ETSI TR 103 502 V1.1.1 (2017-09)

Reconfigurable Radio Systems (RRS); Applicability of RRS with existing Radio Access Technologies and core networks; Security aspects

Reference

DTR/RRS-0314

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

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.

Executive summary

The introduction of RRS capability is shown not to inhibit the provision of the security mechanisms of existing radio access technologies. The reason, shown in the present document, is that the security capabilities for common radio technologies (e.g. LTE/SAE, IEEE 802.11™) are present at layers 2 and higher in the OSI protocol stack, whereas the novel features of RRS apply to the means to provision layer 1. It is highlighted however that a Radio Application addresses a complete protocol stack and provision of all layers of the protocol stack in a single software package may require special provisions in the Reconfigurable Equipment to enable full network communication.

1 Scope

The present document shows a mapping of existing Radio Access Technologies (RATs) to the Reconfigurable Radio System (RRS) model in order to identify missing security requirements, in particular identify the boundary of an RRS Radio Application with regard to the security functions present in existing RAT. Recognizing that a RAT is not bound to a single link but may be supported by functions in the network the present document also considers the role of core networks in supporting any triggering of the Reconfigurable Equipment to reconfigure itself using a push mechanism.

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] ETSI TS 133 401: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401)".

[i.2] ISO/IEC 7498-1:1994 "Information technology -- Open Systems Interconnection -- Basic Reference Model: The Basic Model".

[i.3] ETSI TR 102 945: "Reconfigurable Radio Systems (RRS); Definitions and abbreviations".

[i.4] ETSI EN 303 095: "Reconfigurable Radio Systems (RRS); Radio Reconfiguration related Architecture for Mobile Devices".

[i.5] Len Sassaman, Meredith L. Patterson, Sergey Bratus, Michael E. Locasto, Anna Shubina: "Security Applications of Formal Language Theory".

[i.6] Noam Chomsky: "On certain formal properties of grammars", Information and Computation/information and Control, vol. 2, pp. 137-167, 1959.

[i.7] Michael Sipser: "Introduction to the Theory of Computation", Second Edition, International Edition, Thompson Course Technology, 2006.

[i.8] Seymour Ginsburg and Sheila Greibach: "Deterministic context free languages", in Proc. 6th Symp. Switching Circuit Theory and Logical Design, 1965, pp. 203-220.

[i.9] Dan Kaminsky, Meredith L. Patterson and Len Sassaman: "PKI Layer Cake: New Collision Attacks Against the Global X.509 Infrastructure".

[i.10] Travis Goodspeed, Sergey Bratus, Ricky Melgares, Rebecca Shapiro and Ryan Speers: "Packets in Packets: Orson Welles' In-Band Signaling Attacks for Modern Radios", 5th USENIX Workshop on Offensive Technologies, August 2011.

[i.11] Open Mobile Alliance™. OMA-AD-Push-V2-3: "Push Architecture".

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

[i.12] WAP Forum™ WAP-230-WSP: "Wireless Session Protocol".

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

[i.13] WAP Forum™: "Wireless Application Protocol".

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

[i.14] IETF RFC 2616: "Hypertext Transfer Protocol -- HTTP/1.1".

[i.15] IETF RFC 793: "Transmission Control Protocol".

[i.16] IETF RFC 3261: "Session Initiation Protocol".

[i.17] ETSI TS 123 228: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; IP Multimedia Subsystem (IMS); Stage 2 (3GPP TS 23.228)".

[i.18] ETSI TS 122 146: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Multimedia Broadcast/Multicast Service (MBMS); Stage 1 (3GPP TS 22.146)".

[i.19] Open Mobile Alliance™: "OMA Mobile Broadcast Services".

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

[i.20] 3GPP2 C.S0070-0: "Broadcast Multicast Services (BCMCS) Codecs and Transport Protocols".

[i.21] ETSI EN 302 304: "Digital Video Broadcasting (DVB); Transmission System for Handheld Terminals (DVB-H)".

[i.22] ETSI TS 123 041: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041)".

[i.23] ETSI TS 142 009: "Digital cellular telecommunications system (Phase 2+); Security aspects (3GPP TS 42.009)".

[i.24] ETSI TS 125 302: "Universal Mobile Telecommunications System (UMTS); Services provided by the physical layer (3GPP TS 25.302)".

[i.25] ETSI TS 123 040: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of the Short Message Service (SMS) (3GPP TS 23.040)".

[i.26] ETSI TS 123 204: "Universal Mobile Telecommunications System (UMTS); LTE; Support of Short Message Service (SMS) over generic 3GPP Internet Protocol (IP) access; Stage 2 (3GPP TS 23.204)".

[i.27] ETSI TS 124 011: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface (3GPP TS 24.011)".

[i.28] ETSI TS 144 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Station - Base Station System (MS - BSS) Interface Channel Structures and Access Capabilities (3GPP TS 44.003)".

[i.29] ETSI TS 143 020: "Digital cellular telecommunications system (Phase 2+) (GSM); Security related network functions (3GPP TS 43.020)".

[i.30] ETSI TS 144 064: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile Station - Serving GPRS Support Node (MS-SGSN); Logical Link Control (LLC) Layer Specification (3GPP TS 44.064)".

[i.31] ETSI TS 124 008: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008)".

[i.32] ETSI TS 144 018: "Digital cellular telecommunications system (Phase 2+) (GSM); Mobile radio interface layer 3 specification; GSM/EDGE Radio Resource Control (RRC) protocol (3GPP TS 44.018)".

[i.33] ETSI TS 124 341: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Support of SMS over IP networks; Stage 3 (3GPP TS 24.341)".

[i.34] GSM Association IR.92: "IMS Profile for Voice and SMS".

[i.35] ETSI TS 131 102: "Universal Mobile Telecommunications System (UMTS); LTE; Characteristics of the Universal Subscriber Identity Module (USIM) application (3GPP TS 31.102)".

[i.36] ETSI TS 131 101: "Universal Mobile Telecommunications System (UMTS); LTE; UICC-terminal interface; Physical and logical characteristics (3GPP TS 31.101)".

[i.37] 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.38] ETSI TS 122 016: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; International Mobile station Equipment Identities (IMEI) (3GPP TS 22.016)".

[i.39] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003)".

[i.40] ETSI TR 103 087: "Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems".

[i.41] IEEE 802.11p™: "IEEE Standard for Information technology -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments".

[i.42] ETSI TS 133 102: "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Security architecture (3GPP TS 33.102)".

[i.43] GSM Association TS.06 (DG06): "IMEI Allocation and Approval Guidelines, Version 6.0".

NOTE: Available at http://www.gsma.com/newsroom/wp-content/uploads/2012/06/ts0660tacallocationprocessapproved.pdf.

[i.44] IEEE 801.1X™: "IEEE Standard for Local and metropolitan area networks - Port-Based Network Access Control".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 102 945 [i.3] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 102 945 [i.3] and the following apply:

2G	Second Generation
3G	Third Generation
ASN	Abstract Syntax Notation
BCMCS	Broadcast and Multicast Service
CBCH	Cell Broadcast CHannel
CBS	Cell Broadcast Service
CTCH	Common Traffic Channel
DCCH	Dedicated Control Channel
IMS	IP Multimedia Subsystem
LLC	Logical Link Control
MM	Mobility Management
OMA	Open Mobile Alliance™
P-CSCF	Proxy-Call Service Control Function
P-GW	PDN GateWay
PDN	Packet Data Network
RR	Radio Resource
SACCH	Slow Access Control Channel
SDCCH	Standalone Dedicated Control Channel
SIP	Session Initiation Protocol
SGSN	Service GPRS Support Node
SMS-SC	SMS Service Centre
SQL	Structured Query Language
WAP	Wireless Application Protocol
XMPP	eXtensible Messaging and Presence Protocol

4 OSI stack mapping to RRS

4.1 OSI protocol stack overview

The conventional 7-layer model for Open Systems Interconnection defined in ISO/IEC 7498-1 [i.2] allocates particular functionality to each of the abstract layers. A strict interpretation of the OSI model is that radio technologies apply to layer 1 only, as the nature of the physical media is only apparent at that layer. However, whilst a radio signal is physical the Radio Access Technology is more complex. The physical layer is where the modulation and RF stuff is done, the link layer, layer-2 in the OSI model, is where the logical connectivity is built up and this is carried through to the network layer, layer-3 in the OSI model, where the radio device becomes connected to the wider network. Thus for conventional telecommunications modelling the broadly accepted model has been slimmed down to only 3 layers:

- Layer 1 - physical media, the radio path.
- Layer 2 - the link layer that offers a reliable connection across the radio path between 2 points.
- Layer 3 - the network layer that builds the terminal into a wider network of devices.

The nature of the transmission environment dictates to a very large extent the means by which data can be transmitted and for radio the environment is hostile. The hostility itself takes a number of forms but the corollary of wavelength and transmission range, the impact of noise, the impact of fading, and so on all are addressed across the layers of the protocol stack. In addition the radio resource is highly regulated with regulation defining most of the physical characteristics, e.g. radiated output power, bandwidth, adjacent channel interference restrictions (i.e. how much power can be broadcast in adjacent channels), and for fixed sites also addresses such things as antenna height and antenna gain. Any implementation of RRS has to give assurance the regulation is not abused and the means of enforcing any claims for equipment to the Declaration of Conformity (DoC) has to be added to the security model of the radio device when that device is an RRS capable of being modified on the fly to support one or more Radio Access Technologies (RATs).

In terms of commonly applied security functions the assignments in table 1 are generally applied.

Table 1: OSI mapping of security and transmission functions

n	Name	Basic function for transmission	Commonly applied security functions
4++	Application domain	Everything else	Application security (CIA paradigm)
3	Network layer	Routing, multi-node networking	Authentication, Key management (as part of mobility management in cellular networks)
2	Link Layer	Logical channels creating a reliable link (LLC)	Encryption, Transmission packet integrity, Transmission FEC
1	Physical layer	The radio bits	PHYLAWS, QKD, QE and similar physical layer security

4.2 OSI layers and security mechanisms

4.2.1 Threats and countermeasures

The technical domain of security is often described in terms of the CIA paradigm (Confidentiality Integrity Availability) wherein security capabilities are selected from the CIA paradigm to counter risk to the system from a number of forms of cyber attack. The common model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} such that a triple such as {interception, confidentiality, encryption} is formed. The threat in this example being interception which risks the confidentiality of communication, and to which the recommended countermeasure (protection measure) is encryption.

The very broad view is thus, for communications systems, that security functions are there to protect user content from eavesdropping (using encryption) and networks from fraud (authentication and key management services to prevent masquerade and manipulation attacks). Where encryption is applied to content it is applied prior to radio encoding but the key assignment scheme may be optimized for the radio framing structure.

4.2.2 Radio link specificity of countermeasures

Countermeasures should always be designed to fit the context in which they are applied. On the understanding that radio links are inherently unreliable (bit error rates of up to 10 % are common) any security process applied has to be robust in the face of error. For TDM schemes (e.g. TETRA, GSM) the slot and frame numbering may be used to give a time invariant parameter that is used to drive certain cryptographic modes (e.g. in GSM the 22 bit frame number is used as an input with Kc (the traffic encryption key) to the key stream generator (A5/X algorithm) to generate a variable number of key stream bits (limited to 114 bits for single half slot encryption). For cellular systems codes specific to cell sites, colour codes, are also used to give radio path differentiation and in high security systems such as TETRA site specific keys are used as key modifiers to give assurance of cryptographic separation between cells.

NOTE 1: In TETRA and evolving LTE scenarios the same plaintext may be delivered simultaneously to multiple cell sites and means have been defined in TETRA such that an exploit of a single site cannot be transposed to another site.

The means by which media (spectrum) is shared has some impact on the viability of security measures. The TDMA/FDMA schemes are well known in most simple digital cellular radio models (e.g. GSM, DECT, TETRA). In collision awareness based systems such as those used in WLAN (IEEE 802.11™ [i.37]) the model is also relatively simple. For simple FDMA/TDMA and collision avoidance systems at any one point in time at any chosen frequency only one user holds the right to transmission. The more complex modes in CDMA however break that model such that at any point in time at any chosen frequency many users may be using the same resource but the codes used by each user, as they are orthogonal to each other, provide mathematical and thus physical separation. The challenge for FDMA systems is to give assurance of frequency synchronization between Alice and Bob, for TDMA systems to give assurance of time (clock) synchronization between Alice and Bob, and for CDMA systems to give assurance of power synchronization amongst all users of the channel. For CDMA as each code pair provides a level of rejection of any other code pair that is translated to an equivalence of co-channel interference rejection then the received power from radios in a single cell site have to be aligned to be within a few dB of each other where the granularity of power control is sufficient for the code-based signal rejection to operate.

In CDMA systems the codes used by each ME are assumed to be orthogonal to each other but this orthogonality applies at zero phase offset. In a multi-path environment the same encoded signal is received multiple times at small phase offsets and errors may arise through insufficient rejection of the interfering multipath signal. The level of signal rejection is dependent on the level of processing gain, the ratio of the spreading code rate to the signal rate. For a nominal 1 kHz signal spread to 100 kHz the processing gain is nominally 20 dB (in other words an interfering signal of 1 kHz in the received 100 kHz will be spread across the entire 100 kHz giving a 20 dB interference rejection).

The modulation scheme in use has a significant impact on overall performance, particularly in the presence of interference. The normal convention of modulating a symbol where a transition in the modulated signal indicates the symbol transmitted is only accurate in transmission if the transition can be accurately measured. For a software based implementation of modulation there are a number of real time aspects to consider therefore as the processing (i.e. encoding or decoding of the modulated signal) has to respect the real time transitions. Any phase distortion introduced by processing delay across the I/Q channel is visible as a significant reduction in signal to noise.

NOTE 2: In a homodyne baseband receiver the I and Q channels are assumed to be exactly 90° out of phase. An error of even a few tenths of a degree caused either by physical path or processing inequalities introduces noise and may give rise to an increase in inter-symbol-interference. Similar errors may be introduced by DC offset. Frequency and phase correction fields used in the transmission bursts of most digital communication systems will compensate for any I/Q channel imbalance.

4.3 Core elements of the RRS model

The current model of RRS applies only to the physical layer. This then would apply to the modulation and to a small extent the framing synchronization of a RAT. However, as noted above a RAT may be seen as covering layers 1 and 2 as there is a case for stating that the TDM, FDM or CDM access modes and channelization are defined at layer 2. Similarly the overall performance of a radio link is not defined solely by the physical layer.

The RVM enables an RA to choose one among multiple available protection classes for code to be executed on the RVM as well as a protection class for the RF front-end. Depending on the combination of chosen RF & RVM protection classes, the required re-certification process of the software reconfigurable radio platform will be more or less complex. The basic principle is illustrated in figure 1.

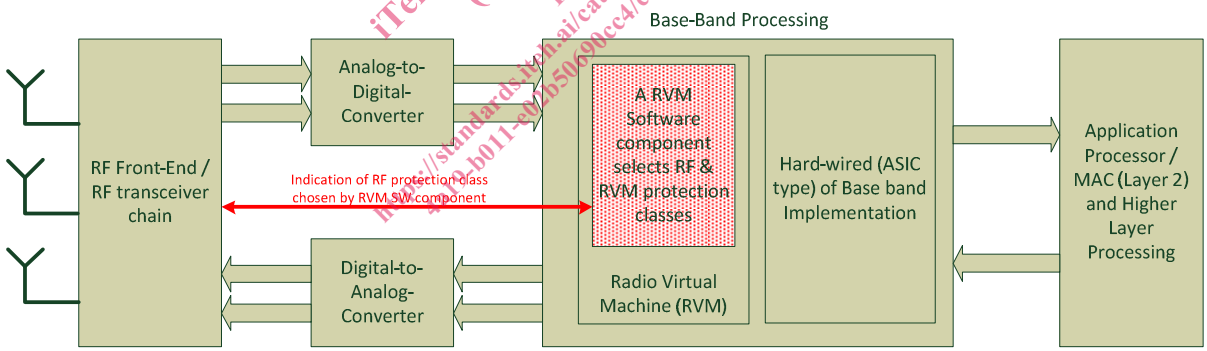

Figure 1: A typical radio equipment architecture comprising an RVM Software Component selecting RF and/or RVM protection class(es) (from ETSI EN 303 095 [i.4])

A typical radio equipment architecture includes an RF Transceiver chain, Analog-to-Digital converters, Digital-to-Analog converters, Base Band Processing, etc. An RVM controls RF Transceiver chain, in particular for selection of an RF Protection Class.

4.4 Applicability of RVM to radio terminal computing

Whilst it is possible to perform general purpose computing using the RVM concept it is not optimized for many of the higher layer protocol and other security capabilities. The state machine based protocols of ISDN-era telephony can be emulated using the RVM although translation of existing code to the RVM model may be problematic. The concern, and security risk, is that existing code, and hardware accelerated firmware, has been mature for many technologies for some years and moving such code to a new platform may introduce performance or functionality uncertainty.