ETSI TS 103 436 V1.1.1 (2016-08)

TECHNICAL SPECIFICATION

Reconfigurable Radio Systems (RRS); Security requirements for reconfigurable radios

Reference

DTS/RRS-03012

Keywords

security, software

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

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.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Reconfigurable Radio Systems (RRS).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**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.

1 Scope

The present document defines the security requirements for reconfigurable radio systems arising from the the use case analysis in ETSI TR 103 087 [i.1]. The present document applies to the lifecycle of Radio Application Packages between a Radio application store and an RRS Reconfigurable Equipment.

2 References

2.1 Normative 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.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

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 necessary for the application of the present document.

[1] Federal Information Processing Standard (FIPS) 202, SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions.

[2] Federal Information Processing Standards (FIPS) 186-4, Digital Signature Standard (DSS).

[3] Federal Information Processing Standards Publication (FIPS) 180-4, Secure Hash Standard.

[4] Federal Information Processing Standards Publication (FIPS) 197, Advanced Encryption Standard.

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

[6] ETSI TS 102 778-1: " Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES".

NOTE: The above standard is composed of multiple parts and implementation of the framework may require implementation of requirements stated in other parts of the standard.

[7] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[8] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[9] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[10] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation Criteria for IT security - Part 2: Security functional components".

[11] ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[12] ISO/IEC ISO/IEC 10181-2: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework - Part 2".

[13] ETSI EN 319 142: "Electronic Signatures and Infrastructures (ESI); PAdES digital signatures".

[14] ETSI EN 319 132: "Electronic Signatures and Infrastructures (ESI); XAdES digital signatures".

[15] ETSI EN 319 122: "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures".

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

[i.2] BlueKrypt: Cryptographic Key Length Recommendation.

NOTE: Available at http://www.keylength.com.

[i.3] ETSI TS 102 165-1: "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.4] ISO/IEC 10181-4:1997: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework - Part 4".

[i.5] Shannon, Claude E. (July/October 1948). "A Mathematical Theory of Communication". Bell System Technical Journal 27 (3): 379-423.

[i.6] Marcelo A. Montemurro, Damián H. Zanette: "Universal Entropy of Word Ordering Across Linguistic Families".

NOTE: Available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3094390/ as PMCID: PMC3094390.

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TR 103 087 [i.1] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TR 103 087 [i.1] and the following apply:

DoS	Denial of Service
DDoS	Distributed Denial of Service
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
OSI	Open System for Interconnection
PKC	Public Key Certificate
PKI	Public Key Infrastructure
PMCID	PubMed Central reference number
TSF	ToE Security Functions
TTP	Trusted Third Party

4 Review of objectives and high level requirements

The objectives stated in ETSI TR 103 087 [i.1] are copied in table 1 and classified in terms of the form of security function that is required to meet the objective. In addressing each objective the form of countermeasure required is discussed in some detail and the overall class or strategy of countermeasure is indicated.

Table 1: Review of security objectives

Id	Text of objective	Countermeasure	Strategy
1	The RRS platform should provide means to ensure that the content of communication between the application store and the RE are protected from exposure to unauthorised 3rd parties (see note 1)	Encryption of content (it is assumed that the link is open (radio broadcast) and that the adversary is able to eavesdrop/intercept the content).	Confidentiality
2	The RRS should provide means to verify that the content of communication between the application store and RE has not been manipulated prior to processing at receipt (see note 1)	Integrity check sum added to content.	Integrity
3	The RRS platform should provide means for the application store to verify the identity of the RE (see note 2)	The RE shall have a unique application store access identity that is bound to a set of credentials shared between the application store and the RE. The identity may be selected by the user of the RE (open market scenario) or may be defined by the RE manufacturer (closed market scenario).	Authentication and Identity Management
4	The RRS platform should provide means for the RE to verify the identity of the application store (see note 3)	The application store shall have an unique name that is tied to its attribute as an application store for RRS in the form of a public key certificate with an attribute extension when operating in an open environment but if operating in a closed environment may allow for authentication using a conventional challenge response protocol in a shared secret mode	Authentication and Identity Management
5	The RRS platform should provide means to detect and prevent denial of access to the communications channel between the application store and the RE	It is possible to limit the entities allowed to offer traffic to the network through an access control policy. In addition DoS (and DDoS) attacks may be mitigated by using resilient and redundant network paths (i.e. mitigation by network topology design)	Access Control, Network Topology
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	The originator of the RAP shall create a signed hash of the RAP, and supply the signature with the attribute certificate of the RAP allowing verification of the hash and signature by the receiving party using the contained public key	Integrity
7	The RRS platform should provide means for the RE to verify the source of the content supplied via the Radio application store	As above where the RAP has been signed by the originator verification of the signature shall result in proof of the source of the RAP	Authentication and Identity Management
8	The RRS platform should provide means to prevent the application store denying provision of an application to the RE	Proof may be lodged with a trusted 3rd party or may be maintained locally within a secure enclave of the device. As such every transaction between the application store and the RE shall be securely logged in such a way that the logs cannot be tampered with by an unauthorized entity	Non-repudiation
9	The RRS platform should provide means to prevent the RE denying receipt of an RA from the Radio application store		
10	The RRS platform should provide means to prevent the RE denying installation of an RA from the Radio application store		

Id	Text of objective	Countermeasure	Strategy
11	The RRS framework should ensure measures are provided to prevent installation of malicious RAPs (see note 4)	Testing and distribution network should verify, as far as reasonable, the functionality of every RAP	Liability framework
12	The RRS framework should ensure measures are provided to prevent modification of an RAP after installation (see note 5)	Run time attestation of integrity	Attestation
13	The RRS framework should provide means to verify the legitimacy of the Declaration of Conformity (DoC) and CE marking (see note 6)	Cryptographically strong document signature verification.	Digital signature
		Maintenance and distribution of blacklist of invalid DoC identities	PKI
		Online verification of signature of DoC	PKI
14	The RRS platform should provide means to be able to uniquely identify the master copy of the DoC (see note 7)	The DoC should be identifiable using a URI or equivalent	Identity management
		Master copy should be named distinctly from any copy and signed as such. In addition copies should be signed/verifiable as legitimate copies and point (URI/URL) to the master copy	Digital signature
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 (see note 8)	This requires the hardware to have tamper-resistant storage to hold the DoC/CE data	Hardware tamper resistance
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	The manifest of required platform capability should be covered in the signature and integrity check function	Integrity
17	The RRS platform should prevent an unauthorised third-party from determining that the DoC is being updated	Authentication of parties	Access Control, Identity Management
18	The RRS platform should prevent an unauthorised third-party from determining that the complete DoC is being retrieved from a simplified DoC over the network	Encryption of signalling	Confidentiality
19	The RRS platform should provide means to prevent modification of the DoC apart from installation and update, in particular at rest	Authenticated access control combined with change management control of the DoC	Integrity
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	The integrity measure here applies to data in transit and may be applied at the transport entity as opposed to the document level	Integrity
21	The RRS platform should prevent an unauthorised third-party to delete, install or otherwise alter a DoC on the RE (see note 9)	The DoC should always be available in read-only form on the RE but authorized 3rd parties shall be allowed to update the DoC. This may happen as a result of installation of a new RAP that requires modification of the stored DoC to support any new capability offered by the RAP	Access Control, Authentication, Identity Management
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	This requires the hardware to have tamper-resistant storage to hold the DoC/CE data	Hardware tamper resistance
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	The checksum for proof of integrity shall be measured across the set of elements that compose the DoC	Integrity
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	Authentication of parties	Access Control

Id	Text of objective	Countermeasure	Strategy
25	The RRS platform should allow for authentication of content (DoC) to the relevant component on the device	The attribute signature of the DoC shall identify by model type the components of the RE that it applies to and this set of data authenticated in the DoC's signature	Identity management
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 as the DoC in Paper form	No technical capability required, however all digital signatures of documents shall be developed in line with the operational framework of the Digital Signature Directive [8] and the eIDas Directive that will supercede it [9]	Liability framework
27	The RRS platform should allow for the traceability of devices that have received an updated DoC	A framework of non-repudiation of origin, and of receipt shall be provided	Non-repudiation
28	The RRS platform system should provide means to prove reception and installation of a DoC by a device		
29	The RRS platform should allow for binding the DoC to the device that receives it	The attribute signature of the DoC shall identify by model type the components of the RE that it applies to and this set of data shall be authenticated in the DoC's signature and thus bind the DoC to the device. Additionally the RE serial number shall be used as a nonce when storing the DoC in a secure enclave of the RE	Secure storage
30	The RRS platform should allow for verifying that the presented DoC is bound to the device	At installation the serial number of the RE shall be used as a nonce in the secure storage of the DoC, thus only if the DoC can be retrieved using the serial number of the RE as a key	Local and Remote attestation

NOTE 1: The means of providing the checksum is to some extent dependent on the nature of the content. In the application store environment the checksum should form part of the digital signature of the content itself. However it may be reasonable to add integrity verification to the transmission path itself, for example mandating IPsec in ESP mode with a valid ICV field (and avoiding use of the NULL algorithm of course), or mandating the use of TLS [7] with authentication, integrity and encryption enabled.

NOTE 2: In conventional systems such as in 2G/3G cellular networks the radio equipment is identified by the International Mobile Equipment Identifier (IMEI) and the subscriber by the International Mobile Subscriber Identity (IMSI). In some systems the radio equipment is identified by its MAC address (at Layer 2 of the OSI stack). In the wider ICT domain equipment is often identified by its serial number. The identity to be verified for the RE has to be immutable and bound to a credential for its authentication.

NOTE 3: The commercial architecture of application stores may influence the design in this case. In the short term it is assumed that a single RE will be associated with a single application store.

NOTE 4: This is a problematic area as it cannot be done with fixed tests as the attacker will craft code to pass such tests whilst remaining malicious. The role of fuzzing and such like may be integrated but such non-deterministic tests are not always valid either. The end result is that the liable party should be clearly identifiable for the correct operation of the RAP.

NOTE 5: This is an area of study in the ISG NFV domain and as such is of direct relevance in RRS. The aim in the NFV work is to prevent installation of a compromised image. It is strongly recommended to harmonise the activity in the ISG NFV and RRS for standardized solutions.

NOTE 6: The Public Key Infrastructure is an almost essential support to the signature scheme used to verify identity and attributes that are asserted using the certificates and associated signatures. In addition a liability framework should be instantiated that clearly identifies the roles of each actor/stakeholder and the penalties that apply for transgressions. The liability framework should be based on the existing market controls with due consideration of the role of stakeholders such as RAP providers that may not have been previously considered.

NOTE 7: For the DoC each copy shall be marked in such a way that it is clear if it is the master, a copy, or an element of a DoC and also marked in this case as either master or copy. It should be clear to the reader of the DoC where it has been generated, by whom and for which equipment (or combination of equipment).

NOTE 8: The mutability of an RE in RRS requires that the DoC/CE data held on the device is also mutable unless the DoC is always stored externally to the device.

NOTE 9: For any implementation not implementing hardware based tamper resistance, an equivalent means of providing persistent storage even if the device operating system is corrupted is required.

Where digital signature is to be deployed there is a risk from advances in computing that may make the more common approaches invalid. Both the RSA and ECC approaches are vulnerable to Shor's and Grover's algorithms when run on a quantum computer that will break the algorithms (i.e. given knowledge of the public key certificate the private key can be found in polynomial time). The alternative for future proof digital signature is to use an approach that is considered Quantum-safe, i.e. an algorithm that is not weakened by the capabilities of a quantum computing attack. Within ETSI the impact of quantum computing is being addressed in 2 groups: ISG Quantum Safe Cryptography (QSC) with a role to identify cryptographic primitives that will be viable for reference in standards; CYBER with a role to identify business continuity requirements in transition to quantum safe cryptography. In addition it is noted that Grover's algorithm reduces the effective strength of symmetric cryptography in such a way that the key length has to be doubled to retain the same level of cryptographic strength (i.e. a system running with 128 bit keys to give 128 bit security will need to run with 256 bit keys to retain 128 bit security in the presence of Grover's algorithm). It is also noted that some cryptographic modes for symmetric key encryption are rendered null for some quantum attacks and such attacks need to be considered for systems with long key life.

5 Countermeasure framework

5.1 Notes for interpretation

NOTE 1: The convention used in the present document is to refer to the thing being protected as a document even if in practice it may be an executable program, or a configuration file or something else.

NOTE 2: The convention of referring to the legitimate parties to a transaction or involved in a security association as Alice and Bob, with the adversary referred to as Eve is followed in the text below.

NOTE 3: Where digital signature is to be deployed there is a risk from advances in computing that may make the more common approaches invalid. Both the RSA and ECC approaches are vulnerable to Shor's and Grover's algorithms when run on a quantum computer that will break the algorithms (i.e. given knowledge of the public key certificate the private key can be found in polynomial time). The alternative for future proof digital signature is to use an approach that is considered Quantum-safe, i.e. an algorithm that is not weakened by the capabilities of a quantum computing attack. The recommendations given in this clause take account of the requirement for cryptographic agility that is necessary to address this specific class of threats.

NOTE 4: The framework for the countermeasures identified has been expanded from the templates given in ETSI TS 102 165-2 [11].

5.2 Identity management and authentication

The following entities shall be named and authenticated in the process of RAP and DoC Distribution, Development and regulatory compliance.

- Developer of RAP - identified by an identity form of Public Key Certificate (PKC) according to Recommendation ITU-T X.509 [5].
- Application store - identified by an attribute form of PKC according to Recommendation ITU-T X.509 [5]

NOTE: The attribute form of certificate extends the public key certificate but does not contain the public key which is contained in the tied PKC.

- RE Manufacturer - identified by both an identity form, and by an attribute form, of PKC according to Recommendation ITU-T X.509 [5] where attribute is of type RRS_RE_MANUFACTURER.

The primary purpose of the authentication service is to counter masquerade attacks with a secondary purpose of verifying identity for a number of accountability services, the latter mainly in the context for RRS of non-repudiation and to verify assertions of ownership and access rights. The authentication framework for RRS is derived from ISO/IEC 10181-2 [12].