ETSI TS 103 436 V1.2.1 (2018-02)

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

Reference
RTS/RRS-0315

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

Essential patents

IPRs essential or potentially essential to normative deliverables 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 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 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 https://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] Void.

[12] Void.

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

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

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

[16] Void.

[17] Void.

[18] Void.

[19] Void.

[20] IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)".

[21] ANSI X9.95: "Trusted Time Stamp Management and Security".

[22] Void.

[23] Void.

[24] ISO/IEC 9646-7: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[25] TGC: "Trusted Platform Module Library; Part 1: Architecture; Family 2.0; Level 00 Revision 01.38; September 29, 2016".

[26] OASIS eXtensible Access Control Markup Language (XACML) Core Specification Version 3.0.

[27] Void.

[28] Recommendation ITU-T X.520: "Information technology – Open Systems Interconnection – The Directory: Selected attribute types".

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". PMCID: PMC3094390.

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

[i.7] Bela Gipp, Norman Meuschke and André Gernandt: "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin", National Institute of Informatics Tokyo, Japan.

[i.8] Void.

[i.9] NIST SP 800-164: "Guidelines on Hardware-Rooted Security in Mobile Devices".

NOTE: Available at http://csrc.nist.gov/publications/drafts/800-164/sp800_164_draft.pdf.

[i.10] ETSI TS 123 040: "3GPP TS 23.040: "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.11] ETSI TS 123 041: "3GPP TS 23.041: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); Technical realization of Cell Broadcast Service (CBS) (3GPP TS 23.041)".

[i.12] ETSI TR 103 502: "Reconfigurable Radio Systems (RRS); Applicability of RRS with existing Radio Access Technologies and core networks; Security aspects".

[i.13] 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.14] 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".

[i.15] ISO/IEC 10181-2: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework - Part 2".

[i.16] ISO/IEC 11889-1:2015: "Information technology -- Trusted platform module library -- Part 1: Architecture".

[i.17] ISO/IEC 11889-2:2015: "Information technology -- Trusted Platform Module Library -- Part 2: Structures".

[i.18] ISO/IEC 11889-3:2015: "Information technology -- Trusted Platform Module Library -- Part 3: Commands".

[i.19] ISO/IEC 11889-4:2015: "Information technology -- Trusted Platform Module Library -- Part 4: Supporting Routines".

NOTE: [i.16], [i.17], [i.18] and [i.19] are also available from the Trusted Computing Group as the TPM 2.0 (Trusted Platform Module) Library Specifications available at https://trustedcomputinggroup.org/tpm-library-specification/.

[i.20] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.21] IETF RFC 6218: "Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.22] NIST Special Publication 800-56B: "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography".

[i.23] ETSI TR 187 010: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Report on issues related to security in identity management and their resolution in the NGN".

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] and the following apply:

protected location: memory location outside of the hardware root of trust, protected in against attacks on confidentiality and in which from the perspective of the root of trust, integrity protection is limited to the detection of modifications

Qualified Signature Creation Device (QSCD): device for creating a digital signature that through its software and hardware is able to ensure that the signatory has sole control over their private key, that the signature creation data is generated and managed by a qualified trust service provider, and that the signature creation data is unique, confidential and protected from forgery

Secure Signature Creating Device (SSCD): device for creating a digital signature that is able to ensure that the signature-creation data involved in creating a signature is unique, protects against forgery and alteration after the signature has been created

shielded location: memory location within the hardware root of trust, protected against attacks on confidentiality and manipulation attacks including deletion that impact the integritiy of the memory, in which access is enforced by the hardware root of trust

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
PAP	Policy Administration Point
PCR	Platform Configuration Register
PDP	Policy Decision Point
PEE	Policy Enforcement Engine
PEP	Policy Enforcement Point
PIP	Policy Information Point
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RED	Radio Equipment Directive
RTM	Root of Trust for Measurement
RTR	Root of Trust for Reporting
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
PMCID	PubMed Central reference number
TAD	Transfer of Authority Document
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TSF	ToE Security Functions
TTA	Trusted Timestamp Authority
TTP	Trusted Third Party
XACML	eXtensible Access Control Markup Language

3a RRS platform security classifications

3a.1 Overview

RRS device security is defined by assignment of mandatory security features to the RE and accompanying system in a series of classes or tiers. To avoid confusion with the term class used in the context of Mobile Device Reconfiguration Class (MDRC) the security levels are referred to as tiers, i.e. Tier#1, Tier#2, Tier#3. Each security tier has associated features that are mandatory or optional and are summarized in table 0.

Table 0: Summary of Security features in RRS RE by tier

Tier	Signature validation	Signature creation	Trusted timestamp	Secure store	Remote attestation	Configuration control	Long term management
1	M						
2	M	M	M	M		Local - M Remote - O	
3	M	M	M	M	M	Local - M Remote - M	M

The features above require that an RRS device implements a hardware root of trust (see clause 9).

3a.2 Signature validation

Electronic signature validation shall be provided in all RRS platforms for the validation of the source and integrity of any downloaded Radio Application.

As defined in clause 5.3 the RA shall be signed and the public key certificate of the signing authority, and any other identifying certificates used in the distribution chain, shall be provided along with the RA. The RE shall be able to verify the signature and shall only act on the content if the authenticity and integrity of the RAP is verified. If the RAP cannot be authenticated, or if the integrity validation fails, the RAP shall be discarded.

3a.3 Signature creation

For the purposes of the non-repudiation service defined in clause 5.4 the RE shall be able to generate evidence of actions related to the use of RAs and sign the evidence (actions may include installation, deletion, operation). For Tier#2 the RE shall act as Secure Signature Creating Device (SSCD), and for Tier#3 the RE shall act as a Qualified Signature Creation Device (QSCD) in accordance with the eIDAS directive [9].

NOTE: The eIDAS directive does not require all signatures to be compliant but as one of the purposes of the non-repudiation service in RRS is to provide proof of an action occurring, that may be tested within a legal framework such as that used for market control of radio equipment, requiring Tier#3 equipment's non-repudiation signatures to be created using a QSCD is intended to increase the assurance of the corresponding RRS equipment across the market control domain.

3a.4 Trusted timestamp

3a.4.1 General requirements

For the purposes of the non-repudiation service defined in clause 5.4 the RE shall be able to generate evidence of the time any actions related to the use occurred and include the timestamp in the evidence generated.

3a.4.2 PKI based trusted timestamps

For Tier#2 devices a Trusted Timestamp complying to IETF RFC 3161 [20] shall be generated. For Tier#3 devices a Trusted Timestamp complying to ANSI X9.95 [21] shall be generated that in addition to providing 3rd party assurance of the time of the action also provides for proof of the integrity of the timestamped data.

3a.4.3 Blockchain based trusted timestamps

An alternative to PKI based trusted timestamps is to adopt a blockchain based approach such as that defined in [i.7] that removes the requirement for a centralized Trusted Timestamp Authority (TTA) and replaces it with the distributed trust model of a blockchain. The current version of the present document only supports PKI based trusted timestamps with a centralized TTA.

3a.5 Secure storage

In addition to security keys held by the RRS elements to allow for validation of signed content, and for Tier 2 and Tier 3 systems to generate signed content the following elements shall be maintained in secure storage:

- Evidence generated by the non-repudiation service.
- Proofs of RAP integrity and the binding of a RAP to the RE.

NOTE: Proofs of RAP integrity and the binding to an RE require the use of a Root of Trust for Measurement as described in clause 9.

The characteristics to be met by the secure storage element are the following:

- Tamper resistant.
- Tamper evident.
- Persistent.

3a.6 Remote attestation

Remote attestation for RRS enables an RE to prove to a remote system the authenticity and integrity of its hardware and software configuration. Thus for RRS the authorized remote system is able to determine the level of trust in the integrity of the RE. The remote attestation service extends the non-repudiation service by allowing for online attestation and delivery of proof (i.e. for non-repudiation the evidence of an action is made available to a trusted third party at the time of the action, whereas for remote attestation evidence of the integrity of the platform is given on demand).

The scope of remote attestation is limited, as defined in ETSI TR 103 087 [i.1], to the following use cases:

- Verification of compliance to the essential requirements of the RED [i.13] 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; and,
- Verification of specific type and version of a Radio Application for access control by a mobile network operator.

The detail definition of the remote attestation service is given in clause 10 of the present document.

3a.7 Configuration control

3a.7.1 Local configuration control

The purpose of configuration control is to only allow installation and operation of RAPs that are listed in the RE Configuration Policy.

The RE Configuration Policy shall be made available to a policy enforcement entity and the following pseudo code implemented (details are given in clause 11 of the present document):

```
IF <<RAP>> EXISTS IN <<RE Configuration Policy>> THEN PERMIT, ELSE DENY.
```

3a.7.2 Remote configuration control

The remote configuration control service extends the local configuration control service by enabling the authorized party to be external to the RE (details are given in clause 11.4 of the present document).

3a.7.3 Long term management

The long-term management service extends the local configuration control service by enabling the transfer of configuration authority over the RRS Platform from one entity to another (details are given in clause 11.5 of the present document.

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.

NOTE: It is the nature of an objective to be a signal of intent and thus objectives are phrased using the term "should". The translation of objectives to mandates is addressed in this clause by the mapping from objective to each of strategy and countermeasure.

Table 1: Review of security objectives

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
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 unauthorized 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	Tier#1
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	Tier#1
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	Tier#1
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	Tier#1