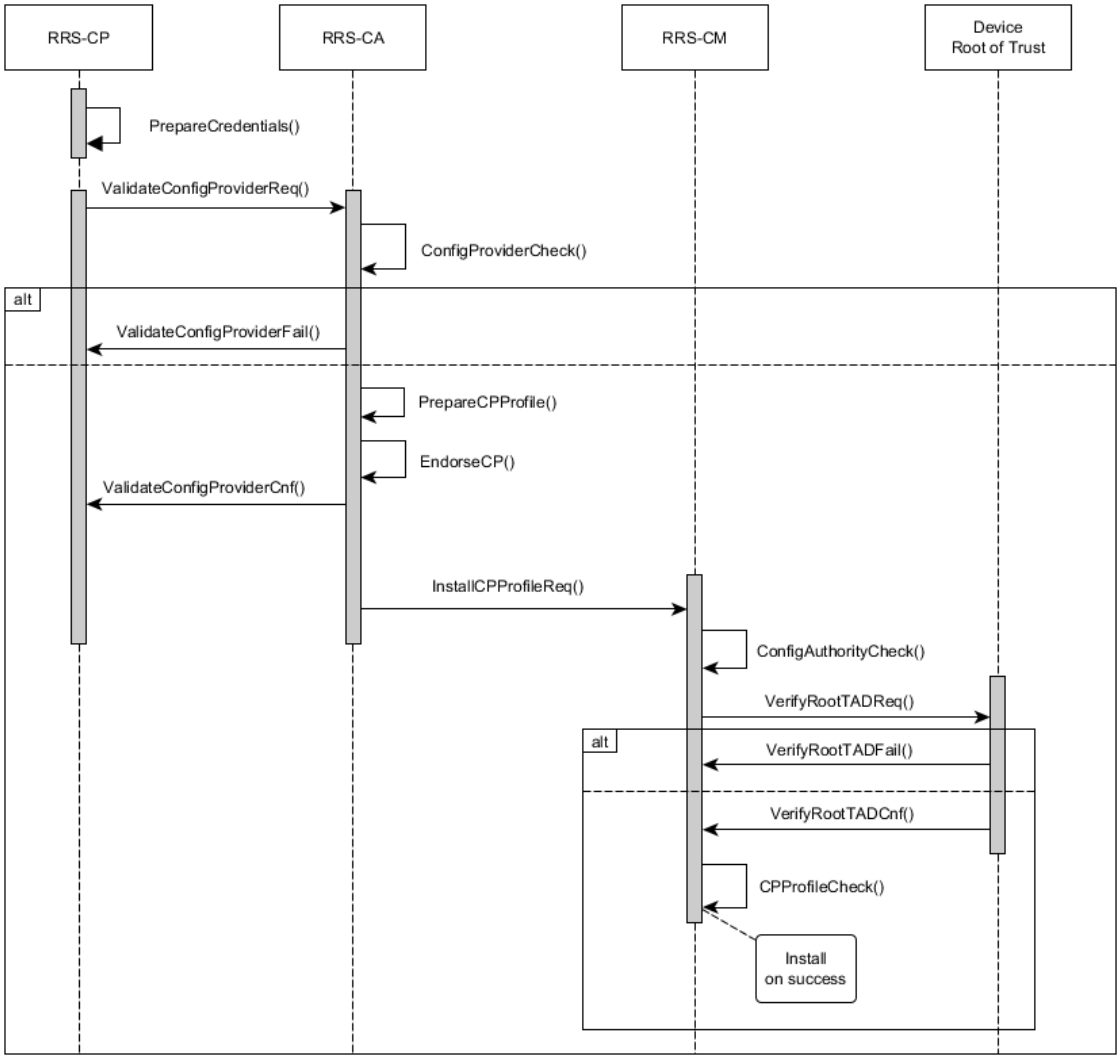

Figure 24: Flow diagram for the designation of a legitimate RRS-CP by the RRS-CA

Similar to the *AuthorityTransferCheck()* step in clause 11.5.1, the *ConfigProviderCheck()* step it also the conclusion of an offline agreement process between the RRS-CA and the RRS-CP. When the designation of a new RRS-CP is confirmed, the RRS-CA prepares and new RRS-CP Profile and endorses it. The profile is then distributed to the RRS-CM on the RE.

When the profile is received by the RE, the RRS-CM verifies the legitimacy of the RRS-CA, followed by the profile origin and integrity. When all checks are successful, the profile is installed and replaces the previous one.

11.5.3 Distribution of a new RRS Configuration Profile

Figure 25 illustrates how a new RRS Configuration Profile is distributed to the RE.

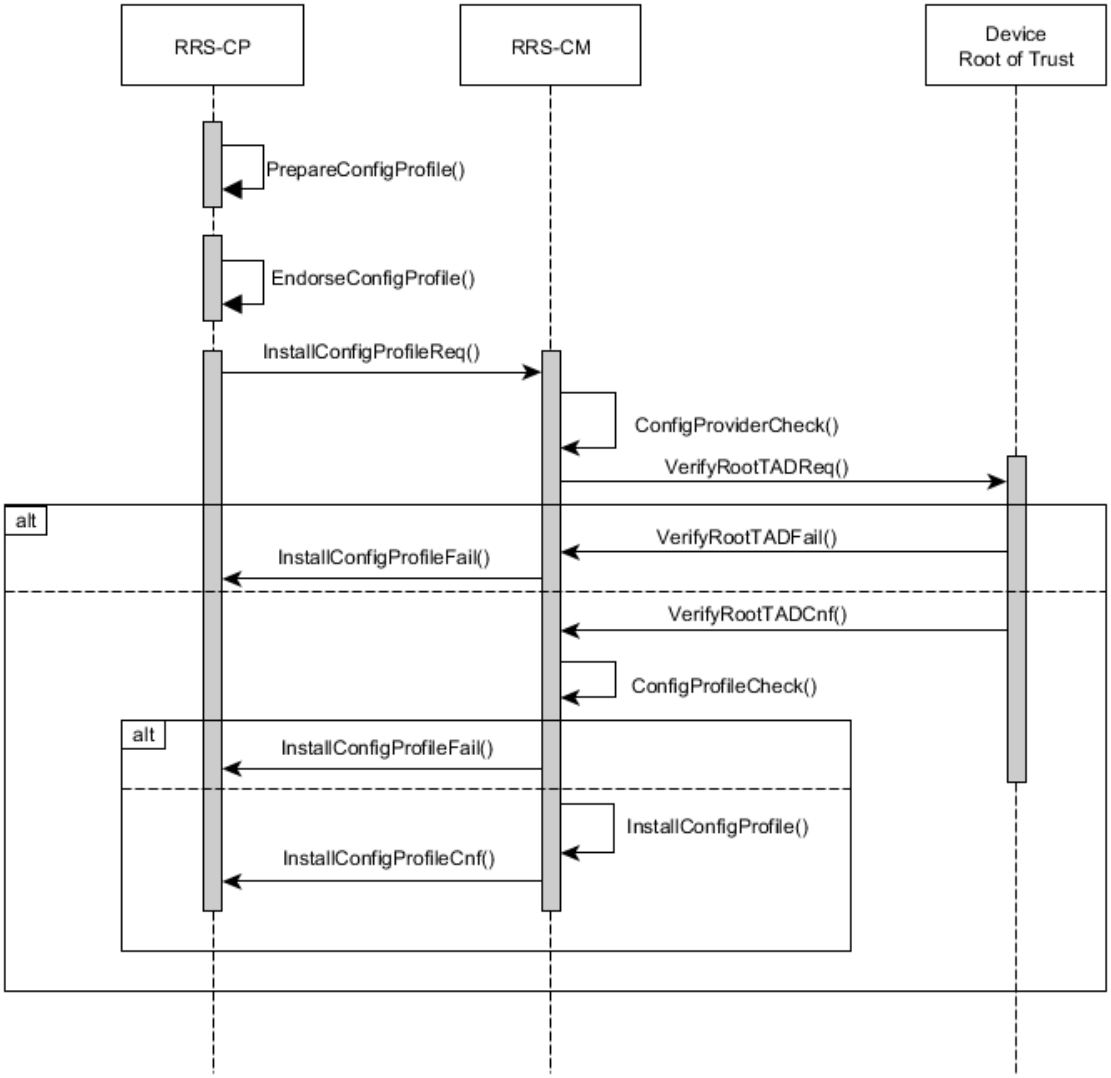

Figure 25: Flow diagram for the distribution of a new RRS Configuration Profile

In this procedure, the RRS-CP first prepares a new RRS Configuration Profile. This can happen e.g. with a change in the RadioApp Store infrastructure or with the RAP/DoC Provider.

Once the RRS-CP validity is verified it is endorsed by the RRS-CP and distributed to the RRS-CM on the RE.

When the profile is received by the RE, the RRS-CM verifies the legitimacy of the RRS-CP, followed by the profile origin and integrity. When all checks are successful, the profile is installed and replaces the previous one.

11.6 Security objectives

Based on the previous assumptions the following security objectives are identified.

At the level of communication security:

- Confidentiality:
  - The long-term management framework should provide means to ensure that the content of the communications between the RRS-CA and the RRS-CP are protected from exposure to authorized 3rd party.

- The long-term management framework should provide means to ensure that the content of the communications between the RRS-CA and the RRS-CM are protected from exposure to authorized 3rd party.
- The long-term management framework should provide means to ensure that the content of the communications between the RRS-CP and the RRS-CM are protected from exposure to authorized 3rd party.

- Integrity:
  - The long-term management framework should provide means to ensure that the content of communications between the RRS-CA and the RRS-CP has not been manipulated prior to processing at receipt.
  - The long-term management framework should provide means to ensure that the content of communications between the RRS-CA and the RRS-CM has not been manipulated prior to processing at receipt.
  - The long-term management framework should provide means to ensure that the content of communications between the RRS-CP and the RRS-CM has not been manipulated prior to processing at receipt.
- Authenticity:
  - The long-term management framework should provide means for the RRS-CA and RRS-CP to verify each other's identity.
  - The long-term management framework should provide means for the RRS-CA and RRS-CM to verify each other's identity.
  - The long-term management framework should provide means for the RRS-CP and RRS-CM to verify each other's identity.

At the level of TAD management:

- Integrity:
  - The long-term management framework should provide means for the RRS-CM to verify the integrity of the TAD at receipt.
- Authenticity:
  - The long-term management framework should provide means for the RRS-CM to verify the source of the TAD.
  - The long-term management framework should provide means for the RRS-CM to verify that the TAD applies to its source.
  - The long-term management framework should provide means to avoid circular transfer of authority.
  - The long-term management framework should provide means to prevent an RRS-CA from transferring its authority more than once.
  - The long-term management framework should provide means to prevent the RE from accepting a TAD that does not originate from the current RRS-CA.

At the level of RRS-CP Profile management:

- Integrity:
  - The long-term management framework should provide means for the RRS-CM to verify the integrity of the RRS-CP Profile at receipt.

- Authenticity:
  - The long-term management framework should provide means for the RRS-CM to verify the source of the RRS-CP.

At the level of RRS Configuration Profile Management:

- Integrity:
  - The long-term management framework should provide means for the RRS-CM to verify the integrity of the RRS Configuration Profile at receipt.
- Authenticity:
  - The long-term management framework should provide means for the RRS-CM to verify the source of the RRS Configuration Profile.

NOTE: No objectives related to accountability are given, as accountability is built-in into the design of the TAD.

11.7 Threats and limitations

The following threats have been identified for the long-term management framework.

Table 13: threats to security objectives for the long-term management framework

Objective class	Threat class	Notes
confidentiality	eavesdropping	Signalling information as well as device status information could be observed and leveraged to build further attacks. In particular, the content of the RRS Configuration Profile and the RRS-CP Profile could provide valuable information to an attacker.
	traffic analysis	Changes in traffic patterns may allow to infer ongoing activities
	fingerprinting & tracking	Interaction with the RE at the level of the RRS-CM, or eavesdropping could be used to gather information for the purpose of fingerprinting the RE (device type, device status) which, when combined with other information, may be used to uniquely identify and track the device. A consequence of illegitimate tracking is the compromise of the user's privacy.
integrity	data modification	A command or response message, a profile, or a TAD is modified on the fly.
	spoofing	Illegitimate command or response messages are injected.
	malicious input	A malformed message allows an adversary to cause malfunction or take control of the RE.
	replay	A previously processed, valid TAD, RRS Configuration Profile, or RRS-CP Profile that has been superseded by a newer version, is being pushed to the RE. Similar threats exist for messages exchanged between the RRS-CA and the RRS-CP.
authentication/identity	masquerading	A third-party pretends to be a legitimate actor to the framework (an RRS-CA or RRS-CP).
	unauthorized access	A specific message, sequence of messages or environmental conditions cause the authorization step on the RRS-CA, RRS-CP, or RRS-CM to be bypassed.

There are a number of threats to the authentication/identity class of security objectives that are specific to the nature of the long-term management framework:

- There is a risk that secrets from the OEM Key Management System or from the RRS-CA may leak after these have phased out of their authority over RE configuration management. For example, this can happen if the secrets are not properly destroyed after a facility is decommissioned. When an adversary obtains the secrets, they can set up an RRS-CA that would appear as legitimate and thus hijack the control of the RRS Platform of relying REs. This threat is mitigated through security objectives pertaining to the management of TAD in clause 11.5.

- Following the previous statement, there is a risk that the RE becomes desynchronized from the latest valid RRS-CA, giving a window of opportunity for an attacker to push a TAD of its own design to the RE (this requires that the attacker also has obtained the secrets of the previous RRS-CA). This can happen when the RE is not active for an extended period. This is a clear limitation of the long-term management framework, which is more suitable for devices that are permanently (or regularly) connected, than for devices that may be seldom activated.

- As the security of cryptographic primitives can only diminish over time there is a risk that progress in cryptanalysis will render old implementations of the long-term management framework insecure so that an attacker can easily pretend e.g. to be the currently valid RRS-CA of an old RE and issue malicious RRS-CP Profiles. The RE should be decommissioned.

- The security of the framework partially relies on the behaviour and security of the RRS-CA. If the RE current RRS-CA issues a TAD to a malicious RRS-CA, then there is now possibility to correct the situation beyond forcing the malicious RRS-CA to issue a TAD to a legitimate one. The use of a master TAD to reset the TAD chain of trust, for example, would defeat the purpose of locking the RE to the current RRS-CA.

12 Device root of trust for RRS

12.1 Introduction

A device root of trust is made of hardware and software components that are inherently trusted to provide security services. Although these services could in turn be used as building blocks for higher-level security mechanisms on the device, the primary purpose of the root of trust is to establish the trustworthiness of the overall platform and software, or of a specific component thereof.

The root of trust should be secure by design and, on devices, implement hardware security measures. A key characteristic that all root of trust provide is resistance to tampering.

Several methods are available to implement a root of trust. The TPM [i.28] provides many of the security services detailed in the following clauses, and more, in a standardized manner, but these may as well be achieved with a secure element providing a fully isolated execution environment. How the root of trust is implemented depends on the result of the cost-risk analysis for a specific device in a given market environment, and remains the responsibility of the device manufacturer. Indeed, the root of trust could be implemented as a discrete TPM or a secure element, or as a software implementation running in a protected environment of the host CPU (among other possibilities). Each option provides a different level of security assurance but also bears different costs. The focus of the present document is to identify the security services that can be beneficial to RRS security rather than to mandate a specific root of trust implementation.

In the context of RRS the location of the root of trust depends on the relationship between the host hardware platform and the RRS Platform. The RRS Platform may have its own root of trust or may depend on the host platform to assert its trustworthiness. The following architectural variants are possible:

a) The RRS Platform is integrated with the host hardware platform (e.g. as a component of a System-On-Chip). The RRS Platform and the host platform share the same root of trust.

b) The RRS Platform is an independent entity on the host platform, in which case the two may initialize independently during the boot process.

c) The RRS Platform is a separate entity from the host platform (e.g. it resides on a USB dongle or an SD card).

While from the device manufacturer's perspective the overall trustworthiness of the device matters, from the perspective of RRS (in particular regarding compliance to the RED [i.14] and other regulatory frameworks) the core concern is the trustworthiness of the RRS Platform as a prerequisite to secure and compliant behaviour of Radio Applications. This aspect is essential regardless of what constitutes the RE - that is, whether the RE is composed of the RRS Platform only, or of the combination of the host platform and the RRS platform.

Some of the services that can be provided by a root of trust are detailed in clause 12.2.

12.2 Services

12.2.1 Immutable pre-provisioned data

For hardware roots of trust this is data that is embedded in the hardware and thus cannot be modified. It can be implemented as memory cells or registers that are rendered read-only via electronic fuses, for example. Typical immutable data are public keys used for the verification of a digital signature, and device identifiers. Such data may be publicly available from the root of trust unless the disclosure of such could lead to security or privacy concerns.

In the case of RRS a good candidate for immutable data at the hardware level is the RRS Platform ID.

12.2.2 Measurement

Measurement is the ability of the root of trust to evaluate the content of specific memory locations, containing e.g. device firmware, or critical configuration registers. For the measurement to be trustworthy, a trusted means is needed by the root of trust to read the content of the memory location - such as a protected bus. The result of the measurement operation is typically a fingerprint of the content, obtained by applying a cryptographically secure hash algorithm or a keyed-hash message authentication code (HMAC), depending on how the measurement should be validated.

In the case of RRS, a good candidate for measurement by the root of trust is the RRS Platform firmware (understood as the set of software components necessary to run the CSL, the RCF, and the Radio Computer).

NOTE: The measurement feature of the root of trust could also support the verification of the integrity and origin of the RAs, the DoC, the RE Configuration Policy, RE Mobility Policies, and other assets (as with a TPM, for example). This can alternatively be done by a software component that would have been verified through the secure boot process.

12.2.3 Secure cryptographic primitives and execution environment

By design, the root of trust provides its own set of securely implemented cryptographic primitives that will support its operations (such as hashes, digital signature, encryption/decryption, and so forth). The implementation provides tamper-resistance and prevents leakage of secrets (e.g. be resistant against key extraction attacks such a Differential Power Analysis).

The root of trust may embed a cryptographic accelerator that can be used by other components of the system (such as user-space software). The advantage of this approach is that application developers are provided with certified implementations of cryptographic primitives. However, for costs reasons (as is common with a TPM) no cryptographic acceleration may be provided.

NOTE: This clause is provided for information only as it is the RRS Platform manufacturer's responsibility to implement the cryptographic primitives required by the root of trust.

12.2.4 Secure boot

This service builds on those previously described and provides security and compliance assurance about the boot process of a platform by allowing for the verification and protection of key software components, starting with the boot image (e.g. boot block and firmware). The boot image is usually composed of software, filesystem and configuration data. Secure boot comes in two variants, which can be combined:

- Authenticated boot ensures that only software of appropriate origin can be loaded on the platform, and it normally also provides integrity protection. This ensure that a given platform will boot in an intended state, using software presenting intended behaviour, as asserted by the entity that verified and signed the software.

- Encrypted boot provides confidentiality protection and is used to mitigate the risks related to reverse engineering and leakage of industrial secrets. Typically, the encrypted software is first loaded into a trusted execution environment (e.g. providing isolation from user space and countermeasures against hardware attacks) before being decrypted and executed.

In the context of RRS, authenticated boot is of primary importance since the RRS Platform firmware is critical to the integrity and compliant behaviour of Radio Applications - this naturally does not preclude other solutions, such a hardware-based limitations of the radio front-end. Encrypted boot remains interesting to manufacturers wishing to protect their intellectual property. However encrypted boot is usually more difficult to implement than authenticated boot. While authenticated boot can rely on asymmetric cryptography (digital signature) with the public key being embedded in the hardware root of trust and common to a large number of devices (e.g. all devices of the same type or of the same generation), encrypted boot relies on a shared secret and depends on the secret not to leak. In order to mitigate the risk of key extraction attacks, such shared secret should be limited to a small group of devices or even be unique per device. This increases the complexity of software image generation and distribution.

Authenticated boot is not limited to the boot block and device firmware and can be arbitrarily extended to higher software layers such as the host Operating System or user space applications (that is, it can be extended from the boot phase to the runtime phase), as each element in the boot chain validates the next one, forming a chain of trust that originates from the hardware root of trust. This is also valid for Radio Applications: a verified RRS Platform firmware can be trusted to verify the integrity and origin of Radio Applications as well as their applicability to the RRS Platform based on the RE Configuration Policy.

The exact scope of authenticated boot depends on the architectural choices presented in clause 12.1:

- the secure boot is initiated by the host platform and covers the RRS Platform firmware in a linear manner; or
- the secure boot is initiated by the host platform and branches at some point to the RRS Platform; or
- two secure boot processes are running independently on the host platform and the RRS Platform (possibly at different times, for example when the RRS Platform is a USB dongle that is inserted in a port on the host platform).

12.2.5 Secure storage

Secure storage covers different aspect of protected memory for runtime data generated by applications or the root of trust itself, in order to provide guarantees on:

- Data confidentiality:
  - resistance against data extraction attacks;
  - access control mechanisms in order to prevent access by an illegitimate application;
  - resistance against brute force attacks (e.g. for passwords).
- Data integrity:
  - access control mechanisms preventing modifications by an illegitimate application;
  - persistence over power cycles with non-volatile memory;
  - resistance against modification and deletion attempts (hardware attacks).

Data confidentiality is essential for device credentials, private keys and shared secrets. This is the case in RRS for RE credentials in the identity management framework and secrets protecting access to the RRS Platform (such as an administrator password).

In RRS data integrity and non-volatility are of primary importance for trust anchors related to authentication of remote entities as per the identity management framework (OEM, CCE, Software Manufacturer, RadioApp Store, regulatory actors and so forth), fingerprints of installed Radio Applications, device identities, or RAT identities (IMEI, MAC address).

Secure storage can be leveraged to create protected data stores outside the root of trust, by protecting (wrapping) the data with a key that resides within the secure store. This provides a way to extend secure storage capabilities, although the data that remains outside the secure store does not benefit from the same level of protection against deletion. In the case of RRS, protected data stores can be used to handle data that is temporary or can be regenerated.

More specialized types of non-volatile memory may also be provided, that prevent rollbacks, such as:

- Monotonic counters:
  - these counters can only increase in value.
- Secure bitfields:
  - these bitfields are initialized to 0 but once a bit is set, it cannot be cleared. When a bit set is associated with a given action or state, information about the action or state cannot be deleted (forgotten).
- Hash-extend registers:
  - one way registers for which the effective value is a hash of the old value concatenated with a new input value, as follow: A ← hash (original A || B). Platform Configuration Registers (PCR) in TPM are hash-extend registers.

In RRS the following information could benefit from monotonic counters in secure storage: number of RRS platform reboot, number of installation for a given RAP ID, number of update for a given RAP ID, version of the last installed RE Configuration Policy.

To illustrate the importance of secure storage for the RRS Platform, the following operational scenarios should be considered:

a) the RRS Platform is a separate logical entity from the host platform, both the RRS Platform firmware and the Radio Applications reside on the RRS hardware platform; or

b) the RRS Platform firmware is loaded from the host platform, the Radio Applications reside on the RRS Platform; or

c) the RRS Platform firmware resides on the RRS Platform, the Radio Applications are provided by the host platform; or

d) both the RRS Platform firmware and the Radio Applications are provided by the host platform.

Operational scenario #4 implies that the RE can be reset by the host platform each time it is activated and thus the RRS Platform is also provided the DoC and RE Configuration Policy by the host platform. In such situation, the RRS Platform would not be able to securely keep track of the RE Configuration Policy version without a secure monotonic counter in non-volatile storage. Thus, the RRS Platform assumes that only the current RE Configuration Policy or an RE Configuration Policy that is newer than the last used one is valid. This is because the RRS Platform cannot know the reason why a RE Configuration Policy has been updated. In particular, it could have been updated because an RA previously thought to be compliant to the regulatory framework would in fact not be (after a second conformance test of because of a newly discovered bug). When the RRS Platform has no means to keep track of the RE Configuration Policy version there is a risk that it runs non-compliant Radio Applications even though all other security checks have passed.

Another requirement concerns permanent RAT identities once the corresponding Radio Application has been installed on the RE, which should not change between RA update or installation and deinstallation cycles. An example is the IMEI for 3GPP RATs, which is required to be immutable by the GSMA and may also be critical for law enforcement (such as for Lawful Interception and recovery of stolen devices). Sticking to the example of 3GPP this would require that the IMEI be managed outside of the RA. One way to comply with this immutability requirement is to reserve a permanent area in secure storage in which the IMEI is configured (via an API available to the Administrator in the CSL). This action would furthermore be marked with a secure bitfield. Together with the authenticated boot mechanism covering the Administrator (as part of the RRS Platform firmware) and the authentication of the RA originator, guarantees can be given that the IMEI will be configured from the first installation of a 3GPP RAT and then remain immutable.

When the secure storage is provided by a TPM, there exists a mechanism called sealing by which specific key and data may only be released when the platform is in a pre-determined state (as given by expected values of relevant PCRs). For example, in RRS:

- the credentials proving the RE identity may not be available to the RRS Platform firmware if the measurement history does not match the value stored in the PCR (in other words, that the firmware is not an approved version);

- the IMEI may not be released to an RA that is not proven to be an RA that depends on the IMEI.

12.2.6 Policy-based access control

The root of trust may provide access control to secure storage based on policies requiring a specific internal state of the root of trust (e.g. internal registers), environmental information, as well as interactions with the root of trust (such as authentication). While it may come with build-in access control policies, the strength of the mechanism lies in the ability of external applications to define policies for the data they save in secure storage. In order to later access the data, the application proves to the root of trust that the policy is satisfied.

The sealing operation described in the previous clause is an example of policy-based access control. As explained previously specific parameters may only be released to the legitimate Radio Application. Policy-based access control may also be leveraged as part of the configuration enforcement and the long-term management framework in RRS.

12.2.7 Random number generation

Some security operations of the root of trust, such as key generation, require high quality random numbers. This implies that the random subsystem can gather enough entropy. For this purpose, a True Random Number Generator (TRNG) may be added to the root of trust. It is then possible to make the TRNG available to other components of the platform, e.g. a device driver to seed the Cryptographically Secure Pseudo-Random Number Generator (CSPRNG) of the host operating system.

While there is no parameter at the level of the RRS specification that depends on high-quality random numbers, it may still be necessary to provide a generator to the RRS Platform for ephemeral secrets and intermediate keys, and to the implementation itself e.g. for memory layout randomization. The threat here is that procedures that require unpredictability may become predictable when the source of randomness is weak.

12.2.8 Trusted time

The root of trust can provide internal timers as well as a clock that can be used for timestamping purposes (e.g. audit) and the evaluation of access policies. The root of trust can provide guarantees on the clock drift, and that timers can only move forward. In RRS a trusted time source is important on the RE for accounting purpose and non-repudiation.

12.2.9 Trusted environmental information

When the root of trust is securely interfaced with other sensors, i.e. the data can be proven to come from a trusted sensor (e.g. by means of asymmetric cryptography), then environmental data can be used in policy assertions and management of sealed secrets. Example of environmental data are the location, temperature, time, presence of other devices, and biometric identification.

In the context of RRS the RE location (as provided by a GNSS or cell ID) can be used to unlock a particular mobility policy.

12.2.10 Audit

In the general sense audit is the ability to securely keep track of events and previously performed actions. The root of trust can provide the security services that are necessary to guarantee the integrity and authenticity of the audit log.

While RRS provides a non-repudiation framework it can be complemented on the RE by an audit log capability for key operations (such as a firmware update, change in RA status, DoC and RE Configuration Policy update, or modification of configuration parameters and trusted network entities) and events (such as security indicators).

12.2.11 Mutual authentication and secure communications between entities

The cryptographic, measurement and secure storage capabilities of root of trusts can be leveraged to allow authentication or mutual authentication of other hardware components. This helps asserting the composition of the overall hardware platform and prevent modifications that could be malicious or detrimental to the platform behaviour.

When the host platform authenticates an RRS Platform (architectural variants 2 and 3 in clause 12.1), then it can assert whether the resulting RE will conform to regulatory requirements of the RED [i.14] as stated in the DoC. RRS Platform authentication may thus be mandatory when the host platform bears the responsibility of compliance to the RED.

Authentication (or mutual authentication) can also take place between the root of trust and logical entities on the host platform or over the network, and can be complemented with communication security. This provides a higher level of security assurance for the completion of sensitive operations between trusted peers over untrusted networks and platforms. For RRS this is the case with configuration enforcement messages related to disturbance control.

12.2.12 (remote) Attestation of platform configuration

When the root of trust is able to measure the status of hardware and software components in a trustworthy manner, and can keep track of events in the system (through automated measurements, audit logs, or interaction of other entities with the root of trust), then this information can be reported to a legitimate third-party. Attestation of platform configuration is addressed in clause 9.

Annex A: Impact on RRS Security of European Radio Equipment Directive

A.1 Introduction

The European Directive 2014/53/EU (RED) [i.14] contains a number of requirements applicable to Reconfigurable Radio Systems (RRS). The present annex highlights and summarizes those requirements that may have an impact on RRS security, provides related considerations, and illustrates the relationships between various items.

NOTE: Some articles in the RED [i.14] require the adoption of a corresponding Delegated Act in order to come into force. The considerations in this annex are provided as if such Delegated Acts had been adopted.

A.2 Summary of applicable requirements

A.2.1 Applicability

Article 1.3 excludes applicability to "*radio equipment exclusively used for activities concerning public security, defence, State security, including the economic well-being of the State in the case of activities pertaining to State security matters, and the activities of the State in the area of criminal law*".

Article 2.1.1 defines radio equipment as:

- electrical or electronic product, which intentionally emits and/or receives radio waves:
  - for the purpose of radio communication;
  - or for the purpose of radio determination (determination of position, velocity, etc.).

NOTE: This includes products that have to be completed with an accessory (e.g. antenna) in order to operate.

A.2.2 General principles

Article 4.1 defines the essential requirement that:

- compliance applies for the radio equipment and its software;
- compliance assessment and statement of compliance apply to a specific combination of radio equipment and software.

Article 3.3 provides a number of compliance requirements:

- (d) radio equipment does not harm the network or its functioning nor misuse network resources, thereby causing an unacceptable degradation of service;
- (e) radio equipment incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected;
- (f) radio equipment supports certain features ensuring protection from fraud;
- (g) radio equipment supports certain features ensuring access to emergency services;
- (h) radio equipment supports certain features in order to facilitate its use by users with a disability;

- (i) radio equipment supports certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated.

Article 3.2 provides expectations that the radio equipment makes efficient use of radio resources and avoids harmful interference (interpreted here as harmful to the efficient use of the radio spectrum).

Article 3.1 provides two essential requirements for radio equipment:

- (a) the protection of health and safety of persons and of domestic animals and the protection of property, including the objectives with respect to safety requirements set out in Directive 2014/35/EU [i.15], but with no voltage limit applying;
- (b) an adequate level of electromagnetic compatibility as set out in Directive 2014/30/EU [i.16].

A.2.3 Technical and security considerations

Any solution allowing reconfiguration of RE by means of updates to its operational software, and that as a consequence may lead to hardware reconfiguration, has to have means to prevent RE misbehaviour and related consequences on health, safety and spectrum efficiency. This does not only mean that RAP is to be carefully crafted, but that measures should be in place to prevent installation of malicious RAP as well as modification at rest and runtime of installed RAP.

A.3 Declaration of Conformity (DoC)

A.3.1 Introduction

Two variants are available:

- (Annex VII, parent article 10.9) simplified version, containing:
  - a simple declaration statement;
  - an *internet address* pointing to the complete declaration of conformity.

Article 10.9 provisions the possibility for the manufacturer to use a simplified DoC:

- (Annex VI) normal version, containing information on:
  - radio equipment (product, type, batch or serial number);
  - name and address of the manufacturer or his authorized representative;
  - object of the declaration and relevant legislations (e.g. but not only, the RED);
  - references to the relevant harmonised standards or to the related technical specifications;
  - information on - and actions performed by - a notified body;
  - information on HW and SW components allowing the RE to operate as intended and covered be the DoC;
  - place and date of issue, signatory, signature.

The DoC is *also* to be provided along with the RE technical documentation (annex V, clause (e)), this information is to be registered on a central system provided by the Commission (article 5.4).

A.3.2 Technical and security considerations

Protection of the DoC in digital or paper form within the central system provided by the Commission is obviously out of scope of the present document. However, if a specific format is to be chosen there may be a race condition as to who decides on the format.

In case of simplified DoC there is a needs to guarantee that the complete DoC is legitimate, that is to say that the combination of the simplified and the referenced DoCs can be verified as legitimate.

A.4 Safekeeping of the Declaration of Conformity

A.4.1 Introduction

In all cases of conformity assessment, the manufacturer keeps a of copy of the DoC, and make it available, for a period of 10 years after the equipment has been placed on the market (article 10.4):

- Module H/annex IV (conformity based on Full Quality Assurance with quality system audited by a notified body), article 5.2:
  - Article 6 requires other documents be similarly kept safe (technical documentations, QA documentation and changes, decisions of the notified body).
- Module C/annex III (conformity of type based on internal production control), article 3.2:
  - Module B/annex III (EU-type validation), article 9, requires the EU-type examination certificate be similarly kept safe.
- Module A/annex II (conformity based on internal production control), article 4.2.

Module B, article 6 describes the content of the EU-type examination certificate:

- name and address of the manufacturer;
- conclusions of the examination, the aspects of the essential requirements covered by the examination, the conditions (if any) for its validity and the necessary data for identification of the assessed type. The EU-type examination certificate may have one or more annexes attached;
- all relevant information to allow the conformity of manufactured radio equipment with the examined type to be evaluated and to allow for in-service control.

Other economic operators should keep a copy of the DoC and make it available (article 15), in particular importers (article 12.8).

Distributors play a critical role in non-compliant RE detection (article 13.4) and in being able to recover information about RE distributed on a given market (article 13.5). Consideration (37) mentions the importance of traceability.

A.4.2 Technical and security considerations

DoC safekeeping implies measures be taken by the manufacturer (and other economic operators) such as storage (DoC in paper form) or backup policies (for DoC in digital form). As detailed later in this annex, several DoC may apply in the lifetime of an RE because of versioning, depending on the DoC method selected and the hardware/software combination. Multiple economic operators may hold a copy of a DoC for the same RE, thus means are needed in order to guarantee that copies remain identical to the original for any given DoC.

The requirement for traceability highlights the importance of the DoC in identifying the liable party. This implies, if a DoC in digital form is used, that it provides at least the same level of confidence and availability as the DoC in paper form.

A.5 Affixing of Declaration of Conformity

A.5.1 Overview

Article 2.1.26 provides the definition of CE marking:

- "*'CE marking' means a marking by which the manufacturer indicates that the radio equipment is in conformity with the applicable requirements set out in Union harmonisation legislation providing for its affixing.*"

Module H, Module C, and Module A all refer to articles 19 and 20 as the requirements for affixing of the CE marking.

Article 19 points to Article 30 of Regulation (EC) No 765/2008 [i.17] for the general principles of CE marking.

Article 20 provides rules and conditions for affixing the CE marking:

- on the RE or its data plate, on the packaging;
- followed by the number of the notified body in case of Module H.

Article 18.2 requires that the DoC and its simplified version be translated in languages required by member states, and continuously updated (to be understood as an update following a reconfiguration). Consideration (16) requires that loading (new) software on the radio equipment do not compromise compliance, however Consideration (19) warns that the verification by the radio equipment of its compliance in combination with a software should not be abused in order to prevent use of software provided by third parties.

Article 18.3 requires that a single DoC be provided that covers all the Union acts relevant to the RE.

Consideration (47) mentions the possibility for the CE marking, DoC and other required information not to be affixed but to be provided on the display of the radio equipment, upon request from the equipment user.

A.5.2 Technical and security considerations

The fact that the CE marking and DoC could be provided on the display of the radio equipment means that they will be stored in the RE memory. Provisions will be required to prevent tampering of such information from the user or an adversary. When properly designed and secured digital marking may provide better assurance than its physical counterpart.

The requirement for the DoC to be updated brings the topic of DoC versioning - not in the sense that the DoC has a version number, but in the sense that the DoC is bound to given hardware and software versions (or ranges thereof). In that case such information would need to be integrity protected.

Regardless of the digital format selected for the DoC, an aggregation step will happen before the DoC is distributed with/to the RE. Security solutions designed to protect the integrity and trustworthiness of the DoC will depend on the number of actors involved in such endeavour and their respective responsibility (consider e.g. notification and assessment bodies). For example, prior to the aggregation each part of the DoC could be subject to cryptographic signatures from different actors - each possibly depending on its own trust anchor.

How does the RE determine compliance in combination with a software? Several methods exist for this purpose and are provided for informative purpose only:

- The RAP metadata contain a statement that the embedded RA can run on the hardware of the RE and, when run, the combination of hardware and RA will remain compliant. In other words, the RE fully trusts a third party for this purpose (e.g. the RAP provider).
- The RAP metadata contain a list of required hardware capabilities and a statement that hardware supporting the required capabilities will be compliant. Here again the RE trusts a third party, but is also entrusted with a capability verification step before installing the RA.
- Without any information available in the metadata, the RE determines that the RA is legitimate (e.g. by way of signature verification) and determines by itself whether the resulting hardware and software combination is compliant. This could be done by code analysis or via and out-of-band request to the network.

Regardless of the method used it is quite clear that there is a need to protect the RAP as a whole (RA and metadata).

A.6 Pre-market actors and roles from the Directive 2014/53/EU perspective

Pre-market consideration in the RED [i.14] focus on certification and the establishment of a Declaration of Conformity. The top-level actor is the notifying authority, which is responsible for notifying and monitoring so-called conformity assessment bodies, also known as notified bodies (article 23). Notified bodies have a duty of informing the notifying authority of matters such as refusal of EU-type examination certificate and of quality system approval, and requests from market surveillance authorities. They also have an obligation to share information with other notified bodies (article 36). Note that the market surveillance authority is not a pre-market actor.

The notified bodies should not be confused with the market surveillance authorities. Notified bodies provide conformity assessment while market surveillance authorities monitor the market for non-compliance and device presenting risks, such activities being yet again different from disturbance control.

There exist three methods of conformity assessment, each with a specific set of actors:

- Module A (annex II), Internal production control:
  - With this method the manufacturer is the sole entity responsible for assessing the conformity of a radio equipment and providing a copy of the declaration of conformity to relevant authorities.
- Modules B and C (annex III), EU-type examination and Conformity to type based on internal production control:
  - With this method the notified body examines the technical design of a radio equipment and assesses the adequacy of said technical design. When the assessment is positive the notified body provides the manufacturer with a EU-type examination certificate. The manufacturer and notified body have an obligation to inform each other of matters that may render the examination certificate invalid. The notified body informs the notifying authority of its activities, and other notified bodies of refused examination certificates.
  - Having the EU-type examination certificate the manufacturer assesses conformity of the radio equipment in accordance with the information present in the examination certificate and its internal production control.
- Module H (annex IV), Conformity based on full quality assurance:
  - With this method the manufacturer is the sole entity responsible for assessing the conformity of a radio equipment, provided the manufacturer operates on an approved quality system. The notified body assesses said quality system and is tasked with the surveillance of the manufacturer with regard to proper implementation. The notified body has an obligation inform other notified bodies and the notifying authority of issues related to the quality system of the manufacturer.

From the point of view of the Reconfigurable Equipment, in all three methods the manufacturer is the sole actor that effectively vouches for the validity of the DoC.

NOTE: Modules A, B, and C are also applicable for assessment of electromagnetic compatibility (Directive 2014/30/EU [i.16]). Module A is also applicable for assessment of safety of electric equipment (Directive 2014/35/EU [i.15]).

A.7 Other information to indicate on the RE

A.7.1 Introduction

Article 10.7 mentions:

1) manufacturer name, registered trade name or registered trade mark;

2) postal address at which they can be contacted (single contact point);

3) where the size or nature of radio equipment does not allow it, on its packaging, or in a document accompanying the radio equipment.

Article 10.6 mentions:

- RE type, batch or serial number or other element allowing its identification.

A.7.2 Technical and security considerations

DoCs are not the only piece of information that will require protection from tampering on the RE. Solutions designed in the context of RRS should take into account existing (deployed) solutions and the fact that protection from tampering will be a shared security function on the RE.

A.8 Actions in case of formal non-compliance, or with compliant radio equipment that presents a risk

A.8.1 Introduction

Article 43.1 provides administrative reasons for formal non-compliance (this does not cover RE misbehaviour).

Article 43.2 describes potential actions in case of non-formal compliance:

- "*Where the non-compliance referred to in paragraph 1 persists, the Member State concerned shall take all appropriate measures to restrict or prohibit corresponding radio equipment being made available on the market or ensure that it is withdrawn or recalled from the market.*"

Article 42 covers compliant equipment that presents a risk:

- "*[...] the relevant economic operator to take all appropriate measures to ensure that the radio equipment concerned, when placed on the market, no longer presents that risk, to withdraw the radio equipment from the market or to recall it within a reasonable period, commensurate with the nature of the risk, as it may prescribe.*"

A.8.2 Technical and security considerations

It should be noted that Reconfigurable Radio Systems have the capability to go beyond the requirements formulated in the RED [i.14], should the following provisioned use cases be given adequate solutions:

- "*Certificate Verification of reconfigurable equipment*", [i.17]:
  - In this use case, the requestor queries the RE for its certificate of conformity and verifies it. When such procedure happens over the network, this is a case of remote attestation.

- "*Configuration enforcement of reconfigurable equipment*", [i.17]:
  - In this use case the NRA (or another body) signals the RE to cease its operation after improper operation has been detected. This may take the form of a complete switch-off of reverting to a previous configuration (i.e. removing a newly installed RA or reverting to a previous version).

The following supported uses cases of [i.17] also help fulfilling these requirements:

- "*OEM Upgrade (individual or en-masse)*".
- "*Third Party reconfiguration (individual or en-masse)*".

For these features to have any value the signalling from the network to the RE should be protected against various forms of abuse. The case of remote attestation is to be given due consideration in order to ensure that the RE response is trustworthy.

A.9 Post-market actors and roles from the RED perspective

In order to identify the post-market actors and roles two different situations should be considered:

- Recertification of the RE after an update, in which case the considerations regarding the pre-market actors apply to the DoC and can be extended to RAP, since they are the cause for the recertification. A software provider or a third-party may replace the manufacturer in this role.
- Configuration enforcement.

In the latter case, a market surveillance authority, maybe the NRA, plays a monitoring and decision role. In its monitoring role the market surveillance authority may perform the monitoring on its own resources or delegate it to other economic operators, such as OEM or Service Providers. When the Reconfigurable Equipment presents a risk the market surveillance authority informs the notified body.

The decision role is of relevance to the RRS architecture. It should be noted that economic operators (Service Providers, Distributors, OEM, and so forth) are expected to take action on their own initiative, and that the market surveillance authority is only expected to act as a last resort (see clause A.10). Thus the RE will have to trust several entities to provide legitimate signalling related to configuration enforcement.

This complexity can be simplified if an intermediate entity is set to act as a proxy between the RE and the economic operators. In that case the set of entities the RE needs to trust is reduced to one. Responsibility of the proxy could be assigned, for example, to the entity that acts as the single point of liability for the RE, or to the entity that is responsible for software upgrade on the device.

If configuration enforcement dictates a modification to the set of RA installed on the RE, the RadioApp Store will be involved.

A.10 Actions in case of RE presenting a risk

A.10.1 Introduction

Article 40 covers the case where the market surveillance authorities have reason to believe that the RE presents a risk to health or safety:

- (article 40.1) an evaluation of the RE is conducted w.r.t. the RED, if non-compliance is found, actions are taken:
  - bring the RE into compliance; or
  - withdraw the RE from the market; or

- recall the RE;
- these action may be done by the market surveillance authority in case of failure of the concerned economic operators (article 40.4).

A.10.2 Technical and security considerations

Same considerations as in previous clause apply.

A.10.3 Additional considerations

Article 15(3) and Articles 16 to 30 of Regulation (EC) No 765/2008 [i.17] have been covered as part of this analysis, as well as conformity modules of European Directives 2014/30/EU [i.16] and 2014/35/EU [i.15].

Annex B:
Summary of security objectives

Table B.1 is a collation of each objective described in the main body of the present document.

NOTE: Table B.1 has been built by using cross references to bookmarked text in the main body of the present document.

Table B.1: Collation of security objectives to be met by RRS

Id	Text of objective	Affected stakeholder or asset	Intervention level
1	The RRS platform should provide means to ensure that the content of communication between the RadioApp Store and the RE are protected from exposure to unauthorized 3rd parties		Technical
2	The RRS platform should provide means to verify that the content of communication between the RadioApp Store and RE has not been manipulated prior to processing at receipt		Technical
3	The RRS platform should provide means for the RadioApp Store to verify the identity of the RE		Technical
4	The RRS platform should provide means for the RE to verify the identity of the RadioApp Store.		Technical
5	The RRS platform should provide means to detect and prevent denial of access to the communications channel between the RadioApp Store and the RE		Technical
6	The RRS platform should provide means to verify that the RAP has not been modified between having been made available by the RAP originator and having been downloaded on the RE		Technical
7	The RRS platform should provide means for the RE to verify the source of the content supplied via the RadioApp Store		Technical
8	The RRS platform should provide means to prevent the RadioApp Store denying provision of an App to the RE		Technical
9	The RRS platform should provide means to prevent the RE denying receipt of an RA from the RadioApp Store.		Technical
10	The RRS platform should provide means to prevent the RE denying installation of an RA from the RadioApp Store		Technical
11	The RRS framework should ensure measures are provided to prevent installation of malicious RAPs		Technical
12	The RRS framework should ensure measures are provided to prevent modification of an RAP after installation		Technical
13	The RRS framework should provide means to verify the legitimacy of the Declaration of Conformity (DoC) and CE marking		Technical
14	The RRS platform should provide means to be able to uniquely identify the master copy of the DoC		Technical
15	Where CE marking and DoC are provided for display of the radio equipment by means of user interaction the RRS platform should provide means to assure that the marking is resistant to tampering		Technical
16	The RRS platform should provide means to validate data used to describe the installation requirements of the RAP (the RAP metadata) against the capabilities of the RE and prohibit installations where a mismatch is identified		Technical
17	The RRS platform should prevent an unauthorized third-party from determining that the DoC is being updated		Technical
18	The RRS platform should prevent an unauthorized third-party from determining that the complete DoC is being retrieved from a simplified DoC over the network		Technical
19	The RRS platform should provide means to prevent modification of the DoC apart from installation and update, in particular at rest		Technical
20	When the DoC is being updated, or the complete DoC is being retrieved, the RRS platform should allow integrity protection of said DoC while it is in-transit between the relevant entities in the network and components on the device		Technical
21	The RRS platform should prevent an unauthorized third-party to delete, install or otherwise alter a DoC on the RE		Technical

Id	Text of objective	Affected stakeholder or asset	Intervention level
22	When there is only a digital DoC and no paper DoC provided with the RE, the RRS platform should provide means towards tamper-resistance of the DoC at rest on the RE		Technical
23	When the complete DoC is requested over the network based on a simplified DoC residing on the RE, the RRS platform should provide means towards the availability of complete DoC to the RE		Technical
24	When the DoC is being updated, or the complete DoC is being retrieved, the RRS platform should allow for identification and authentication of relevant entities in the network and components on the device		Technical
25	The RRS platform should allow for authentication of content (DoC) to the relevant component on the device		Technical
26	When there is only a digital DoC and no paper DoC provided with the RE, the system should implement measure to ensure that the digital DoC provides at least the same level of confidence than the DoC in Paper form		Technical
27	The RRS platform should allow for the traceability of devices that have received an updated DoC		Technical
28	The RRS platform system should provide means to prove reception and installation of a DoC by a device		Technical
29	The RRS platform should allow for binding the DoC to the device that receives it		Technical
30	The RRS platform should allow for verifying that the presented DoC is bound to the device		Technical
31	The configuration enforcement framework should provide means to ensure that the command APDUs are protected from exposure to 3rd parties		Technical
32	The configuration enforcement framework should provide means to verify that the content of the command APDU has not been modified prior to processing at receipt		Technical
33	The configuration enforcement framework should provide means to protect against traffic manipulation		Technical
34	The configuration enforcement framework should ensure that malformed commands cannot compromise the proper operation of the RE		Technical
35	The configuration enforcement framework should provide means for the RE to verify the identity of a command originator, without the availability of a return channel		Technical
36	The configuration enforcement framework should provide means for a network entity to verify the identity of the RE		Technical
37	The configuration enforcement framework should not process control messages that have not been issued by an authorized entity		Technical
38	When the sensitivity of the command is high the configuration enforcement framework should provide means to prevent the related actor denying the transfer of such command		Technical
39	The long-term management framework should provide means to ensure that the content of the communications between the RRS-CA and the RRS-CP are protected from exposure to authorized 3rd party		Technical
40	The long-term management framework should provide means to ensure that the content of the communications between the RRS-CA and the RRS-CM are protected from exposure to authorized 3rd party		Technical
41	The long-term management framework should provide means to ensure that the content of the communications between the RRS-CP and the RRS-CM are protected from exposure to authorized 3rd party		Technical
42	The long-term management framework should provide means to ensure that the content of communications between the RRS-CA and the RRS-CP has not been manipulated prior to processing at receipt		Technical
43	The long-term management framework should provide means to ensure that the content of communications between the RRS-CA and the RRS-CM has not been manipulated prior to processing at receipt		Technical
44	The long-term management framework should provide means to ensure that the content of communications between the RRS-CP and the RRS-CM has not been manipulated prior to processing at receipt		Technical
45	The long-term management framework should provide means for the RRS-CA and RRS-CP to verify each other's identity		Technical
46	The long-term management framework should provide means for the RRS-CA and RRS-CM to verify each other's identity		Technical

Id	Text of objective	Affected stakeholder or asset	Intervention level
47	The long-term management framework should provide means for the RRS-CP and RRS-CM to verify each other's identity		Technical
48	The long-term management framework should provide means for the RRS-CM to verify the integrity of the TAD at receipt		Technical
49	The long-term management framework should provide means for the RRS-CM to verify the source of the TAD		Technical
50	The long-term management framework should provide means for the RRS-CM to verify that the TAD applies to its source		Technical
51	The long-term management framework should provide means to avoid circular transfer of authority		Technical
52	The long-term management framework should provide means to prevent an RRS-CA from transferring its authority more than once		Technical
52a	The long-term management framework should provide means to prevent the RE from accepting a TAD that does not originate from the current RRS-CA		Technical
53	The long-term management framework should provide means for the RRS-CM to verify the integrity of the RRS-CP Profile at receipt		Technical
54	The long-term management framework should provide means for the RRS-CM to verify the source of the RRS-CP		Technical
55	The long-term management framework should provide means for the RRS-CM to verify the integrity of the RRS Configuration Profile at receipt		Technical
56	The long-term management framework should provide means for the RRS-CM to verify the source of the RRS Configuration Profile		Technical

Annex C:
Summary of high level security requirements

A summary of the high-level requirements deriving from the present document is given in ETSI TS 103 436 [i.12], clause 4. Changes required in RRS are summarized in clause 8 of the present document.

Annex D:
Completed TVRA pro forma for RRS security

The pro forma is taken from ETSI TS 102 165-1 [i.9] and is used to capture the TVRA results.

Table D.1

A Security Environment		
a.1 Assumptions		
a.1.1	The RRS platform and the standards defining it do not define how the DoC is issued, this aspect is governed by the regulatory framework (Directive 2014/53/EU [i.14]).	*Citation for full text*
a.1.2	The RRS platform does not define the content of DoC attestations.	
a.1.3	For purposes of the detail requirements definition of security processes there is assumed to be a lower and upper bound on the performance of the RE (e.g. processor instructions per time period, memory capacity, memory access rate).	
a.1.4	The point of observation and control for verification of the RRS platform operating as a valid RE is identical to that for a non-RRS platform operating as a valid RE, e.g. a GSM-900 radio should not be distinguishable in any conformance test as being an RRS or non-RRS implementation.	
a.1.5	The RRS platform does not define the radio application but only defines how it is installed, updated, and how it interfaces to the RE.	
a.1.6	It is considered that at least the following models apply for reconfiguration of the RE: The RE manufacturer updates the device using the RRS capability to add functionality over the lifetime of the RE (this is somewhat analogous to a software developer extending the functionality of an application or operating system). The user is offered limited control over the configuration of its device, e.g. by being able to choose whether to install an RA implementing a specific RAT in a controlled environment; this may in the future evolve into a model whereby the end user of the radio chooses to extend the functionality of the RE by installing a Radio Application of their choice from a public store.	
a.1.7	Whilst there will be a communications network with associated network roles involved in the distribution of RRS apps and who will support REs that are RRS enabled it is assumed that the packaging of the app and the knowledge that a terminal is an RRS-RE is transparent and the network has only got a passive role in the RRS platform.	Clause 5.2
a.2 Assets		
a.2.1	*Short text describing asset*	*Citation for full text*
a.2.2		
a.3 Threat agents		
a.3.1	Natural or human disaster: In the context of this ToE, an external event that causes disruption of the communication channel service. Such disruption ranges from being with limited impact (e.g. temporary failure of one specific network service) to complete failure of the network or radio link (in particular from interferences) over an extended period of time. Cause could be natural (fire, earthquake, solar wind etc.) or human (e.g. mistake, riots, war).	*Citation for full text*
a.3.2	Malicious insider: from one economic actors involved with the network path (not only a network provider), a member of personnel with sufficient access privileges mounts an attack or leak information.	
a.3.3	External attacker: an attacker successfully compromises an element on the network path and uses this position to mount further attacks.	
a.3.4	Over-the-air attacker: an external attacker that possesses appropriate equipment to listen on the radio channels, jam or hijack communications.	
a.4 Threats		
a.4.1	*Short text describing threat*	*Citation for full text*
a.4.2		
a.5 Security policies (OPTIONAL)		
a.5.1	*Short text describing security policy*	*Citation for full text*

a.5.2		
B Security Objectives		
b.1 Security objectives for the asset		
b.1.1	*Short text describing objective for the asset*	*Citation for full text*
b.1.2		
b.2 Security objectives for the environment		
b.2.1	*Short text describing objective for the requirement*	*Citation for full text*
b.2.2		
C IT Security Requirements		
c.1 asset security requirements		
c.1.1 asset security functional requirements		
c.1.1.1	*Short text describing security functional requirement*	*Citation for full text*
c.1.1.2		
c.1.2 asset security assurance requirements		
c.1.2.1	*Short text describing security assurance requirement*	*Citation for full text*
c.1.2.2		
c.2 Environment security requirements (OPTIONAL)		
c.2.1	*Short text describing security environment requirement*	*Citation for full text*
c.2.2		
D Application notes (OPTIONAL)		
E Rationale		
The eTVRA should define the full rational, if this is true only a citation (reference) to the full text is required		

Annex E:
TVRA Risk Calculation for selected RRS aspects

The evaluation and calculation of the factors that affect the risks posed by particular threat groups (as defined in Steps 4, 5, 6 and 7 of the TVRA method) have been consolidated into a Microsoft Excel spreadsheet, TS102165_1_Risks.xls, contained in archive ts_10216501v040203p0.zip which accompanies ETSI TS 102 165-1 [i.9]. An example entry in this spreadsheet is shown in table E.1.

Table E.1: Initial risk for RRS with no security measures applied for DoC and RAP delivery

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
RAP delivery without test, validation, accountability	Time	≤ 1 day	0	No Rating	Likely	High	**Critical**
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Unnecessary	0				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
DoC delivery without validation, accountability	Time	≤ 1 day	0	No Rating	Likely	High	**Critical**
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Unnecessary	0				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
DoC manipulation	Time	≤ 1 day	0	No Rating	Likely	High	**Critical**
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Unnecessary	0				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
RAP manipulation	Time	≤ 1 day	0	No Rating	Likely	High	**Critical**
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Unnecessary	0				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
Masquerade as source of RAP	Time	≤ 1 day	0	No Rating	Likely	High	**Critical**
	Expertise	Layman	0				
	Knowledge	Public	0				

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
	Opportunity	Unnecessary	0				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
Falsified application of DoC to RRS-RE	Time	≤ 1 day	0	No Rating	Likely	High	**Critical**
	Expertise	Layman	0				
	Knowledge	Public	0				
	Opportunity	Unnecessary	0				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				

The analysis in the core of the present document suggests a number of strategies to protect the core aims of securing the RAP delivery by being able to verify the identity of the developer and the target RE. In addition the core of the present document identifies a strategy to counter concerns of accountability. The succeeding tables in this annex consider the threat scenarios from Table E.1 with the application of countermeasures. The principal finding of Table E.1 is that prior to the application of countermeasures the RRS system is at critical risk. The metric for critical risk defined in ETSI TS 102 165-1 [i.9] is stated as follows: "*The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker to implement the threat(s) is not high. Critical risks should be minimized with highest priority.*"

Table E.2: Modified risk for RRS with digital signature security measures applied for DoC and RAP delivery

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
RAP delivery via trusted channel (confidentiality, end-point authentication, integrity check)	Time	> 6 months	999	Beyond High	Unlikely	High	**Minor**
	Expertise	Expert	5				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
DoC delivery via trusted channel (confidentiality, end-point authentication, integrity check)	Time	> 6 months	999	Beyond High	Unlikely	High	**Minor**
	Expertise	Expert	5				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
DoC with integrity check function to counter manipulation	Time	> 6 months	999	Beyond High	Unlikely	High	**Minor**
	Expertise	Proficient	2				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
	Asset Impact	High	3				

Threat Group	Attack					Impact	Risk
	Factor	Range	Value	Potential	Likelihood		
	Intensity	Single instance	0				
RAP with integrity check function to counter manipulation	Time	> 6 months	999	Beyond High	Unlikely	High	**Minor**
	Expertise	Proficient	2				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
Masquerade as source of RAP prevention by cryptographic source authentication	Time	> 6 months	999	Beyond High	Unlikely	High	**Minor**
	Expertise	Expert	5				
	Knowledge	Public	0				
	Opportunity	Easy	1				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				
Falsified application of DoC to RRS-RE prevention by DoC binding to RE	Time	≤ 6 months	26	Beyond High	Unlikely	High	**Minor**
	Expertise	Proficient	2				
	Knowledge	Public	0				
	Opportunity	Difficult	12				
	Equipment	Standard	0				
	Asset Impact	High	3				
	Intensity	Single instance	0				

The analysis presented in table E.1 assumes that no protective measures are available, whereas table E.2 assumes that cryptographically strong countermeasures are deployed. Notwithstanding any advances in cryptanalysis it is broadly assumed that today's state of the art in cryptographic techniques makes any attack on cryptographically protected entities to be invulnerable to attack over a short time period (where short time period is considered by the metrics given in ETSI TS 102 165-1 [i.9] to be greater than 6 months).

Annex F:
Void

Annex G:
Trust models in RRS app deployment

G.1 Overview of trust

ETSI GS NFV-SEC 003 [i.22] provides a detail examination of the role of trust in a virtualized environment that has significant commonality with RRS. This annex is a simplified and re-targeted examination of the role of trust as introduced in [i.22] with a specific focus on the trust requirements for RRS.

Trust is defined as confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities.

Trust is highly dynamic and contextual, and may be described in assurance levels based on specific measures that identify when and how a relationship or transaction can be relied upon. Trust measures can combine a variety of assurance elements that include identity, attribution, attestation and non-repudiation.

Trust is a complex issue, but in many cases, the decisions that are required within a particular RRS deployment will be simple.

Some myths or commonly ignored features about trust:

- Having a secured communications channel with another entity is never sufficient reason to trust that entity, even if one trusts the underlying security primitives on which that communications channel is based.
- Trust is not a binary operation. There may be various levels of trust that an entity has for another.
- Trust may be relative, not absolute. Entity A may trust Entity C more than Entity B, without trusting either absolutely.
- Trust is rarely symmetric. Entity A may trust Entity B completely, whereas the amount of trust that B has for A may be very low. This does not always matter: a schoolchild may trust a schoolteacher, for instance, without any requirement for that trust to be reciprocated.
- One of the axes for trust is almost always time, and the trust relationship between two entities may be highly dynamic over time. Just because a certain level of trust was established at point T, it does not mean that that level will be maintained at time $T+\tau$, as it can increase and decrease.

As noted above, trust is defined as confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities. An entity A has no need to have a direct trust relationship with another entity B if B's operation has no direct impact on A. It may be that entity C is affected by entity B's operations, and that entity A relies on entity C, but this does not affect entity A directly, and therefore the trust relationship can be considered separate.

There are other occasions on which entity A may choose to trust entity B to some extent, based on the trust relationship which entity C has with entity B and the trust relationship which entity A has with entity C. This is a subtly different case, and is defined as transitive trust.

G.2 Role of trust in RRS

The role of trust in RRS is complex and depends on the trusting entity.

From a market surveillance perspective:

- The regulator (Market Surveillance Body, Disturbance Control Body) has to trust that the Declaration of Conformity has been correctly established for every device on the market.
- The regulator has to trust the Notified Body or the Compliance Contact Entity to properly and honestly assess compliance of a device to Union Acts.

NOTE: This only accounts for a simplified view of the assessment process since it is not the primary focus of the present document.

- The regulator (Market Surveillance Body, Disturbance Control Body) has to trust the veracity of the Declaration of Conformity that is retrieved on the device.

From a manufacturer perspective:

- The OEM has to trust the Software Manufacturer that they will provide legitimate Radio Applications.
- The Conformity Contact Entity has to trust the OEM and the Software Manufacturer to conduct proper testing of compliance.
- The Software Manufacturer has to trust the OEM in providing a reliable operating platform.
- The RAP Provider has to trust that the RE can maintain device and RRS assets integrity, and implement proper decision making based on RAP metadata.

From the user perspective:

- The RE user has to trust that his device will remain compliant, usable, and non-malicious.

From a distribution perspective:

- The RAP Provider has to trust the RadioApp Store to fulfil its role and to interact with the RE in a legitimate manner, but may not trust the RadioApp Store to safeguard the integrity of RAP.
- The DoC Provider has to trust the entity distributing the DoC to fulfil its role and to interact with the RE in a legitimate manner, but may not trust said entity to safeguard the integrity of the DoC.

From the device perspective:

- The Reconfigurable Equipment has to trust that the assets installed on his device from a 3rd party (the RAP or DoC Provider) will not attempt to bring the device in a non-compliant state or otherwise compromise it.
- The RE has to trust the DoC Provider to deliver a legitimate DoC.
- The RE has to trust the RAP Provider to deliver legitimate RAP.
- The RE has to trust the RadioApp Store to provide valid signalling.
- The RE has to trust the entity distributing the DoC to provide valid signalling.

Trust is, like many other aspects of an architecture, layered. Direct trust relationships should generally not extend beyond the following bounds:

- Trust within an architectural layer.
- Trust up one architectural layer.
- Trust down one architectural layer.

This allows architectural abstractions to be maintained. The key techniques to allow broader trust to be built up are chains of trust and the delegation of trust between multiple entities. It is also more likely that relevant communications will be available between the various entities involved in forming trust relationships.

G.3 Public Key Infrastructures and Trust

Machine based trust is often cryptographically assured using asymmetric (public key) cryptography and certificates. There are a number of ways of achieving this but essentially they all rely upon a certificate showing the identity of the trusted party, the scope of the trust relationship, and the identity of the delegated trusted 3rd party.

A public key infrastructure requires that parties Alice and Bob generate public-private key pairs and proof that the public key they want certified belongs to them and to the paired private key. This activity is done through registration to a Certificate Authority (CA) resulting in a Public Key Certificate (PKC) that is used to attest to a third party (Alice say) that the CA is confident that Bob is the real owner of the public key.

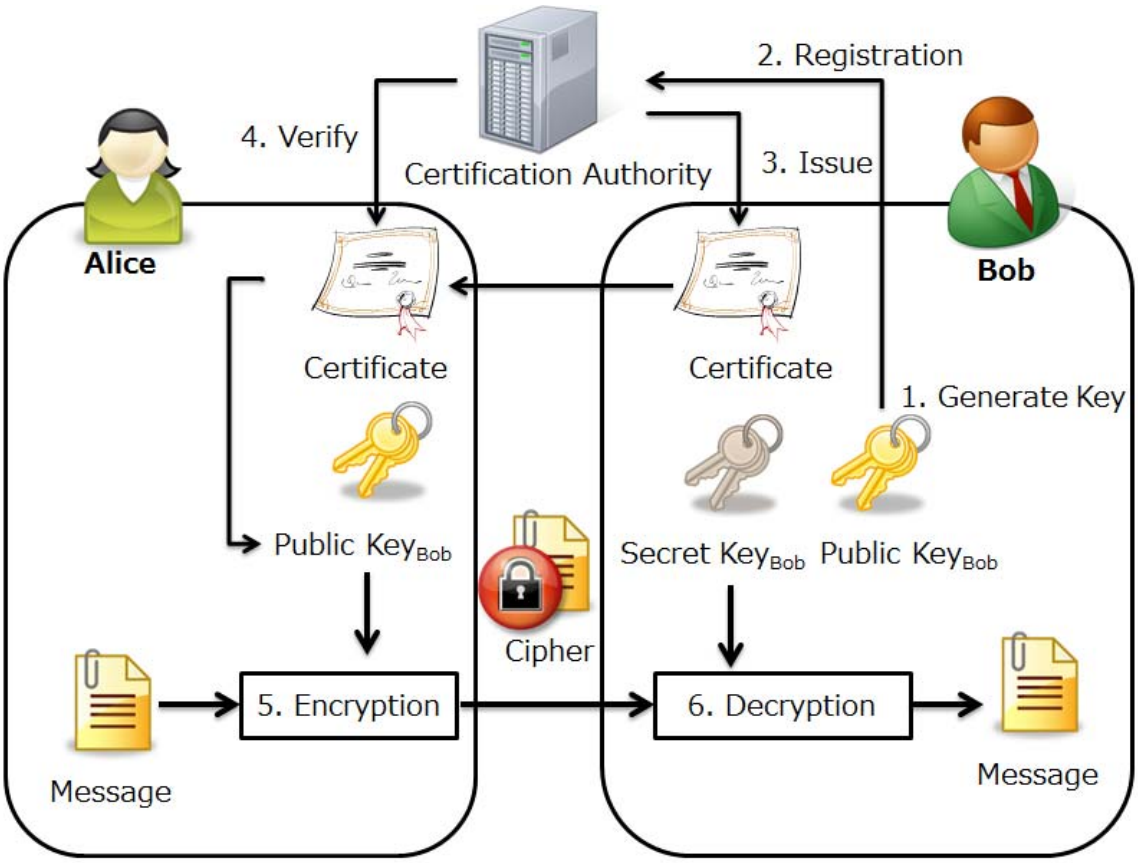

Figure G.1: Public key encryption with public key certificates used for key exchange

The relationship to trust is shown in figure G.2.

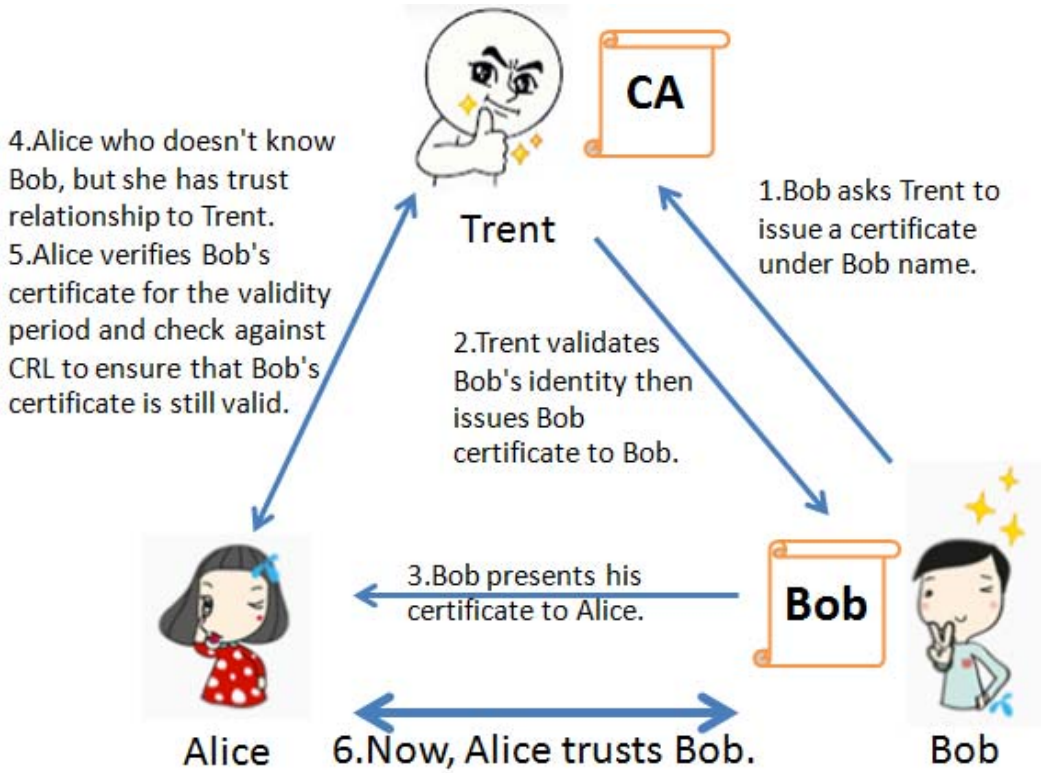

Figure G.2: PKI to reinforce trust

Modelling of PKI and the role of certificates.

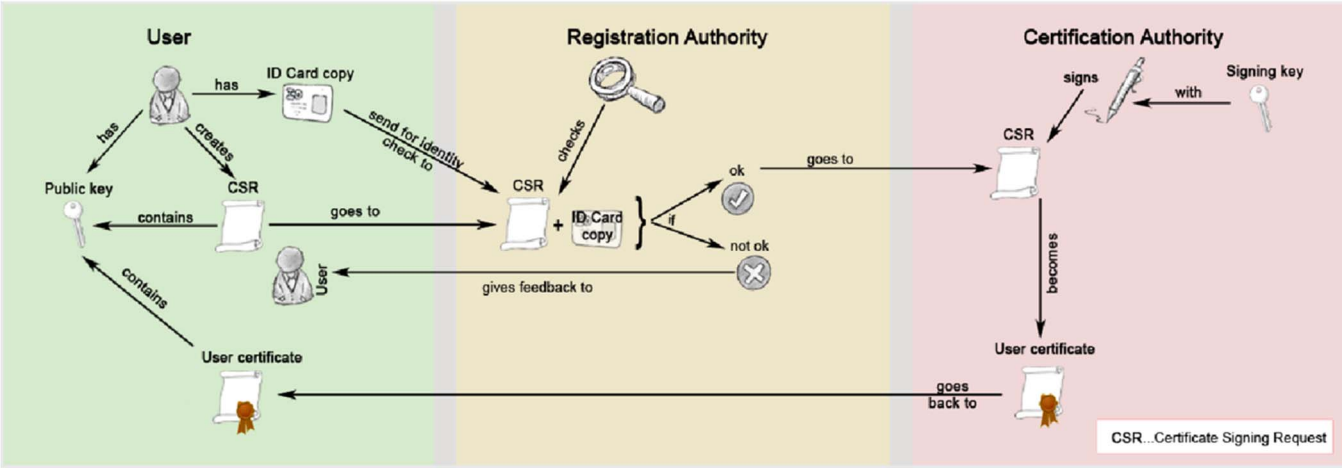

Figure G.3: PKI architecture with addition of Registration Authority

G.4 Models of trust

G.4.1 Overview

The trust model is developed using 3 parties initially: Alice, Bob, Charles (ABC). Models of trust are either direct, in which Alice needs to trust Bob and bases that trust solely on their prior relationship, or indirect in which Alice needs to trust Bob without either a direct relationship to base that trust on or a prior relationship. In the indirect model Alice can seek the assistance of a 3rd party, Charles, in building and assigning trust to Bob.

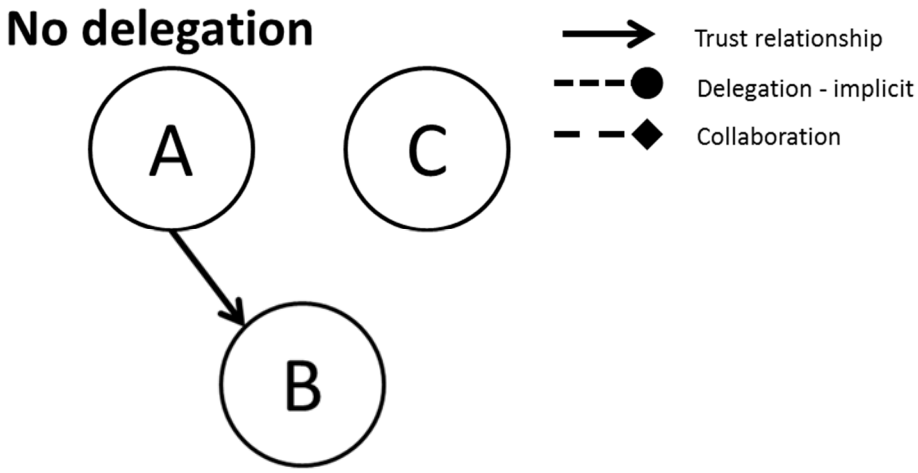

Figure G.4: Trust Delegation - No Delegation

Sometimes an entity A needs to establish a trust relationship with an entity B, but lacks some or all of the necessary capabilities to evaluate the appropriate level of trust. This lack could be due to a variety of issues, for example:

- Lack of access to historical information about entity B's behaviour.
- Lack of framework to evaluate B's trustworthiness.
- Lack of direct network access to a Revocation Authority to check whether a certificate that B has presented is current.

Quite often, it is inappropriate to include sophisticated trust logic within a component such as a VNFCI which has very specific duties, and where duplication of such logic across multiple components would be computationally wasteful or architecturally messy.

G.4.2 Directly delegated trust

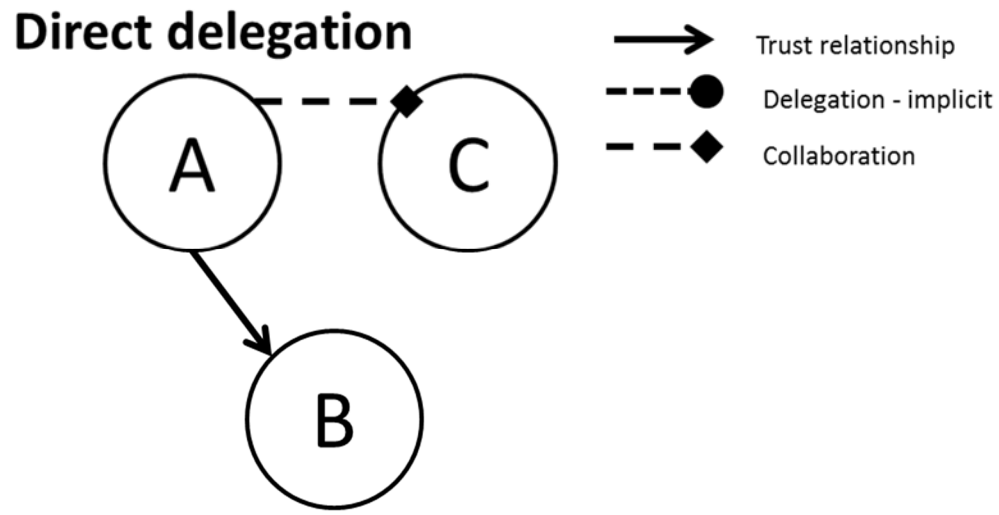

Figure G.5: Trust Delegation - Direct

Where Alice is unable to evaluate the appropriate level of trust for a relationship with Bob, Alice may choose to delegate the decision to Charles, who is in a better position to make such a decision. In this case, there should be an explicit element to the trust relationship from Alice to Charles that shows that Alice is happy for Charles to make such decisions for Bob.

The delegation of this trust may not be an explicit one, but may be implicit in the design and/or deployment options of Alice.

G.4.3 Collaborative trust

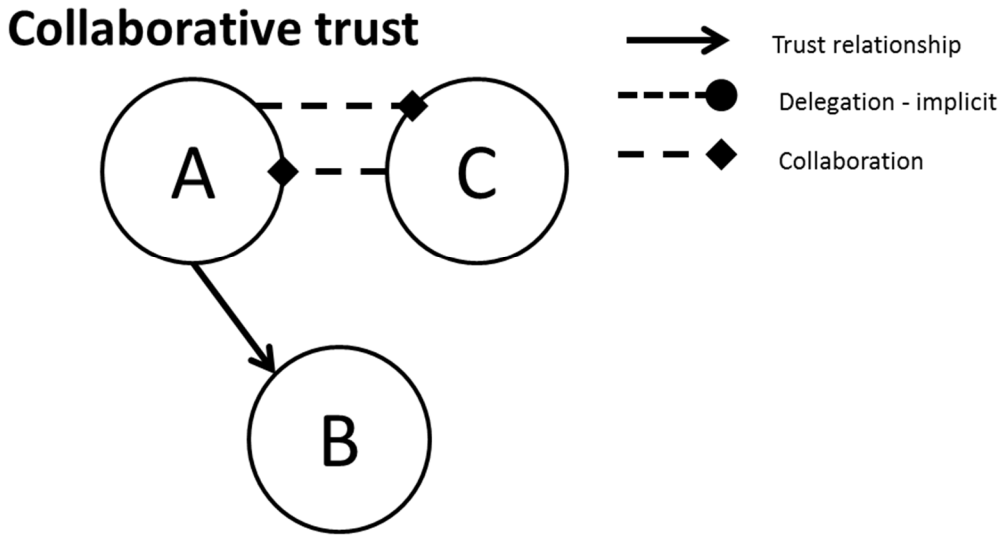

Figure G.6: Trust Delegation - Collaborative Trust

Collaborative trust involves two entities (Alice and Charles) working together to decide whether to trust another (Bob) - the final goal may be for both Alice and Charles to have a trust relationship with Bob, or just one of them. The expectation is that Alice and Charles may have different information available to them which will help them to make a more informed decision about the trust relationship with Bob.

The expectation with collaborative trust is that contexts of trust will be shared, but parameters may be different. There should also be opportunities for Alice and Charles to communicate if trust levels - or the parameters on which they are based - change, so that re-evaluation can be performed by all relevant parties.

G.4.4 Transitive trust

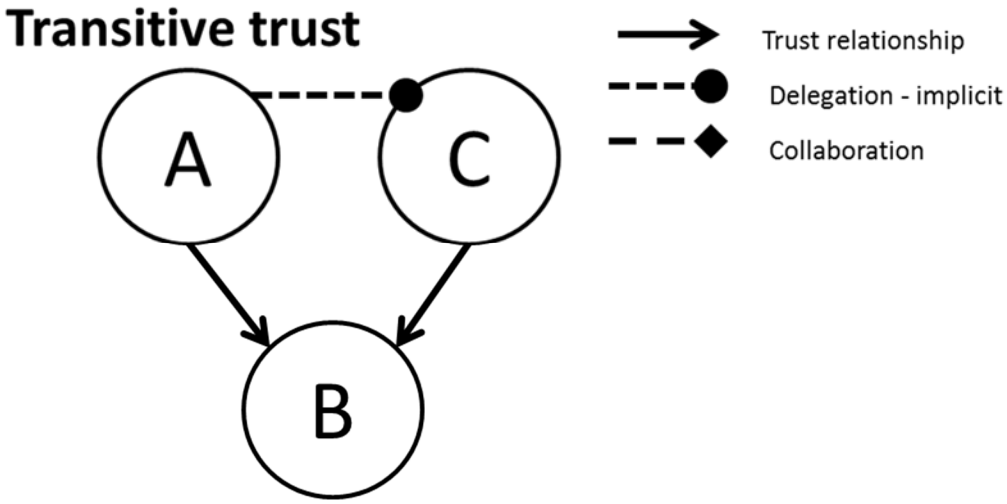

Figure G.7: Trust Delegation - Transitive Trust

Transitive trust is the decision by Alice to trust Bob because Charles trusts him. This is not the same as a pure delegation of trust, as Charles may be unaware of Alice's reliance on it: in other words, Charles is no way brokering the trust relationship from Alice to Bob. Unlike in "pure" delegated trust there is no explicit element to the trust relationship to Alice to Charles (that the latter is aware of) that Bob is trusted due to the Alice->Charles relationship.

The key danger of transitive trust is that because there is no explicit element of this type, Alice cannot be certain that the contexts for trust - and associated parameters - from Charles to Bob are entirely aligned with Alice's contexts. Nor can it be sure that the relationship from Charles to Bob is still current unless it has methods by which is can examine any re-evaluations, re-validations and invalidations of the Charles-> trust relationship.

G.4.5 Reputational trust

Reputational trust is a specific instance of transitive trust, where Alice takes a view on the trustworthiness of Charles based on a rating of Bob's trust relationship with Charles. Usually, there will be many other entities that trust Charles (say D, E, F, G, etc.), and some algorithm will be applied to the various ratings published by these entities in order to allow Alice to make a decision about trusting Bob. This algorithm may be applied by Alice (in which case Alice needs access the ratings of the various parties C, D, E, F, G, etc.) or by a third). A distinguishing point about this type of transitive trust is that it is almost always explicit: the entities C, D, E, F, G, etc. are likely to be aware that they are participating in a reputational trust scheme.

Annex H: Wireless Innovation Forum security considerations for SDRD

H.1 Introduction

WINNF-08-P-0003 [i.4] from the Wireless Innovation Forum, titled "Securing Software Reconfigurable Communications Devices" provides security considerations for Software Defined and Reconfigurable Devices (SDRD) systems. While the Software Communication Architecture (SCA) used for SDRD does not match the model selected for Reconfigurable Radio Systems, several items are of relevance and it is the purpose of the present annex to highlight such item from [i.4] and complement them in the context of RRS security.

Among the topics of most interest are the identification of asset and stakeholder as well as vulnerabilities, threats and exploits. [i.4] also covers security design principles, some of them addressing topics not directly in the technical scope RRS specifications yet relevant to RRS deployments (such as the manufacturing phase or hardware security).

H.2 Identification of assets

A number of assets in WINNF-08-P-0003 [i.4] match those in RRS from a security perspective: communication service and network, electromagnetic spectrum, health of individuals and safety of other assets, reputation, software and hardware.

In the context of RRS, the electromagnetic spectrum should be viewed from two angles: the spectrum itself and the access method to the spectrum. Not all threats against the availability of the radio spectrum come from radio jamming, it is also possible to attack the radio protocols.

The physical device is considered and asset in the [i.4] as it could be lost or stolen, and used for abusive actions in various ways. In the context of RRS, this asset is of lesser importance as countermeasures are typically implemented by the manufacturer for the whole platform or as part of Radio Access Technologies embodied in a Radio Application. However, both SDRD and Reconfigurable Equipment are desirable targets in terms of computing resources available to an attacker that would successfully compromise the device locally or remotely. This is true for radio applications too, as they would have access to specific hardware and software resources that could be diverted from their original purpose. Interest from attackers will rise as soon as a way to monetise the resource exist (even compared to what would be available on the generic purpose host OS), especially if such resources are standardized and technical documentation easily available.

WINNF-08-P-0003 [i.4] divides the software/firmware asset into four categories: Radio Platform Applications (equivalent to RRS Radio Applications), Service Provider Applications (SPA), User Applications (UA), and Radio Platform Operating Environment (RPOE, which includes in particular the host OS and security services). The main attack vectors considered with these assets are those related to reconfiguration (loading, installation, execution). Due to architectural differences this classification does not exactly match with what is found in RRS. While higher level applications (such as user applications) are not in the scope of RRS, it is relevant to consider their potential interaction with RRS RA. Thus Radio Applications should be considered both as an attack vector against other assets in the RE, and as an asset that could be compromised in transit as well as from other parts of the system within the RE (including another RA).

Just like in RRS, reputation and liability are viewed as essential assets, however focus is later given to security certification and Evaluation Assurance Levels and less on regulatory compliance. It should be noted that security certification is very important towards gaining trust that a device will remain compliant. Identifying the party liable for compliance throughout the lifetime of the device and guaranteeing the integrity of compliant software on the RE are among the objectives of RRS.

In [i.4], user data are also part of the assets. For Radio Applications this is implicitly acknowledged by ensuring that they will behave and be used in the way intended by the economic operators (in particular the OEM and Software Providers).

The last asset considered in [i.4] are Platform Configuration and Operating Data. In the context of RRS this obviously includes configuration metadata found in Radio Application Packages, but it may also include policies and internally generated information such as history information of the RA installer, or information such as file hashes generated by security services.

H.3 Actors (stakeholders)

WINNF-08-P-0003 [i.4] identifies a larger number of stakeholders than one can find in RRS, and the chosen model differs as well:

1) Device User.
2) Device administrator/owner (e.g. enterprise or parent).
3) Regulator.
4) Communication Service Provider.
5) Manufacturer.
6) Software/Content Provider.
7) Download Authorization Authority (DAA).
8) Software Distributor (SD) (similar to a RadioApp Store operator).
9) Policy Distributor.
10) Policy Issuer.

The model follows what can be found for IT systems operations. The Regulator is presented as the authority that assigns spectrum rights and establishes limits for safe radio operations. Absent in the description are its role as notification and certification bodies that can be found in the RED [i.14]. Note also the distinction between the device user and the device owner, as well as the existence of the Download Authorization Authority and the policy-related actors (which are all defined for the purpose of security).

An interesting characteristic of the Communication Service Provider (CSP) stakeholder is that the device may be tied to several CSP if the user subscribes to different services (through one or more RAT). One delivery method of RA is via the RA themselves, that reside on the RE.

It is useful to refer to [i.4] regarding the manufacturer. The following quote is taken from Wireless Innovation Forum document WINNF-08-P-0013 [i.4]:

"*In most current regulation, the radio manufacturer is held responsible for the behavior of the radio. So long as this continues, the manufacturer stakeholder will want to continue to restrict behavior on the device throughout its life cycle. However, identifying a single manufacturer may be difficult for reconfigurable communications because devices may involve the integration of several hardware and software components, potentially in a plug-and-play manner. For this reason, the manufacturer role may be filled by several stakeholders in certain environments. In the end, the manufacturer is the entity that assumes liability for the performance of the device, which in most cases is an integrator of hardware and software components to create a platform for radio software. In other instances governing authorities may define the responsible entity.*"

In RRS the OEM stays the original manufacturer and the term is not used to name another actor that holds liability, although the OEM may keep the responsibility of ensuring compliance of the RE as part of a different role.

The Software/Content Provider (SCP) actor in WINNF-08-P-0003 [i.4] loosely matches the Software Provider actor in RRS. It is stated that the SCP may want to protect their Intellectual Property and restrict access to their code only to known good platforms. These interests may however contradict the requirements of the RED [i.14] which mandates that security functionalities not be used for market discrimination.

The Software Distributor (SD) can be partially mapped to the RRS RadioApp Store, as the SD can also take other forms such an independent server or a user connecting storage media directly on the device. The RadioApp Store may also be the entity that acts as a DAA.

There is no equivalent of the Policy Distributor or the Policy Issuer in RRS.

H.4 Threat analysis

H.4.1 Vulnerability classes

WINNF-08-P-0003 [i.4] identifies vulnerabilities applicable to different weaknesses of SDRD. These are presented below. Those that fall within the scope of RRS are mentioned as such.

In the **Design Process**: flaws in coding standards, peer review and testing. Emphasis is given to cleaning the final product of any debugging functionality (such as symbols, debug codes, testing accounts and backdoors) and undocumented features. Recommendation is given to reduce the feature set to a required minimum in order to keep the attack surface as small as possible. In RRS, the shadow platform, compilers, and RPI are part of the design process.

In the **Manufacturing process**: substitution of trusted firmware by an insider, compromise of key material and other sensitive material (such as certificate chains) during generation and/or transfer to the device, and hidden hardware functionality (backdoor).

While these processes are largely not in the scope of RRS, the capability to update Radio Applications would provide an after-the-fact countermeasure against some forms of substitution, provided mechanisms are in place to ensure its reliability. Relevant weaknesses could further be addressed in RRS by facilitating security services such a monitoring and anomaly detection. However, the manufacturing phase is where trust towards a platform begins and there is comparatively little that can be done in RRS against devices that have been compromised during that phase.

With the **Communication Protocols**, in particular design flaws and implementation flaws. In the context of RRS communication protocols fall at least in two categories: the protocols (and their implementation) that support RRS functionalities (e.g. RAP download and security services) on the one hand, and those that are implemented within Radio Applications on the other hand and which are out of scope.

With **Open-Source and Third-Party software**, in two aspects: firstly, that third party tools such as compilers could be malicious (such as introducing a back-door at compile time); secondly, that the same level of audit applies to third-party code and in-house code alike in order to avoid importing code of lesser security. Related threats are better addressed by manufacturers and software providers rather than within RRS. However, an update mechanism would provide after-the-fact mitigation.

With **Software based on Open Standards and open APIs**, in the sense that it is easier for an attacker to learn about an open system and identify vulnerabilities. This is especially true for technical specifications, for which the update cycle can be counted in years. Design principles such as cryptographic flexibility and defence in depth can help mitigate vulnerabilities in the long term.

With **Policy-based operations**, as well as **configuration data**, that can be an efficient venue of attack. They could be modified in transit, at rest, or come from a malicious source. In the context of RRS this includes in particular RAP metadata, over-the-air signalling, files for capability-based decisions, and files for RadioApp Store selection.

With **External interfaces**: an unprotected JTAG or an available port allowing DMA, for example, are good venues of attacks against the device.

With **Cognitive and smart radio**: the behaviour of such radio can be influenced by a determined attacker. For cognitive radios the pilot channel may be jammed or spoofed. For smart radios, influencing the radio environment may allow for controlling the RAT selection on the device, potentially leading to a downgrade in security. For RRS such threats are to be taken into account when dealing with RAP transmission and signalling between the RadioApp Store and the RE.

WINNF-08-P-0003 [i.4] later covers the run-time environment and execution of software, which can also be subject to vulnerabilities.

H.4.2 Threat classes

Identified threats in WINNF-08-P-0003 [i.4] are:

- Denial of Service.
- Unauthorized access:
  - physical, to the device at manufacture time;
  - to internal data on the device (user data or device data) via control or user interfaces.
- Eavesdropping.
- Masquerade.
- Modification.
- Repudiation.
- Replay.
- Traffic analysis.

In the context of RRS, unauthorized access via the control interface should also be understood as coming from a network service or from a trusted - albeit compromised - Radio Application. Several threats apply to the compliance of RRS systems to radio regulation (taken as an objective of RRS) in particular regarding interferences and efficient use of the spectrum: Denial of Service, Masquerade, Modification, Replay.

H.4.3 Attacks and exploits

Identified attacks classes in WINNF-08-P-0003 [i.4] are:

- malicious software installation;
- software misuse;
- spectrum misuse;
- tampering;
- spoofing;
- unauthorized modification of data or software on the device;
- unauthorized access to user (or other) data on the device.

There exist significant architecture differences between SDRD and RRS: instead of providing a middleware layer, RRS splits the RA between software and hardware capabilities and allows hardware reconfiguration through metadata in the RAP. This means that attacks against the hardware could be possible from a malicious RAP, allowing compromise of elements in the RE that are beyond the reach of the host OS or radio OS. Once again, a Radio Application that has been compromised either through its own operation or through RRS functions can be used as an attack vector against other elements on the RE or against the network.

H.5 Identification of security critical processes

Quoting [i.4], "Security Critical processes are those processes which, if compromised, could prevent the enforcement of the platform's security policy". They are provided below:

- Design and development phase.
- Manufacturing/Provisioning phase.

- Platform operation:
  - secure boot;
  - secure instantiation and execution of software (integrity check, secure transit from storage to execution space, built-in-tests);
  - software download and installation;
  - policy download.
- SDRD local and remote management operations.
- Platform decommission and disposal (security sensitive data could remain on the device).

As stated earlier in the present annex, the design and development phase as well as the manufacturing and provisioning phase are on the scope boundary of RRS. However, RRS should be able to handle remediation in case RRS assets get compromised during these phases. For example: what can be done after deployment, if it is discovered that an available Radio Application, that has been installed via legitimate means, has in fact been compromised during the development phase? Of course, not all such attacks can be remediated in RRS.

H.6 Security services

WINNF-08-P-0003 [i.4] provides an extensive set of security concepts, hardware measures and logical services that can be employed for the design of a secure architecture.

Security services include:

- Access control and access control model.
- Information integrity.
- Information security (confidentiality).
- Transmission security.
- Key and credential management services:
  - key and random number generation;
  - key management infrastructure;
  - key material distribution and reception;
  - key material identification and expiration;
  - key material storage and protection;
  - key material erasure.
- Platform resource security management:
  - memory management enforcement;
  - platform software configuration management;
  - radio platform operating environment;
  - radio platform applications.
- Logging, auditing, and security alarm.
- Policy enforcement and management.

An item of particular importance will be the inclusion of RRS implementation within the secure boot procedures of the RE (for example requirements relative to a Trusted Platform Module).

Concepts for the security architecture presented in [i.4] include:

- Principle of least privilege.
- Reference monitor.
- Trusted Computing Base (definition from the Orange Book).
- Communication channels:
  - trusted path (meaning extended by WINNF);
  - trusted channel;
  - protected channel;
  - unprotected channel;
  - covert channel.
- Defence in depth.
- Assurance levels.
- Anti-tamper.
- Accountability and auditing.

Not all communication channels in the RRS architecture may have to be protected in the same way, if at all. There exist in RRS message-based interfaces (such as the MURI), descriptive interfaces (such as the RPI), and command based interfaces (such as the interface between the CM and the URA). Covert channels could exist e.g. between Radio Applications running concurrently.

As mentioned in [i.4] defence in depth is an important concept. However, it is common for attackers to chain exploits in order to compromise a target. The ability to securely fail within RRS is critical (e.g. with running Radio Application, install time).

Tamper detection measures could be leveraged in RRS in order to inform the network of potential compromise of the RRS subsystem on a device.

Auditing implies the ability to gather information. In the case of RRS this includes, for example, RA installation logs (with date, origin, version, etc.), identification of interfaces where suspicious behaviour could be detected (e.g. a Radio Application trespassing its current RVM protection class), logging of authentication failure or invalid control commands from the network.

Architectural design considerations in [i.4] include:

- Isolation and separation (in OS, processor, memory).
- Information flow control.
- Simplicity versus complexity.
- Hardware (path separation and flow control. tamper-resistance, dedicated processors).
- Object labels (information attached to objects and subjects, that governs access control).

While these design considerations concern foremost the development phase, implementation can be facilitated by choices in RRS architecture in particular in terms of separation of concerns and identification of components providing security services.

EXAMPLE: Better isolation can be enforced by separating the download, verification, and installation phases of Radio Applications between different components. Also, RRS offers a form of information flow control thanks to the interface model which only allows information to flow up or down the interface stack made of the RRFI, the URAI, and the MURI. The interfaces themselves, being part of the attack surface, require careful consideration.

Simplicity is an essential aspect that should be balanced with other objectives. Simpler security that is implemented and used is better than complex security that is not implemented or not used. In RRS the user interaction is supposedly limited but other stakeholders have an interest in having solutions that can be easily deployed.

While RRS has been designed to accommodate various hardware design choices, it should be noted that security modules could be leveraged, in particular for secure storage of sensitive material specific to RRS.

Finally, RVM protection classes and RF front-end protection classes are example of systems for which resources could be labelled.

H.7 Other considerations

H.7.1 Downloadable policies

WINNF-08-P-0003 [i.4] highlights that downloadable policies are a critical part of the overall security policy for SDRD, but at the same time are an attractive venue of attack. As such they require careful design so that they can be safely parsed and unambiguously interpreted by the device. This also includes behavioural policies for cognitive radios and regulatory compliance. [i.4] mentions the work of IEEE Standards Coordinating Committee (SCC) 41 (formerly P1900) regarding downloadable policies.

Proper security mechanisms are also required to guarantee at least the integrity of the policies. Ideally the originator of the policy should also be identified, authenticated and authorized.

Annex I:
Review of remote control management protocols

I.1 Overview

The present annex provides an overview of device management protocols and their use to remotely control devices.

I.2 OMA Device Management

I.2.1 Introduction

The main purpose of OMA Device Management [i.24] is to allow management authorities to manage and configure devices on behalf of users. This includes creation, update and retrieval of configuration information, obtaining events from the device (monitoring and alerts), and execution of management primitives on the device. A large set of transport mechanisms are supported. The present description of OMA DM will focus on version 1.3.

I.2.2 General principles

OMA DM builds on a tree of Management Objects (MO) which represent resources on the device. The tree structure allows identification of an MO using its path in the tree from the root node, as part of a URI. The data model provides a standardized tree of Management Objects, their semantic, and syntax. It is divided into three groups: generic (bearer neutral), bearer-specific, and vendor-specific objects.

A standard set of Management Objects have been specified, but the specification allows for extensions. Such standardized extensions include for, example, software update, firmware update, and connectivity management.

The Device Management protocol uses a request/response transactional model and is based on a simple set of commands (Get, Replace, Add, Delete, Exec, Copy). In the normal procedure, the DM client always initiates the device management session by registering with the DM server. After this step, the server sends DM commands to the client. The client may continue the transaction in case results or alerts are to be reported to the server.

The DM session runs over the HTTP Binding, in which case the DM client is (or uses) an HTTP client.

The DM server may trigger the establishment of a DM session by sending an out-of-band notification to the DM client. Such notifications are sent via the delivery methods available in OMA Push (WAP Push, SIP Push, OBEX, HTTP Push, Cell Broadcast).

OMA DM also provides a mode of operation outside a DM session:

- sessionless alerts from DM Client to DM Server (while the alert message is well defined, the protocol bindings are not);
- sessionless commands from DM Server to DM Client (transported via OMA Push).

A bootstrapping process is defined so that the DM client can learn about the DM server it should contact, by means of a bootstrap message. The bootstrap information contains the address of a DM server to contact. OMA DM supports four bootstrap methods to accommodate various deployment scenarios:

- Customized bootstrap, where the bootstrap information is pre-configured on the device at device provisioning time.
- Smarcard bootstrap, tying this information to the smartcard (which may be swappable) instead of the device.
- Client-initiated bootstrap, where connection information to a bootstrap server is known to the client. The bootstrap server will then provide the necessary information for the client to connect to the DM server, via a bootstrap message.

- Server-initiated bootstrap, where the bootstrap server can send a bootstrap message once it becomes aware of the device (e.g. when the device first joins the network).

The bootstrap process can be conducted over OMA Client Provisioning or via the Device Management bootstrap server.

Finally, user interactions (e.g. for information about the ongoing management operations, or to obtain agreement from the user) are supported by means of an embedded or side-loaded web browser.

I.2.3 Security

I.2.3.1 Communication security

When the DM session is conducted over HTTP, TLS can be used to provide confidentiality, integrity authentication. These properties are dependent on underlying mechanisms when other protocol bindings are used.

The designers of OMA DM have identified the need for transport-neutral security (in this case, end-to-end authentication and integrity of messages), for scenarios where the transport layer cannot provide these services, such as with sessionless operations. Authentication and integrity is provided using the HMAC-SHA256 construct. Notification messages are also subject to authentication and integrity protection, but with a SHA256 digest only.

I.2.3.2 Bootstrap security

Communication with the bootstrap server can be performed with HTTPS, but this is not mandatory. A smartcard can be used to provide a higher level of security assurance for the storage of bootstrap messages.

I.2.3.3 Access control

The DM server and client can authenticate each other either at the transport or at the application layer. An Access Control List properties can be instantiated for each node in the Management Object tree in order to define access rule. The subject is defined by the server identifier.

I.2.3.4 Other mechanisms

The DM enabler allows for the Management Objects to be encrypted prior to communication or storage on the device, without specifying the encryption scheme.

I.3 OMA LWM2M

I.3.1 Introduction

The OMA Lightweight M2M enabler [i.25] is a device management protocol designed for efficiency in the context of machine to machine communications over constrained resources. Although the protocol borrows concepts from OMA DM [i.24] (e.g. the concept of objects), it is not built on top of it.

I.3.2 General principles

The model of controllable client device resource follows a flat structure of Objects, each composed of one or more Resources. Both Objects and Resources can have multiple instances, and are addressable via a URI path. In addition, attributes can be attached to Objects and Resources, and represent their metadata. LWM2M specifies several encoding formats to represent the data: plain-text, opaque, TLV, and JSON. Conformant clients support the TLV format by default. The opaque format is in principle only used to represent binary resources such as firmware.

Several standardized Management Objects are available, allowing for:

- definition of security parameters for communication with servers;

- definition of other parameters for communication with servers;
- definition of access control rules;
- definition of device information and access to reboot and factory reset functions;
- definition of connectivity monitoring information;
- access to the firmware upgrade function.

LWM2M is a point-to-point management solution in which clients first registers to the server before management operations can proceed. These operations are server-driven, they include:

- Read/Write (to obtain, respectively set, the values of Objects and Resources);
- Discover/Write Attributes (to obtain, respectively write, attributes attached to Objects and Resources);
- Execute (to have the client execute an operation represented by a given Resource);
- Create/Delete (to create, respectively delete, an Object instance on the client).

The LWM2M server can also request that specific resource be monitored, via the Observe operation. When the resource changes, the client notifies the server via the Notification operation. This is similar to the concept of trap in other protocols, such as SNMP.

The core protocol for the interactions between LWM2M servers and clients is CoAP, with bindings to UDP and SMS transports. Both bindings support a "Queue Mode" whereby the server queues requests until the client sends a message indicating it as awaken. This allows the client to optimize energy consumption by going offline.

Similar to OMA DM [i.24], there exist several ways to bootstrap the LWM2M client:

- Factory bootstrap providing information for connecting to the LWM2M server;
- Smarcard bootstrap providing this information in the smartcard;
- Client-initiated bootstrap, where connection information to a LWM2M Bootstrap Server is known to the client (the bootstrap server will then provide the necessary information for the client to connect to the LWM2M server);
- Server-initiated bootstrap, where the LWM2M Bootstrap Server automatically configures the LWM2M Client.

I.3.3 Security

I.3.3.1 Communication security

LWM2M 1.0 implements communication security allowing confidentiality, integrity, and authentication of parties by using the DTLS protocol for both:

- the UDP protocol binding, using Pre-Shared-Key, Raw Public Key Certificates, or X.509 Certificates mode; and
- SMS protocol bindings, using Pre-Shared-Key mode.

Replay detection is not mandated. With SMS protocol binding, decryption can occur on the smartcard.

I.3.3.2 Bootstrap security

As the bootstrap phase is critical, communication security is required between the LWM2M Client and Bootstrap Server. When the bootstrap information in located on a smartcard, the establishment of a secure channel between the smartcard and the LWM2M Client is recommended.

I.3.3.3 Access control

In LWM2M 1.0, the access control mechanism allows the client to operate with several servers and to authorize management operations for each Object and on a per-server basis. The Authorization process is based on Access Control Objects which provide a functionality similar to that of Access Control Lists. When the client is bound to only one server, that server has full access rights.

I.4 GSMA Service Provider Device Configuration

I.4.1 Introduction

The GSMA SPDC [i.26] is presented as an alternative to OMA DM [i.24], adapted to the use cases of mobile operators, and designed to operate over cellular and third-party networks.

I.4.2 General principles

In SPDC, configuration data is represented as an XML document in which parameter elements are logically grouped through characteristic elements representing specific aspects of the configuration.

The configuration document is meant to hold configuration profiles defined in other management technologies. It can also embed a message to be display to the user before the configuration occurs, possibly with a request to accept the configuration and the conditions in the message (typically, the terms of use of the service).

At the transport level, SPDC uses HTTP and the binding is such that the HTTP client runs on the device to be configured, and the HTTP server runs on the configuration server. The configuration server is under the control of the service provider (the mobile operator). The client normally request configuration data, but the configuration server can also trigger the client into doing so via a notification SMS.

SPDC supports several scenarios:

- Configuration over cellular networks:
  - In this scenario, the device establishes a connection through a packet-switched data network in order contact the configuration server. The URL to contact the configuration server is built from a standardized template filled with the MCC and MNC of the mobile operator. In this scenario, the configuration client requires a SIM to be present on the device.
  - When a configuration update occurs, the configuration client may be given a token to use for configuration over non-3GPP access.
- Configuration over non-3GPP access:
  - In this scenario, the configuration client authenticates with the configuration server on top of HTTPS, by means of a token (e.g. the one received in the previous case) or by means of a one-time password sent to the device over SMS.
- Configuration with GBA authentication:
  - This is a variant of the previous two scenarios, in which the Generic Bootstrapping Architecture is used, achieving a stronger form of authentication.
- Configuration of additional devices sharing the same identity:
  - In this scenario, the user can configure secondary devices using their primary device. The secondary device does not possess a SIM allowing user authentication. In this case, the user configures the secondary device manually. When the secondary device executes the reconfiguration procedure for the first device, a one-time-password is sent to the user on the primary device by means of an SMS.

- Configuration of non-cellular devices with a dedicated identity:
    - In this scenario, the device does not possess a SIM and has a dedicated identity. The user manually configures the device and enter a one-time-password provided by out-of-band means, allowing the configuration client to perform the configuration procedure.

The use of a standardized request URI and the presence of the SIM resolves the bootstrapping problem in most cases.

I.4.3 Security

As detailed above, the security of SPDC relies on 3GPP security mechanisms. In addition, there is no fine-grained access control mechanism in place: the party responsible for the configuration server has full control over the device configuration.

Part of the network discovery mechanism - identifying whether the connection to the configuration server is done over a packet-switched mobile data network - involves the use of plain HTTP. The authentication and configuration steps, however, use HTTPS.

Annex J:
Usage of the DoC and the RE Configuration Policy in RRS

J.1 Introduction

In the regulatory framework of the European Union, the DoC of a device is a declarative document listing the Union Acts for which conformance of the device is claimed. RRS makes a distinction between:

- the DoC as a legally binding document to be provided to the consumer and regulatory bodies; and
- the verification procedures, that the combination of hardware and software (Radio Applications) on the RE is compliant with the essential requirements of the RED.

The RE Configuration Policy is used for the later purpose. It is an electronic, machine-readable document (e.g. a file or an instance of structured data in memory) that is prepared by the RAP/DoC Provider (likely, the OEM). It provides rules for the RE about which Radio Applications can be installed (e.g. with a mapping between the RE Type and RAP IDs), and other statements that would be necessary for the RE to remain compliant (the exact data model is specific to an RE Type).

NOTE: the RE Configuration Policy remains in the technical domain and applies at the level of the implementation. It should be understood as having a role similar to an access control policy (e.g. and XACML policy) or a mobility policy for a mobile phone.

The RE Configuration Policy is not a translation of the DoC in a machine-readable format, but a set of instructions from the RAP/DoC Provider used by RE to determine that a reconfiguration will lead to a legitimate state. From the point of view of the RE there is no concept of compliance but only of permitted operations leading to a legitimate state of the RE. The compliance of the RE and RA combination to the regulation is tested by the RAP/DoC Provider before the RA is allowed in the RE Configuration Policy. Thus, the number of valid software and hardware combination announced in the RE Configuration Policy at any point in time is bounded by the expected market flexibility and manufacturer's testing capabilities that underpin the deployment of a given RRS Platform.

Figure J.1 illustrates the relationship between the two documents.

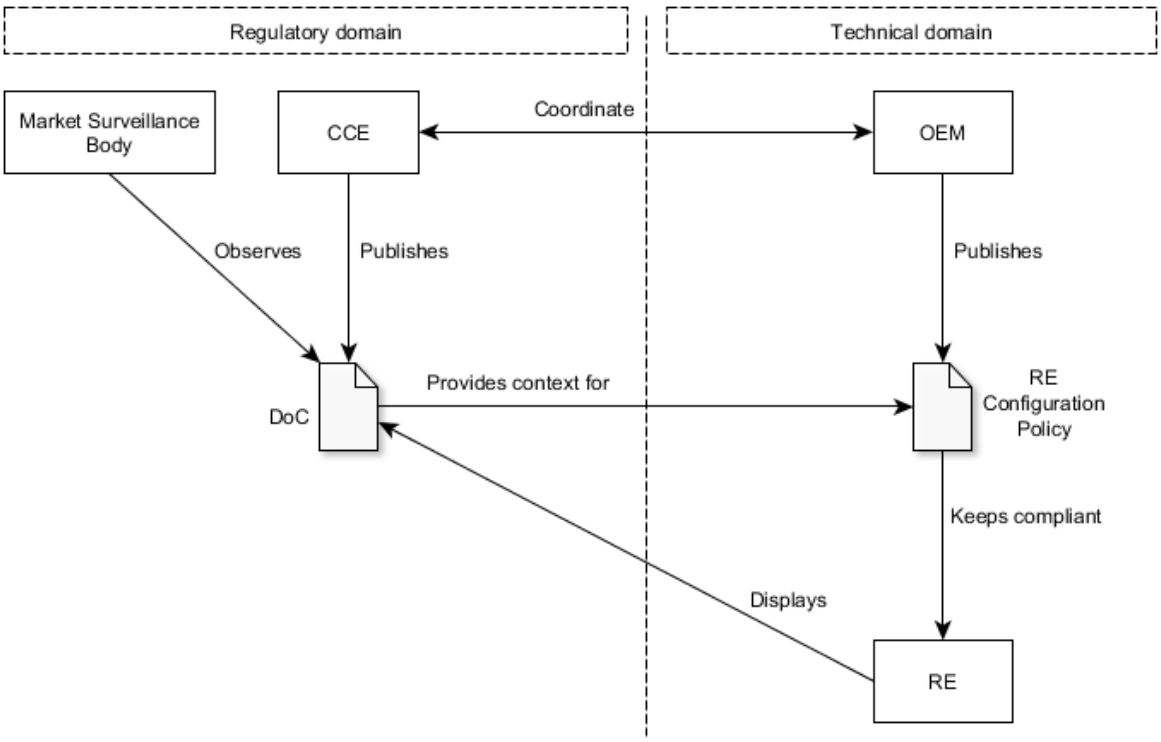

Figure J.1: Relationships between the Doc and the RE Configuration Policy

J.2 Distribution scenarios

The separation between the DoC in the regulatory domain and the RE Configuration Policy in the technical domain gives full flexibility for handling compliance of the RE, regardless of how the DoC is distributed.

Diverse market deployments can be supported as illustrated in table J.1.

Table J.1: possible DoC distribution scenarios

Value	DoC form	Current scenario	Future scenario #1	Future scenario #2
legal	Paper DoC, complete or simplified	x	x	
informative	Digital DoC, complete or simplified		x	
legal	Signed digital Digital DoC, complete or simplified			x
technical	**RE Configuration Policy**	x	x	x

The DoC could be distributed:

a) as a signed paper document, along with the device (complete DoC per annex VI of the RED); or

b) as a signed, short paper document, along with the device, and giving a link (URL) to a complete version of the DoC on the World Wide Web (simplified DoC per annex VII of the RED).

With both options a) and b) above, a digital copy of the DoC could also be added on the device. Later, as regulatory frameworks for legally binding digital document gain wider acceptance, these digital copies could be signed, for example under the eIDAS digital signature regulation of the EU, as detailed in [i.12], annex E. At this point, it is possible that the paper copy of the DoC will not be provided any longer when a device is introduced on the market.

In any of the possible scenarios detailed above the RE Configuration Policy provides a forward-compatible solution as it remains the reference document for the RE and is distributed by the RadioApp Store - even when the RadioApp Store does not distribute a digital version of the DoC. RRS supports both the (optional) distribution of the DoC to devices, and the (mandatory) distribution of the RE Configuration Policy.

If supported by an RRS deployment, the distribution of the DoC in digital form is independent of the distribution of the RE Configuration Policy. When new or updated RAs are available for installation on the RE, the RE Configuration Policy is updated and distributed, but the DoC itself may remain unchanged.

J.3 Applicability to other regulatory frameworks

Since the RE Configuration Policy provides rules for the RE to achieve compliance, it makes it possible for RRS compatible devices to be compliant to radio regulations other that the RED.

Whether said regulations use a form of declaration of conformity or other means to announce compliance, the clear distinction between the RE Configuration Policy and the DoC guarantees the applicability of the technical solution in a generic manner. If necessary, the data model of the RE Configuration Policy could be adapted to these regulations and enhanced with support for geolocation so that policies relevant to the local regulatory framework are selected.

Annex K: Implementation guidelines

K.1 Introduction

The statements in the present annex are meant as guidance for the implementer to successfully leverage the security requirements in ETSI TS 103 436 [i.12] when implementing the frameworks defined in clauses 10 and 11 of the present document.

NOTE: These guidelines may be leveraged to produce additional conformance statements complementing those defined in [i.12], annex G, when the testing environment allows such additional statements to be verified.

K.2 Guidelines for the configuration enforcement framework

K.2.1 APDU identification and anti-replay

The unique message identification in the APDU header is meant for the Administrator to reject an APDU if it determines that an APDU with the same identification information was already received (and validated), thus preventing replay attacks.

Note that it can be safe to check for the APDU identification before performing the signature verification (thus preventing unnecessary processing). This is possible when the APDU grammar is of low enough complexity, provided that the parser leverage these restrictions.

K.2.2 Leveraging the root of trust for management of critical assets

The presence of the root of trust on tier#2 and tier#3 devices (as defined in [i.12]) makes it possible to use protected locations for ensuring the confidentiality and (partial) integrity of critical assets. For example, the Administrator could store the following assets in protected locations:

- public keys of authorized APDU senders (APDU authorized senders manifest);
- representation of installed RAP, DoC, RE Configuration Policy, and RA parameters, as available at manufacturing time, (safe mode manifest);
- representation of installed RAP, DoC, RE Configuration Policy, and RA parameters, as taken by a snapshot (snapshot manifest);
- representation of all available snapshots (snapshot list manifest);
- in order not to waste memory resources on the root of trust, it is possible to use hash-based representations of the data located in a protected location (such as a hash-list or a Merkle tree) and protect the root node (the root hash) in a shielded location.

K.3 Guidelines for the long-term lifecycle management framework

K.3.1 Certification paths

As detailed in clause 11 the TAD is the digital embodiment of a transfer of authority between one RRS-CA to the next one. In ETSI TS 103 436 [i.12] the TAD and other supporting assets are defined as attribute certificates in accordance with Recommendation ITU-T X.509 [i.32], so that the RRS-CM can leverage the rules for certification path validation related to the RRS Configuration Profile, the RRS-CP Profile, and the TAD - in order words to verify that the chain of trust points to the RRS-CA that was originally configured for the RE.

An example set of certification paths is given below.

The validation and acceptance of a new TAD can be made dependent on the following conditions:

- the verification of the certification path for the TAD is successful, and
- the "issuer" field of the new TAD matches the "holder" field of the most recent TAD in the TAD installation log, and
- the "issuer" and "holder" fields of the new TAD do not match, and
- the "holder" field of the new TAD does not match the "holder" field of any of the TAD in the TAD installation log.

The certification path for the TAD of the currently valid RRS-CA can be implemented as follow:

- the RRS-CM selects the TAD with the "effectTime" closest to the clock time (this is the currently valid RRS-CA), and
- each intermediate TAD is verified using, as time, the verification time for said TAD (the time said TAD was first verified by the RE), according to the verification rules in Recommendation ITU-T X.509 and, on success,
- the TAD path is walked in backward order until reaching the bootstrapping TAD and, finally
- the bootstrapping TAD is be verified.

The certification path for the RRS-CP Profile can be implemented as follow:

- the RRS-CP Profile signature is verified with the Asset Signature Key of the currently valid RRS-CA and, on success,
- the RRS-CM verifies that the "issuer" field in the RRS-CP Profile matches the identity in the "holder" field in TAD applying to the currently valid RRS-CA and, on success
- the certification path for the TAD of the currently valid RRS-CA is verified.

The certification path for the RRS Configuration Profile can be implemented as follow:

- the signature of the RRS Configuration Profile is verified and, on success,
- the certification path attesting to the identity of the RRS-CP is verified.

K.3.2 Leveraging the root of trust for management of critical assets

Due to its nature the security of the long-term management service relies on proper implementation of security services by the RE, such as when leveraging the capabilities of the root of trust.

In particular the RE normally keeps a copy of each accepted TAD in order to reconstruct the certification path to the origin RRS-CA. Shielded locations provide higher tamper resistance but consume secure memory, which is a limited and costly resource on the root of trust. Alternatively to using shielded locations, the RRS-CM can use protected locations for such purpose and still provide high assurance on the integrity of each TAD.

If the later approach is taken, it is advisable to have means in place in order to detect successful deletion attempts of installed TAD. For this purpose the RRS-CM can further leverage the root of trust and use a hash-extend register in order to save a secure digest of a TAD installation log. A way to implement a compatible installation log would be, for example:

- to design the TAD installation log as a chronologically ordered event log, where
- each record in the event log summarizes the characteristics of an accepted TAD, and
- the last record corresponds to the most recently accepted TAD,
- with this approach it is possible to produce a secure digest of each record in the installation log and operate the log in a way compatible with the operations of a hash-extend register. There exist several suitable cryptographic hash functions for the production of secure digest.

Similar considerations apply for integrity protection of the RRS-CP Profile and the RRS Configuration Profile, for which protection locations could be used.

Annex L: Bibliography

- Boris Balacheff, Liqun Chen, Siani Pearson (ed.), David Plaquin, and Graeme Proudler: "Trusted Computing Platforms: TCPA Technology in Context". Prentice Hall PTR, Upper Saddle River, NJ, 2003.
- E. Brickell, J. Camenisch and L. Chen. Direct anonymous attestation. In Proc. 11th ACM Conference on Computer and Communications Security, pages 132-145, ACM press, 2004
- "Principles of Remote Attestation": George Coker, Joshua Guttman, Peter Loscocco, Amy Herzog, Jonathan Millen, Brian O'Hanlon, John Ramsdell, Ariel Segall, Justin Sheehy, and Brian Sniffen

NOTE: Retrieved from http://web.cs.wpi.edu/~guttman/pubs/good_attest.pdf.

History

Document history		
V1.1.1	June 2016	Publication
V1.2.1	November 2017	Publication