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

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

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
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	n/a (see note 13)
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	Tier#1
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	Tier#1
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	Tier#3
9	The RRS platform should provide means to prevent the RE denying receipt of an RA from the Radio application store			Tier#3
10	The RRS platform should provide means to prevent the RE denying installation of an RA from the Radio application store			Tier#3
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	n/a (see note 14)
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	Tier#3
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	Tier#1
		Maintenance and distribution of blacklist of invalid DoC identities	PKI	n/a (see note 15)
		Online verification of signature of DoC	PKI	n/a (see note 15)
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	Tier#1 (see note 16)
		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	

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
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	Tier#2
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	Tier#2
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	Tier#3
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	n/a
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	Tier#2
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	n/a
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	Tier#3
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	Tier#1 (secure storage)
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	Tier#1

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
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	n/a
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	Tier#1
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 DoC documents shall be developed in line with the operational framework of the Digital Signature Directive [8] and the eIDas Directive that will supersede it [9]	Liability framework	n/a
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	Tier#3
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 RE platform shall include a RTS facility (see clause 9) and on receipt of the DoC or the RE Configuration Record shall retain the hash in a Platform Configuration Register (PCR), and accessible using the RTV facility of the root of trust	Secure storage	Tier#1
30	The RRS platform should allow for verifying that the presented DoC is bound to the device		Local and Remote attestation	Tier#3
31	The configuration enforcement framework should provide means to ensure that the command APDUs are protected from exposure to 3rd parties	Encryption of the command APDU (refer to ETSI TR 103 087 [i.1], clause 10.4.2) understood to be the command itself. The APDU may contain its own header to complement the capabilities of the underlying transport mechanism	Confidentiality at the application layer	Tier#2
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 (see note 10)	The command APDU shall be appended with a signed hash covering the APDU header and payload. The APDU header shall contain the public key identifier allowing verification of the signed hash	Digital signature	Tier#2
33	The configuration enforcement framework should provide means to protect against traffic manipulation	In addition to the above, each command APDU shall contain a unique message identifier. Implementations shall discard duplicates of a command based on the identifier	Integrity	Tier#2
34	The configuration enforcement framework should ensure that malformed commands cannot compromise the proper operation of the RE	The data model defined in ETSI TR 103 087 [i.1], clause 10.4.2 shall be translated into a grammar for which the complexity allows for decidability of the recognition problem. Parsers shall strictly abide to the defined grammar	Langsec	Tier#2

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
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	Binding of the public/private key pair used for the signed hash to the unique identity of the command originator	Identity management	Tier#2
		Offline provisioning of public keys on the RE	PKI	Tier#2
36	The configuration enforcement framework should provide means for a network entity to verify the identity of the RE (see note 2)	The RE shall have a unique identity that is bound to the RE device certificate.	Authentication and Identity Management	Tier#3
37	The configuration enforcement framework should not process control messages that have not been issued by an authorized entity	The implementations on the RE and in the network shall discard command APDUs for which verification of the signed hash fails	Digital signature	Tier#2
		A command APDU shall be discarded when the issuer's identity (after successful verification of the digital signature) is not part of the set of identities authorized to issue said command	Authorization	Tier#2
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	Use of a signed hash over the command APDU provides the required non-repudiation property	Digital signature	Tier#3
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	Encryption of content	Confidentiality	Tier#3
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	Encryption of content	Confidentiality	Tier#3
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	Encryption of content	Confidentiality	Tier#3
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	Integrity checksum added to content	Integrity	Tier#3
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	Integrity checksum added to content	Integrity	Tier#3
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	Integrity checksum added to content	Integrity	Tier#3

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
45	The long-term management framework should provide means for the RRS-CA and RRS-CP to verify each other's identity	The RRS-CA shall have a unique name that is tied to its attribute as an RRS-CA in the form of a public key certificate with an attribute extension; The RRS-CP shall have a unique name that is tied to its attribute as an RRS-CP in the form of a public key certificate with an attribute extension	Authentication and Identity Management	Tier#3
46	The long-term management framework should provide means for the RRS-CA and RRS-CM to verify each other's identity	The RRS-CM shall have a unique name that is tied to its attribute as an RRS-CM (as a specific application on the RE) in the form of a public key certificate with an attribute extension. For communications between the RRS-CA and the RRS-CM, a means to verify the credentials of the RRS-CA shall be provided in the TAD	Authentication and Identity Management	Tier#3
47	The long-term management framework should provide means for the RRS-CP and RRS-CM to verify each other's identity	As above. For communications between the RRS-CP and the RRS-CM, a means to verify the credentials of the RRS-CP shall be provided as part of the RRS-CP Profile	Authentication and Identity Management	Tier#3
48	The long-term management framework should provide means for the RRS-CM to verify the integrity of the TAD at receipt	The RRS-CA shall create a signed hash of the TAD, and supply the signature with the attribute certificate of the TAD allowing verification of the hash and signature by the receiving party using the contained or referenced public key	Integrity	Tier#3
49	The long-term management framework should provide means for the RRS-CM to verify the source of the TAD (see note 11)	The identity of the originating RRS-CA shall be mapped to the 'Originator' field in the TAD. Verification of the TAD signature shall result in proof of the source of the TAD	Authentication and Identity Management	Tier#3
		Each accepted TAD and public keys necessary to verify TAD signatures shall be permanently stored on the RE	Secure storage	Tier#3
		The RE shall reject a new TAD when the verification path does not lead to the TAD of the first valid RRS-CA for the RE	Authentication and Identity Management	Tier#3
50	The long-term management framework should provide means for the RRS-CM to verify that the TAD applies to its source (see note 11)	The identity of the beneficiary RRS-CA shall be mapped to the 'Beneficiary' field in the TAD. The TAD shall contain the public key of the beneficiary RRS-CA matching the identity of the beneficiary	Authentication and Identity Management	Tier#3
51	The long-term management framework should provide means to avoid circular transfer of authority	The RRS-CM shall keep a copy of each TAD and reject a new TAD when the beneficiary is the beneficiary of any previously accepted TAD	Implementation	Tier#3
52	The long-term management framework should provide means to prevent an RRS-CA from transferring its authority more than once. (see note 12)	As above where the RRS-CM shall reject a new TAD when the originator of the TAD is the originator of a previous TAD	Implementation	Tier#3

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)
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	As above where the RRS-CM shall reject a new TAD when the originator of the TAD is not the beneficiary of the last valid TAD	Implementation	Tier#3
53	The long-term management framework should provide means for the RRS-CM to verify the integrity of the RRS-CP Profile at receipt	The RRS-CA issuing the RRS-CP Profile shall create a signed hash of the RRS-CP Profile and supply the signature with the attribute certificate of the RRS-CP allowing verification of the hash and signature by the receiving party using the contained or referenced public key	Integrity	Tier#3
54	The long-term management framework should provide means for the RRS-CM to verify the source of the RRS-CP	As above where the RRS-CP Profile has been signed by the originator verification of the signature shall result in proof of the source of the RRS-CP Profile	Authentication and Identity Management	Tier#3
55	The long-term management framework should provide means for the RRS-CM to verify the integrity of the RRS Configuration Profile at receipt	The RRS-CP issuing the RRS Configuration Profile shall create a signed hash of the RRS Configuration Profile and supply the signature with the attribute certificate of the RRS Configuration Profile allowing verification of the hash and signature by the receiving party using the contained or referenced public key	Integrity	Tier#3
56	The long-term management framework should provide means for the RRS-CM to verify the source of the RRS Configuration Profile	As above where the RRS Configuration Profile has been signed by the originator verification of the signature shall result in proof of the source of the RRS Configuration Profile	Authentication and Identity Management	Tier#3

Id	Text of objective	Countermeasure	Strategy	Applies to … (minimum security tier)

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.
NOTE 10: The selection of this countermeasure assumes that the underlying transport mechanism can accommodate large enough payloads such that a digital signature can be included - as possible with SMS-PP [i.10] and SMSCB [i.11].
NOTE 11: In objective 49 the source should be understood as the originator of the TAD (the previous RRS-CA). In objective 50, the source should be understood as the new RRS-CA which presents the TAD to the RRS-CM.
NOTE 12: The long-term management framework is constructed so as to avoid the involvement of a trusted third-party.
NOTE 13: The communications channel between the RE and the Radio Application Store is not described in the present document.
NOTE 14: The developer is responsible and liable for the correct functioning of the RAP but this is not tested within the scope of the present document. In this case the developer is expected to apply best industry practices in software development and verification prior to delivery of the RAP.
NOTE 15: The nature of the PKI is outside the scope of the present document although best practices should be followed in its management, including the timely distribution of certificate revocation lists (see e.g. IETF RFC 5280 [i.20] and IETF RFC 6218 [i.21] for an example application).
NOTE 16: A digitally signed DoC shall include in the scope of the signature a flag identifying the signed object as original. This shall be in the form of an attribute value in the subjectDirectoryAttributes extension of DoC_Original, or DoC_ValidatedCopy.

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 ETSI TC CYBER, working group QSC, 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 (at least) 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 may be 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 [i.14].

5.2 Identity management and authentication

5.2.1 Identity of entities in RAP and DoC lifecycle

The general model of identity management given in ETSI TR 187 010 [i.23] consists of the following 3 actors:

- Principal:
  - Often synonymous with the end-user or an electronic agent of the end-user;
  - The entity being identified.
- Identity Provider (IdP):
  - The organization generally required to authenticate the Principal and to provide an assertion of this authentication to the Relying Party;
  - The entity giving authority to the name.

NOTE 1: In some instances where the identity is self-asserted the principal and the identity authority are one and the same entity although for the purposes of the present document the nature of the roles is distinct.

- Relying Party (RP):
  - An organization providing a service to the Principal;
  - The RP may be willing to rely on an assertion of the identity of the principal provided by the IdP

NOTE 2: This is the normal practice where identity is asserted within a public key architecture and the principal offers his identifier within a public key certificate that has been verified by the IdP.

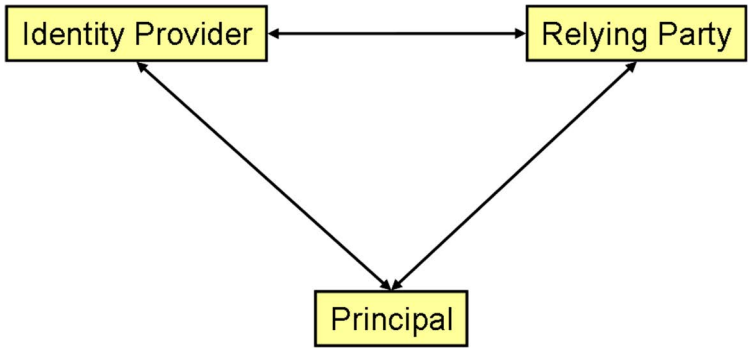

Figure 0: The three primary roles in the common IdM thematic model

The following entities, acting as the Principal from the model given in figure 0, shall be named and authenticated by the Identity Manager in the process of RAP and DoC Distribution, Development and regulatory compliance.

- The Developer of RAP shall be identified by an identity form of Public Key Certificate (PKC) according to Recommendation ITU-T X.509 [5].
- The Application store shall be identified by an attribute form of PKC according to Recommendation ITU-T X.509 [5] with a subjectDirectoryAttributes extension containing the attribute RRS_APPLICATION_STORE.

NOTE 3: The attribute form of certificate extends the public key certificate but does not contain the public key which is contained in the tied PKC.

- The RE Manufacturer shall be identified by both an identity form, and by an attribute form, of PKC according to Recommendation ITU-T X.509 [5] with a subjectDirectoryAttributes extension containing the attribute RRS_RE_MANUFACTURER.
- The Conformity Contact Entity shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_CCE.
- The Market Surveillance Body shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_MARKET_SURVEILLANCE.
- The Disturbance Control Body shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_DISTURBANCE_CONTROL.
- The Radio Network Manager shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_RAN_MANAGER.
- The RRS-CA shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_RRS_CA.
- The RRS-CP shall be identified by both an identity form and an attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_RRS_CP.

NOTE 4: The RRS-CM is viewed as an internal function of the RE and is thus identified as coincident with the RE and shares the identity of the RE (see clause 6.4).

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 [i.15].

There are a number of ways of achieving authentication where for each specialization the countermeasure remains constant: to give assurance that Bob is really Bob and not Alice (i.e. to counter masquerade). An example of the specialization hierarchy for authentication is shown in figure 1.

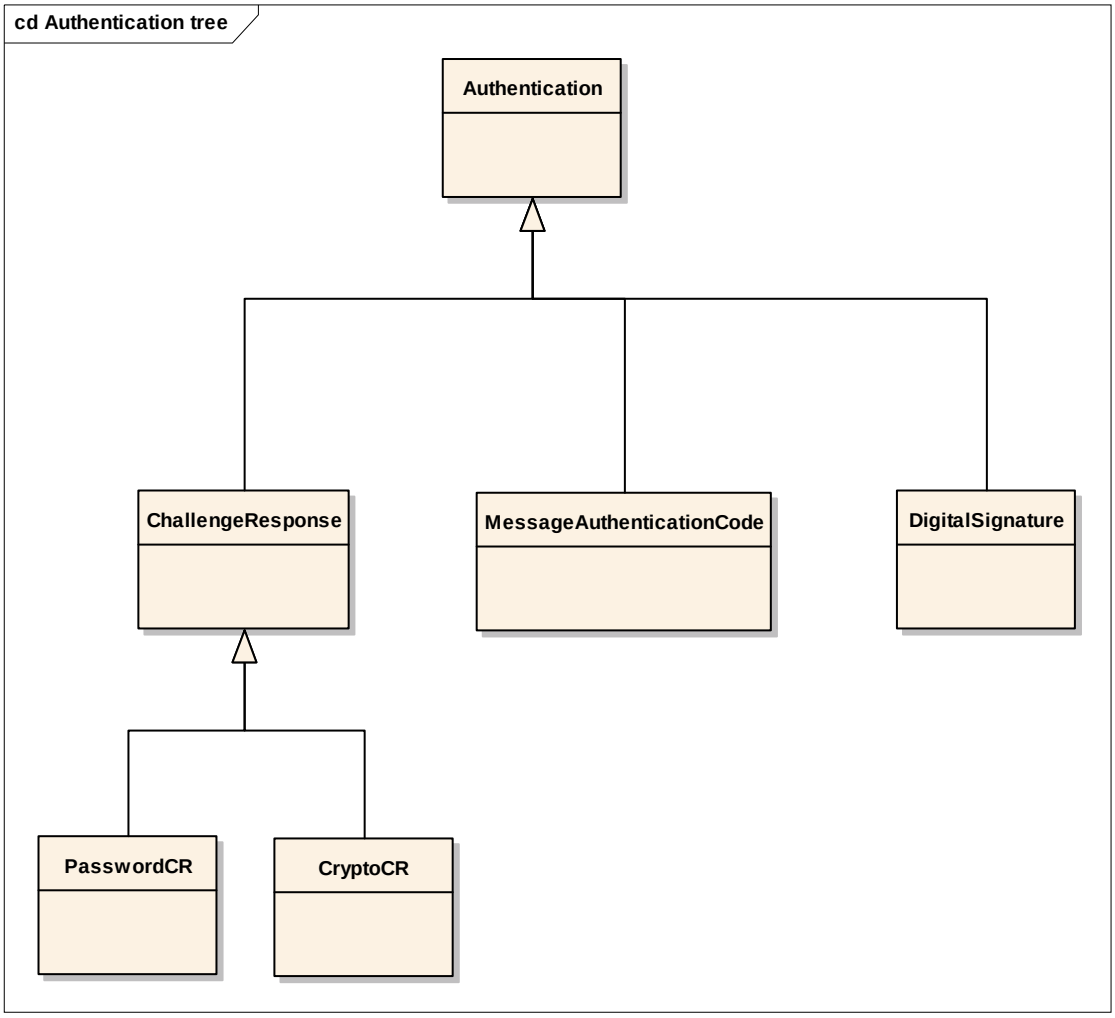

Figure 1: Authentication countermeasure specializations

Whilst challenge response protocols may be based on a username-password combination this is categorized as weak (see annex on strong passwords) and is not considered further in the present document (see also annex B).

5.2.2 Class and role based identity

A RAT shall indicate its type (e.g. GSM-900), its software version number, and link to the developer identity. The RAT type shall be indicated in the DoC in the case of a machine readable DoC. For a 3G cellular radio RAT the IMEI-SV shall act as the radio equipment identity with the following assertions made:

- For RRS the International Mobile Equipment Identity (IMEI) structure shall be identical to that of any other 3G device and allocated in an identical manner.
- The Mobile Equipment Type Identifier (METI) shall be attested to by the manufacturer and maintained by the Reporting Body.

The METI identifies the forms of RAT assigned to the ME. The ME is the specific instance of a Reconfigurable Equipment.

As indicated in clause 5.2.1 each entity shall be assigned to a specific role in RRS and that role shall be attested to using an attribute form of PKC according to Recommendation ITU-T X.509 [5]. All of the roles shall be defined in the Object Identifier Tree as follows:

- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-rap (0)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-market-surveillance (1)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-application-store (2)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-re-manufacturer (3)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-disturbance-control (4)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-ran-manager (5)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-rrs-ca (6)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-rrs-cp (7)
- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-cce (8)

5.3 Document integrity proof and verification

5.3.1 Overview of process

The developer of the RAP shall provide proof of the integrity of the package. The proof of integrity shall be provided by digital signature of the entire package (commonly referred to as document) to be delivered. Most commonly this is achieved by encrypting the cryptographic hash of the document using the private key of the signer and distributing the signed hash with the public key of the signer and the document.

The process extends that used for general distribution of Java Midlets and is summarized in figure 1 for application in RRS.

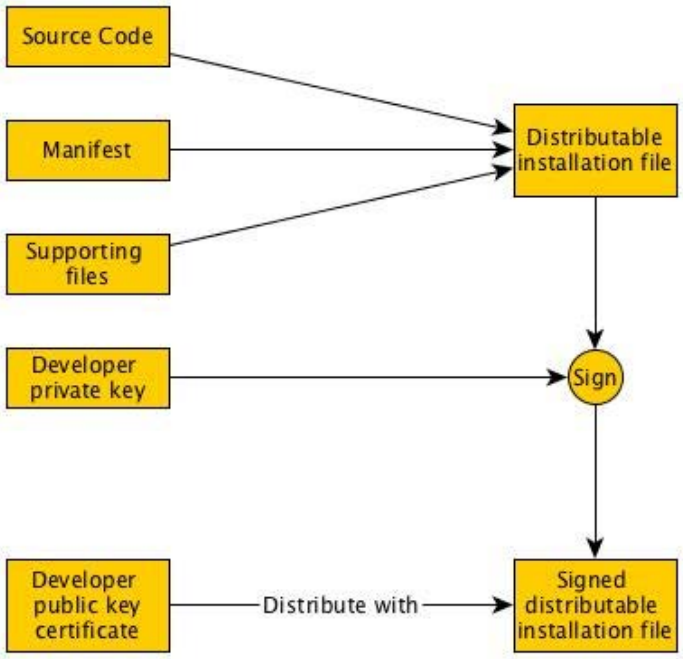

Figure 2: Simplified distribution of signed RAP

The software developer of a RAP shall distribute software as a signed data object in the context of an Recommendation ITU-T X.509 [5] digital signature. The software to be distributed shall be identified as of type RRS-RAP using the Object IDentifier (OID):

- itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-rap (0)

NOTE 1: The ASN.1 OID is defined within the ETSI deliverable branch of the OID tree.

The developer of the RAP shall include a copy of the DoC for the target platform in the set of supporting files such that the relevant DoC from the perspective of the developer is distributed for comparison to the DoC that exists in the RE prior to installation.

NOTE 2: The developer copy of the DoC has to be able to identify the particular functionality subject to conformance testing that is provided in the supplied software.

5.4 Non-repudiation framework

5.4.1 Overview of non-repudiation

ISO/IEC 10181-4 [i.4] states: *"The goal of the Non-repudiation service is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action in order to solve disputes about the occurrence of the event or action".*

A Non-repudiation service may be considered as a suite of discrete facilities that when considered in a process generate a non-repudiation service. Each discrete facility may be considered using a "use-case" in UML (see figure 3).

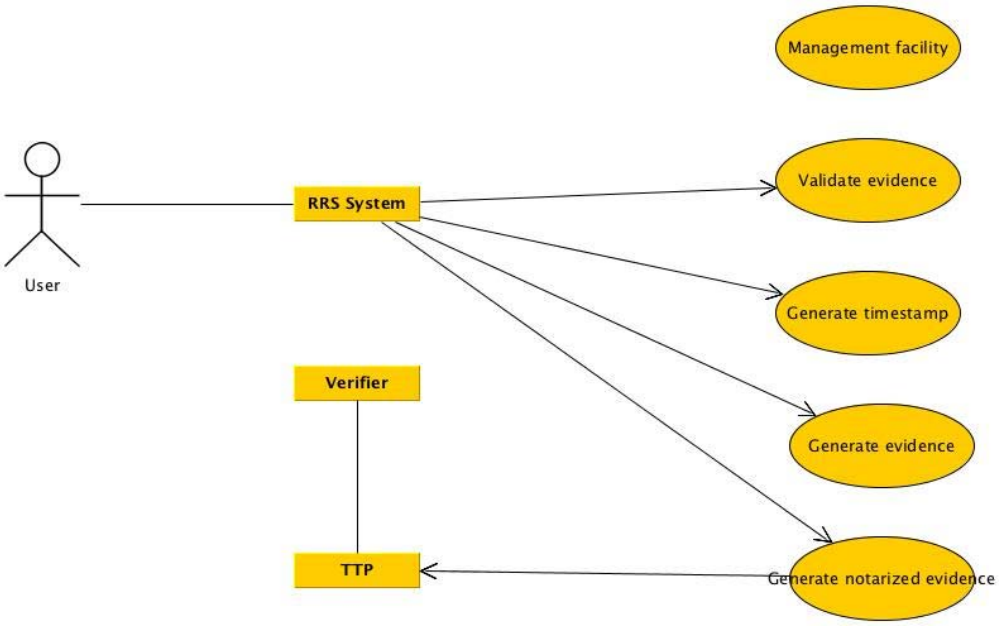

Figure 3: Simplified architecture of use of non-repudiation facilities in NGN

Using ISO/IEC 10181-4 [i.4] as a framework the non-repudiation service involves the generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. Disputes cannot be resolved unless the evidence has been previously recorded.

The purpose of the Non-repudiation service described in this framework is to provide evidence about a particular event or action, in particular the installation of a RAP and the distribution of RAP. Non-repudiation services may be requested by entities other than those directly involved in the event or action, an example for RRS may be the carrying out of regulatory market surveillance and the requirement of proof that the RAP is identified in the DoC and has been installed from a legitimate source.

When messages are involved, to provide proof of origin, the identity of the originator and the integrity of the data shall be able to be confirmed by examination of the appropriate evidence. To provide proof of delivery, the identity of the recipient, and the integrity of the data shall be able to be confirmed by examination of the appropriate evidence. In some cases, evidence concerning the context (e.g. date, time, location of the originator/recipient) may also be required.

5.4.2 Stage 1 model for non-repudiation

5.4.2.1 Procedures

5.4.2.1.1 Provision/withdrawal

Non-repudiation shall always be available.

5.4.2.1.2 Normal procedures

5.4.2.1.2.1 Activation/deactivation/registration/interrogation

Non-repudiation shall always be activated. Non-repudiation shall not be de-activated.

NOTE: These terms are difficult to address as non-repudiation is a composed countermeasure (see clause 5.4.2.2) and requires its composite elements to be activated and de-activated.

5.4.2.1.2.2 Invocation and operation

Non-repudiation is a composed countermeasure, this means that it requires other countermeasures including identity management, authentication, integrity (the latter two may be combined in digital signature). The invocation and operation procedures of the other countermeasures are defined in the present document.

5.4.2.1.3 Exceptional procedures

5.4.2.1.3.1 Activation/deactivation/registration/interrogation

Not applicable.

5.4.2.1.3.2 Invocation and operation

Non-repudiation is a composed countermeasure. The exceptional invocation and operation procedures of the other countermeasures defined in the present document apply in clause 5.

5.4.2.2 Interactions with other security services

In ISO/IEC 10181-4 [i.4] there is a description of how other security services can be used to support non-repudiation. The bulleted list below indicates the relationship between the services.

- Authentication:
  - When entities interact with a TTP they may be required to prove their identity using an authentication service.
- Access control:
  - An access control service may be used to ensure that information stored by a TTP, or service offered by a TTP, is made available only to authorized users.
- Confidentiality:
  - Confidentiality services may be required to protect the data from unauthorized disclosure and also to protect against unauthorized disclosure of evidence.

- Integrity:
  - As the non-repudiation service relies upon proof of particular data either being sent (proof of delivery) or received (proof of receipt) it is imperative that the data item can be shown to be maintained in a known and consistent state which may require the use of integrity services as described elsewhere in the present document.
- Key management:
  - As a non-repudiation service may be cryptographically ensured it is required that the set of keys used in the service is properly managed. There is a description of key management elsewhere in the present document.

6 Information flows and reference points (stage 2)

6.1 Overview

The stage 2 information flows and reference points are extracted from the use case model given in ETSI TR 103 087 [i.1] copied in figure 4.

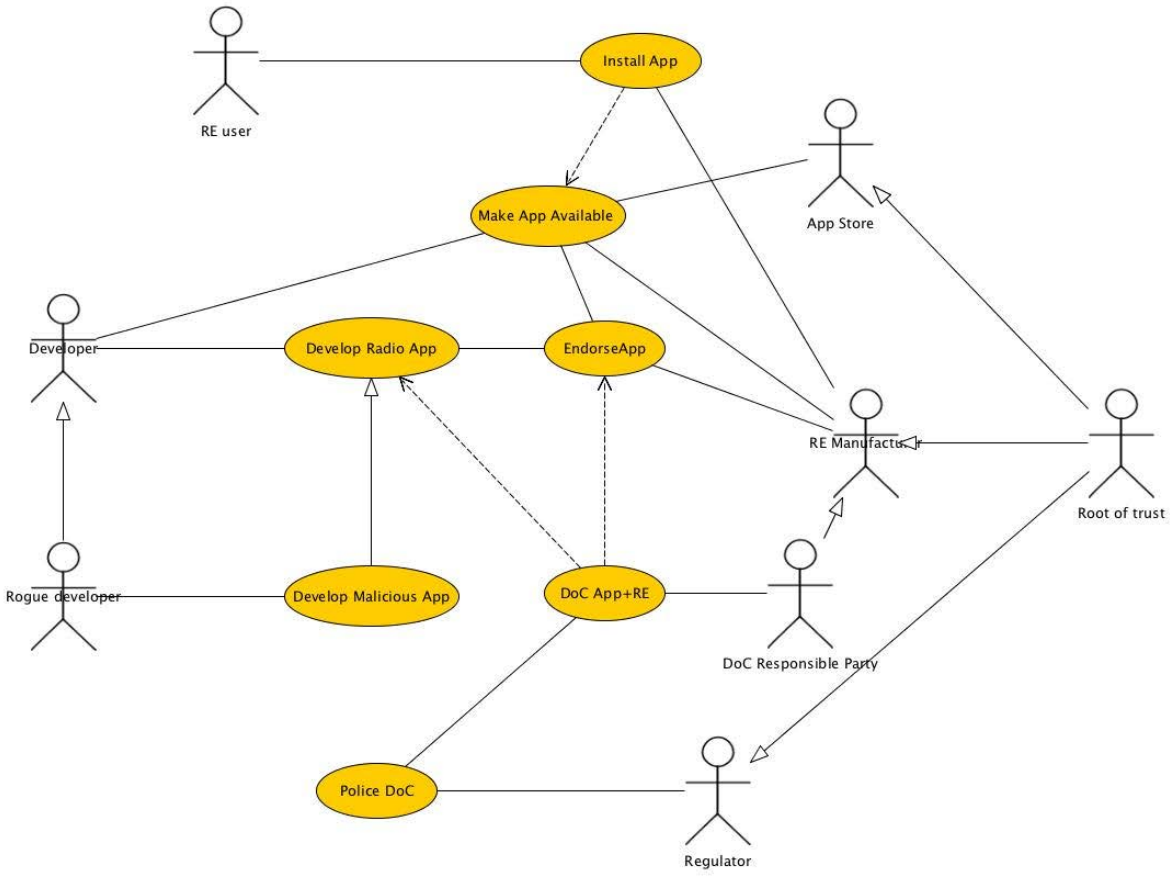

Figure 4: Use cases and actors for RRS application deployment from ETSI TR 103 087 [i.1]

As identified in ETSI TR 103 087 [i.1] the following actors exist in the distribution of RAP:

- Developer
- Rogue developer
- RE Manufacturer

- DoC responsible party
- Regulator
- Application store
- Root of Trust

NOTE: The root of trust in the RE platform itself is described in clause 9 of the present document. In addition the PKI underpinning the digital signature framework provides an external root of trust that is not described in the present document.

Taking note of the capabilities required from table 1 the sets of relationships can be derived for each of the countermeasure strategies as shown in the succeeding clauses.

6.2 Confidentiality

Table 2: Extract from table 1 for "Confidentiality" strategy

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	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
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
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	Encryption of content	Confidentiality
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	Encryption of content	Confidentiality
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	Encryption of content	Confidentiality

The Functional model derived from objectives 1 and 18 is as shown in figure 5 and in table 3. The Functional model derived from objectives 39 to 41 is as shown in figure 5a and in table 3.

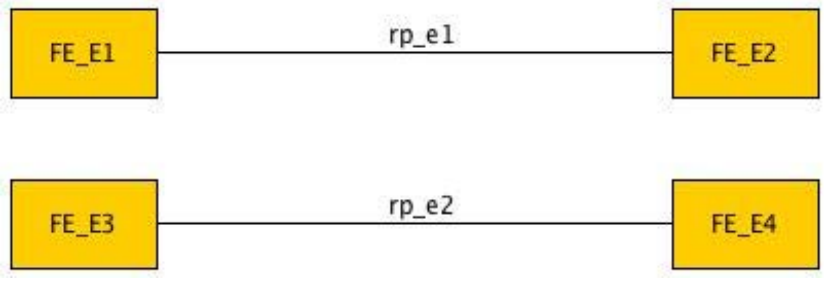

Figure 5: Functional entity model for "Encryption" strategy

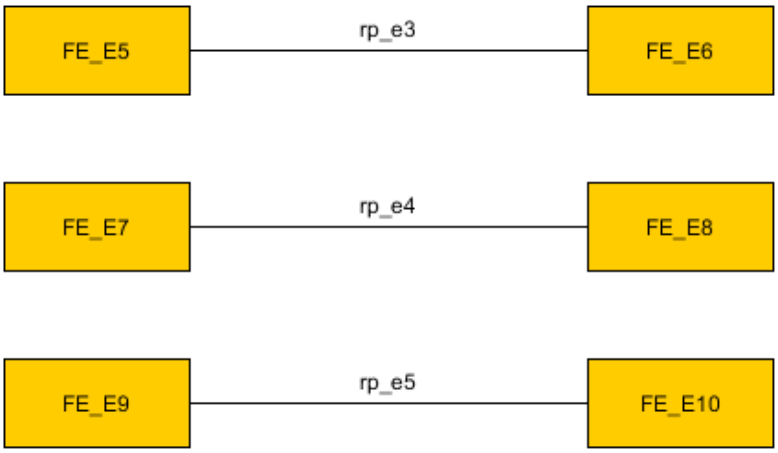

Figure 5a: Functional entity model for "Encryption" strategy of the long-term management service

The functional entities are described in table 3.

Table 3: Functional entity descriptions for Encryption Strategy

FE_E1	Entity representing the RE as a communications end point	rp_e1
FE_E2	Entity representing the application store as a communications end point	
FE_E3	Entity representing the RE as a communications end point	rp_e2
FE_E4	Entity representing the DoC storage location as a communications end point	
FE_E5	Entity representing the RRS-CA as a communication end point	rp_e3
FE_E6	Entity representing the RRS-CP as a communication end point	
FE_E7	Entity representing the RRS-CA as a communication end point	rp_e4
FE_E8	Entity representing the RRS-CM as a communication end point	
FE_E9	Entity representing the RRS-CP as a communication end point	rp_e5
FE_E10	Entity representing the RRS-CM as a communication end point	

Functional capabilities from ISO/IEC 15408-2 [10] for the confidentiality (encryption) capability to be deployed are the following:

- FDP_UCT.1 (User data confidentiality):
  - Basic data exchange confidentiality, the goal is to provide protection from disclosure of user data while in transit.

Functional capability FDP_UCT.1 shall be implemented using the TLS mechanisms defined in clause 7.

6.3 Integrity

Table 4: Extract from table 1 for "Integrity" strategy

Id	Text of objective	Countermeasure	Strategy
2	The RRS platform 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	Integrity check sum added to content	Integrity
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		Integrity
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 or digest of capability should be covered in the signature and integrity check function	Integrity
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
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
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	Integrity checksum added to content	Integrity
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	Integrity checksum added to content	Integrity
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	Integrity checksum added to content	Integrity

Functional capabilities from ISO/IEC 15408-2 for [10] the integrity capability to be deployed are the following:

- FDP_UIT.1 (User Data Integrity):
  - Data exchange integrity addresses detection of modifications, deletions, insertions, and replay errors of the user data transmitted.
- FDP_SDI.1 (Stored Data Integrity):
  - Stored data integrity monitoring, requires that the TSF (Target of Evaluation Security Functions) monitor user data stored within containers controlled by the TSF for identified integrity errors.

The integrity service shall be implemented using the hash functions within digital signature as defined in clause 7.

6.4 Identity management

The identities of the RE Manufacturer, the RAP Software developer, and the Conformity Contact Entity shall be attested using identity public key certificates.

The DoC and RE Configuration Policy shall be identified by association to a specific RE type (see clause 7.5.3.1.1 in ETSI TR 103 087 [i.1]).

The RE instance (RRS Platform ID) shall be identified by serial number in the namespace of a specific RE type (see clause 7.5.2.1.1 in ETSI TR 103 087 [i.1]).

Table 4a

Principal	Identity structure	Relying Party	Identity Manager
RE Manufacturer	X.509 Identity Certificate	RAP provider	FFS
RAP Software developer	X.509 Identity Certificate	RE user Conformity Contact Entity	FFS
Conformity Contact Entity	X.509 Identity Certificate	Market surveillance body Disturbance control body Notified body	Root: Level 1: RAP provider
NOTE: The identification of specific identities of the identity manager is not considered in detail in the present document, rather the deployment of any PKI based identity structure has to be able to assign the identity manager, as trust anchor for the identified relationship in the active management and configuration of the PKI relationships.			

The relying party shall maintain a copy of the PKC of the identity manager relating to each principal role it manages to enable verification of the identity or role of the principal. The PKC shall be stored in the secure storage enclave enabled by the installation of a root of trust for storage as defined in clause 9 and made available to the root of trust for verification when required.

6.5 Non-Repudiation services

6.5.1 Non-repudiation stage 2 models

The generic model for a non-repudiation system consists of 5 functional elements. Some of these elements are also defined in ISO/IEC 10181-4 [i.4].

Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information. For RRS the concept of "Enforced proof of origin" as defined in ISO/IEC 15408-2 [10] shall be implemented such that evidence of origin is always generated for transmitted information.

Information in RRS that is subject to non-repudiation and the entity responsible for generating the proof of origin and the receiving party are as identified as below. In addition, under certain conditions certain 3rd parties may be allowed access to the proofs of transmission in which case there may need to be consent from the intended recipient or other appropriate authorization to view the proof.

The requirements for the non-repudiation service may be stated using functional capabilities as defined in ISO/IEC 15408-2 [10] and shown in table 5.

Table 5: RRS Functional capabilities (Communication class (non-repudiation)) based on ISO/IEC 15408-2 [10] template

Shortname	Definition	Measure in RRS
FCO_NRO.1.1	The system (RRS) shall be able to generate evidence of origin for transmitted RAP associated events and messages at the request of the originator.	When distributing information the distributor shall record the details of the transaction (time, recipient details, originator details, meta-data of the supplied information that shall include the information type (i.e. DoC or RAP), the digital signature of the information). This data shall be maintained in tamper proof storage in read only format.
FCO_NRO.1.1	The system (RRS) shall be able to generate evidence of origin for transmitted RAP associated events and messages at the request of the recipient.	When distributing information the distributor shall record the details of the transaction (time, recipient details, originator details, meta-data of the supplied information that shall include the information type (i.e. DoC or RAP), the digital signature of the information). This data shall be maintained in tamper proof storage in read only format.
FCO_NRO.1.3	The system (RRS) shall provide a capability to verify the evidence of origin of information to originator.	Authorized users shall be able to read the content of the evidential data store and to validate the stored logs.
FCO_NRO.1.3	The system (RRS) shall provide a capability to verify the evidence of origin of information to recipient.	Authorized users shall be able to read the content of the evidential data store and to validate the stored logs.
FCO_NRO.2.3	The system (RRS) shall provide a capability to verify the evidence of origin of information to originator given evidence of origin complies with FCO_NRO.1.1.	Authorized users shall be able to read the content of the evidential data store and to validate the stored logs.
FCO_NRO.2.3	The system (RRS) shall provide a capability to verify the evidence of origin of information to recipient given evidence of origin complies with FCO_NRO.1.1.	Authorized users shall be able to read the content of the evidential data store and to validate the stored logs.

Shortname	Definition	Measure in RRS
FCO_NRR.1.1	The system (RRS) shall be able to generate evidence of receipt for received RAP associated events and messages at the request of the originator.	When receiving information the receiver shall record the details of the transaction (time, recipient details, originator details, meta-data of the supplied information that shall include the information type (i.e. DoC or RAP), the digital signature of the information). This data shall be maintained in tamper proof storage in read only format.
FCO_NRR.1.1	The system (RRS) shall be able to generate evidence of receipt for received RAP associated events and messages at the request of the recipient.	When receiving information the receiver shall record the details of the transaction (time, recipient details, originator details, meta-data of the supplied information that shall include the information type (i.e. DoC or RAP), the digital signature of the information). This data shall be maintained in tamper proof storage in read only format.

7 Protocol sequences and data content (stage 3)

7.1 Confidentiality

7.1.1 Data in transit (encryption)

The encryption capability shall be implemented using TLS [7] with the following constraints:

- Cipher suite selection shall be "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA"

Each party shall be identified by an attested public key certificate containing their public key attested by the root Certificate Authority (CA) for the RRS system.

7.1.2 Data in storage (access control)

Data in storage shall be protected by access control measures. Access shall only be permitted to authorized users or roles. For the DoC read only access shall only be permitted with the following exception:

- If the DoC is modified and the storage needs to be updated this shall only be allowed by the Administration Function of the RE.
- A log shall be maintained at the RE of all updates made to the DoC in a manner sufficient to support the non-repudiation service, thus shall contain a record of the time the DoC was updated, a copy of the hash of the DoC being replaced and of the new DoC being stored.

The mechanism of Access Control is not specified further in the present document.

7.2 Integrity

7.2.1 Data in transit

The integrity verification capability shall be implemented for data in transit using TLS [7] with the following constraints:

- Cipher suite selection shall be " TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA"

Each party shall be identified by an attested public key certificate containing their public key attested by the root CA for the RRS system.

7.2.2 Data in storage

7.2.2.1 Single storage point

The proof of integrity of any document (e.g. DoC) maintained in a store shall be implemented by calculating a cryptographic hash using the Secure Hash algorithm defined in FIPS 186-4 [3] (or as updated by SHA-3 [1]). The calculated hash shall be stored in a secured enclave distinct from the document.

Strict access control shall be provided to ensure that no update to the DoC by an authorized party can be performed without update of the hash. The delta between versions of the DoC shall be recorded in such a way that all changes to the DoC are recorded with the following data:

- Timestamp of the change.
- Signed hash of the original document (complying to ETSI TS 102 778-1 [6] and ETSI EN 319 142 [13] for PDF documents).
- Signed hash of the revised document (complying to ETSI TS 102 778-1 [6] and ETSI EN 319 142 [13] for PDF documents).
- Identity of the authorized party making the change (included within the digital signature for PDF documents).
- Difference record of the changes made between versions (including all formatting and text changes).
- Finally the revised DoC shall be attested by the final author (the authoritative source) using a digital signature conforming to ETSI TS 102 778-1 [6] and ETSI EN 319 142 [13].

For the Declaration of Conformity (DoC) stored in PDF format the authoritative source, and document integrity, shall be attested by the source of the DoC using a digital signature conforming to ETSI TS 102 778-1 [6] and ETSI EN 319 142 [13]. Where the DoC is provided in XML format the provisions of ETSI EN 319 132 [14] shall apply instead of those for PDF documents. Where the DoC is provided in any other binary format the provisions of ETSI EN 319 122 [15] shall apply.

7.2.2.2 Distributed storage points

Each component of the DoC shall follow the process identified in clause 7.2.2.1. In addition the root element of the DoC shall create a hash of the combination of the hashes of each component of the DoC and sign that. Whenever a component of the DoC changes the process identified in clause 7.2.2.1 shall be followed and the DoC root shall recalculate the combined hash.

7.3 Combined authentication and integrity using digital signature

A digital signature is a cryptographically based signature assurance scheme and is used in the context of public key infrastructure (PKI) schemes in which the public key used in the signature scheme is tied to a user by a digital identity certificate issued by a certificate authority. PKI systems use asymmetric key cryptography to unbreakably bind user information (a document) to a public key.

Figure 6 illustrates the digital signature process.

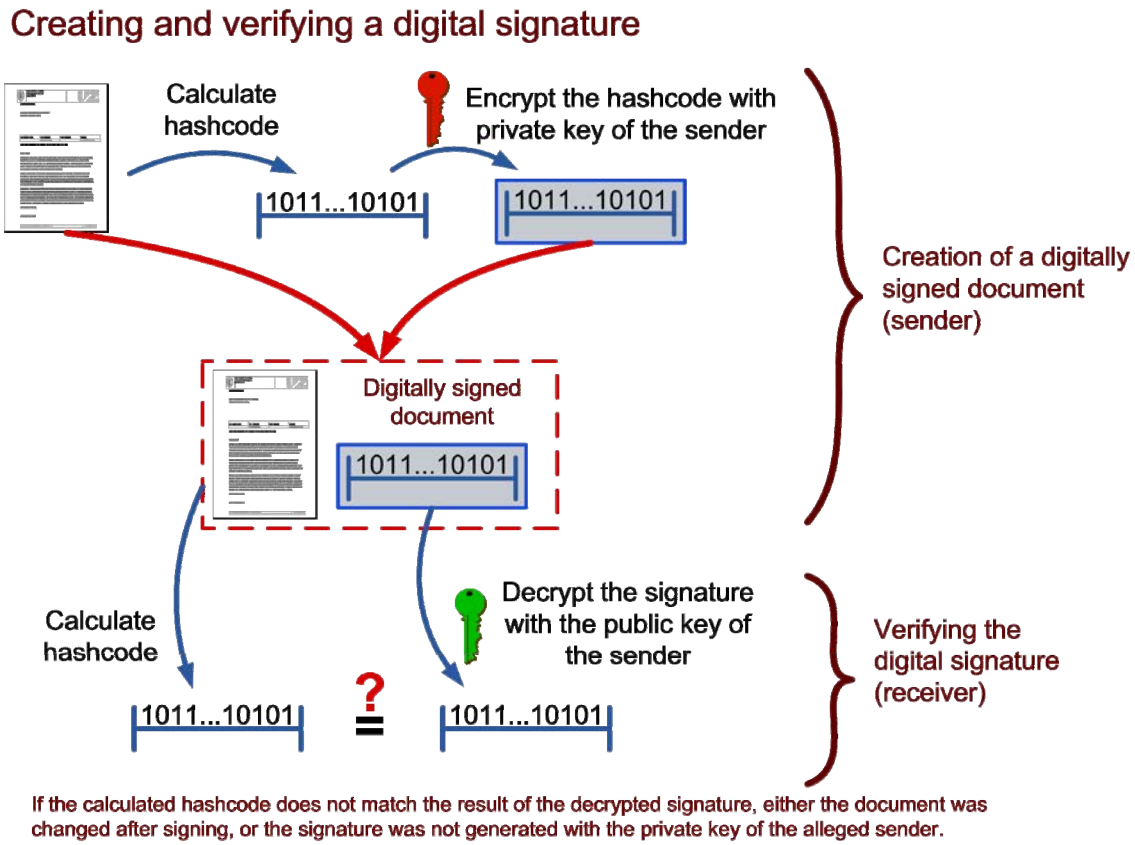

Figure 6: Digital signature process

The hash provides proof of integrity of the document, the encryption of the hash with the sender's private key provides proof of authenticity of identity of the source/sender.

NOTE: It is also possible to combine confidentiality in the signature process by encrypting the document prior to taking the hash. Although confidentiality is not specifically required except for the document in transit it is recommended that the RAP and DoC are each encrypted using the public key of the source prior to the calculation of the hash and the creation of the digital signature.

7.4 Non-repudiation service

The non-repudiation service shall be addressed using digital signature where each signature shall identify by timestamp and form of action the capability of RRS that is not to be repudiated. Digital signatures for distribution of the DoC when in a conventional document form (e.g. PDF, XML) shall follow the requirements of ETSI TS 102 778-1 [6] and ETSI EN 319 142 [13] for PDF documents, ETSI EN 319 132 [14] for XML documents, or ETSI EN 319 122 [15] for any other binary format. The DoC shall be bound to a single class of equipment from a specific manufacturer and shall include with the scope of the signature the combination of RAP and RE covered by the DoC.

The RRS system shall retain, at a trusted third party (TTP) associated to the application store, a record of the request and the subsequent signed delivery of a RAP to a specific RE in order to be able to repudiate any claim of the RE not to have requested a RAP. In addition, the RAP delivery protocol shall include a document complete message and the receipt of this message shall be included in the records maintained at the TTP.

8 Cryptographic algorithm and key considerations

8.1 Symmetric cryptography

For use in TLS [7] the AES algorithm [4] shall be used. This shall be identified in TLS using the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA.

8.2 Asymmetric cryptography

The digital signature algorithm shall be the Elliptic Curve Digital Signature Algorithm (ECDSA) [2] applied to the hash of the message (*m*) where the hash algorithm shall be as specified in FIPS 186-4 [2] or as updated to refer to SHA-3 [1]. This shall be identified in TLS [7] using the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA.

9 Provision of root of trust

NOTE 1: The current version of the present document endorses the TPM model from OGC that has been published as the Trusted Platform Module Library Specification 2.0 with concurrent publication by ISO as International Standard ISO/IEC 11889 [i.16], [i.17], [i.18] and [i.19].

NOTE 2: The cryptographic primitives of the TPM model from OGC are not, in version 2.0, fully cryptographically quantum safe but there is some provision for cryptographic agility. The means to achieve cryptographic agility to give hardware acceleration does mean that a hardware accelerator that is optimized for current public key primitives is unlikely to be optimized for any future quantum safe set of cryptographic primitives.

NOTE 3: The provisions in the present document are described only with respect to the RRS capabilities but the nature of a hardware root of trust and its implementation in a TPM may be extended to other functions that may include secure boot and OS based platform encryption (e.g. whole disk encryption) but such functionality is not described in the present document.

The RRS platform shall implement a root of trust where the scope of functions enabled by the root of trust shall be defined within each RRS Security Tier (see clause 3a of the present document). The trust model provided by the RRS platform is of type Delegated (see clause G.4 of ETSI TR 103 087 [i.1]) where the software entities trust a single designated component for each security function.

The guidelines given in NIST SP 800-164 [i.9] shall be followed in order to provide the following services for all security tiers:

- Root of Trust for Verification (RTV) - this shall provide a cryptographic accelerator to verify digital signatures associated with software/firmware and create assertions based on the results. Shall apply to Tier#1, Tier#2 and Tier#3 devices.

- Root of Trust for Storage (RTS) - this shall provide a protected repository and a protected interface to store and manage keying material (i.e. Public Keys and Public Key Certificates, symmetric keys and their related security association records). Shall apply to Tier#2 and Tier#3 devices. In addition the RTS shall maintain the Platform Configuration Registers (PCR) output from the secure boot and configuration processes. The minimum length of the PCR shall be 256 bits.

NOTE 4: The term Platform Configuration Register is used in the OCG TPM specification to refer to the storage used for platform configuration measurements which are normally cryptographic hash values of the running code.

- Policy Enforcement Engine - to enforce the capabilities described by the RE Configuration Record. Shall apply to Tier#2 and Tier#3 devices.
- Root of Trust for Measurement (RTM) - to undertake the measurement of system state, typically taking a cryptographic hash of the particular platform element.
- Root of Trust for Reporting (RTR) - for use in the remote attestation service and therefore shall apply only to Tier#3 devices.

NOTE 5: The root of trust may be implemented in a number of ways including specific chipsets or by specific combinations of software and chipsets.

The manufacturer of the RE shall attest to the provision of the root of trust by reference to the method applied (e.g. a TCG conformant TPM [25]) and shall publish that attestation in the technical specification of the RE.

NOTE 6: It is not considered possible to verify the existence of a hardware root of trust by a protocol query hence the requirement on the manufacturer to make the attestation as above.

In addition, as identified the definition for root of trust in NIST SP 800-164 [i.9], the presence of the hardware root of trust shall be asserted by platform specific attribute certificate.

10 Remote attestation service

10.1 Applicability

The Remote Attestation service shall apply only for Tier#3 devices.

10.2 Scope of remote attestation service

The scope of the remote attestation service is to provide evidence to the requesting party of the following platform states:

- compliance to the essential requirements of Directive 2014/53/EU [i.13] by the market surveillance authority;

NOTE 1: The attesting party, the RE, is not expected to identify the localized RED essential requirements but they may be provided in the RE Configuration policy. Thus the requesting party, the market surveillance authority, may have to request a record of all enabled capabilities on the platform for offline analysis. This may be provided by provision of the RE Configuration policy.

- RRS platform status for device management purpose by the manufacturer;
- notification of the active set of Radio Applications by the disturbance control authority; and
- notification of specific type and version of a Radio Application for access control by a mobile network operator.

Platform states to be attested to shall be recorded in a Platform Configuration Register (PCR) (see RTS and RTM in clause 9).

Tier#3 devices shall implement the principle of Direct Anonymous Attestation as defined in Annex C of the Trusted Platform Module Library [25].

NOTE 2: To give guarantee of the understanding of the assertion record the content of the PCR should be defined in advance.

10.3 Dependencies of remote attestation service

The remote attestation service shall extend the non-repudiation and local access control services of the RE to identify the requesting party. The requesting party shall indicate to the RE, acting as the attesting party, the form of attestation to be supplied.

11 Configuration control service

11.1 Overview

The security aspects of the configuration control service extend the capability of the RRS-CM entity to specifically address the requirement to only allow installation and operation of RAPs that are listed in the RE Configuration Policy.

11.2 RE Configuration record format

The RE Configuration record shall be provided by the manufacturer in a machine readable format consistent with that used in the Policy Enforcement Engine (PEE) (see clause 9).

NOTE: The RE Configuration record format required for the PEE is not specified in detail as it is internal to the device and is not expected to interoperate with devices from multiple manufacturers.

11.3 Policy enforcement

11.3.1 XACML Model

The eXtensible Access Control Markup Language (XACML) provides a model for policy enforcement that has broad commonality to any generic model of distributed access control. The architecture and message exchange model is shown in figure 7. The entities involved are:

- Policy Enforcement Point (PEP)
- Policy Decision Point (PDP)
- Policy Administration Point (PAP)
- Policy Information Point (PIP)

For mapping to the RRS configuration model the policy that is present in the RE Configuration Policy shall comply to the XACML document structure defined in the OASIS XAML Core Specification [26]. The PEP shall co-exist with the access protected entity in order to restrict access to the protected entity only through the PEP, the remaining XACML architectural elements may be implemented internally to the RE platform.

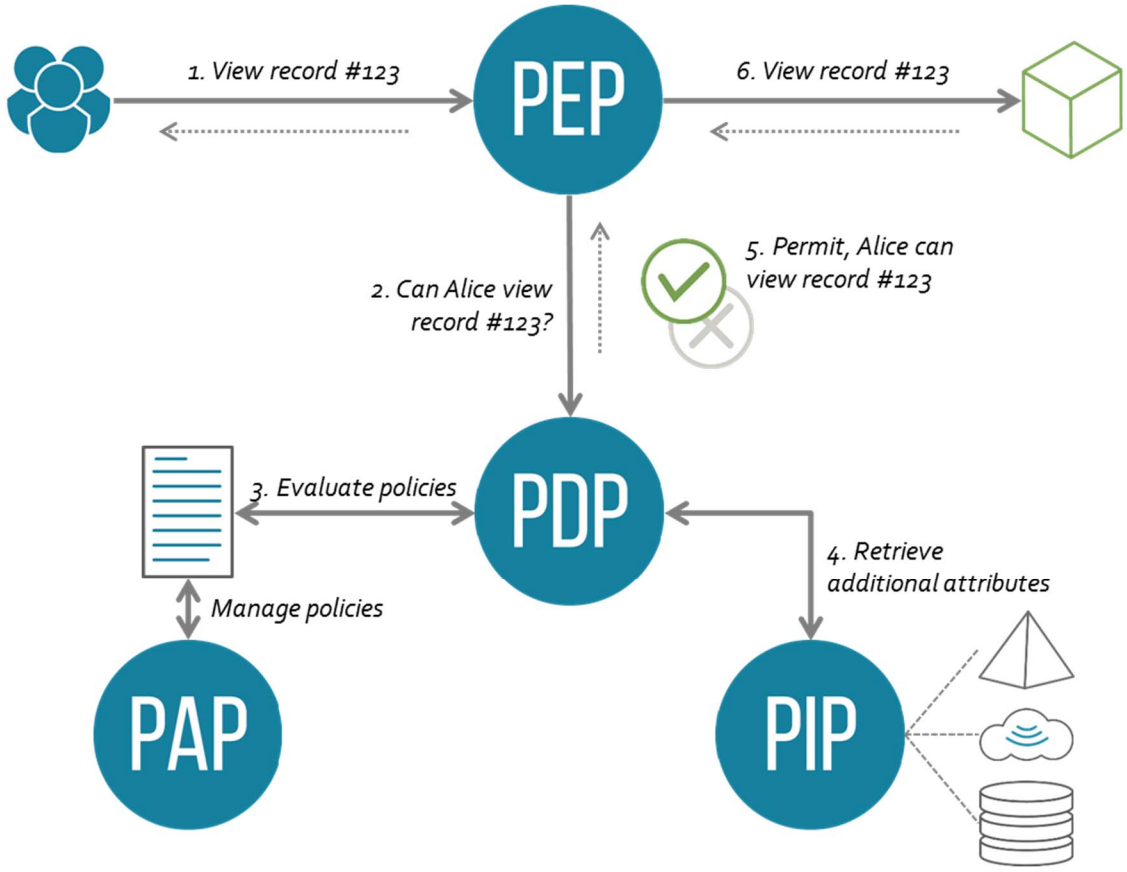

Figure 7: XACML model (unmodified diagram from https://commons.wikimedia.org/wiki/File:XACML_Architecture_%26_Flow.png released under Creative Commons licence CC-BY-3.0)

Where the XACML model is deployed the policy shall comply to the policy structure defined in [26]. An illustration of the policy structure in its component form can be found in [26].

The <condition> statement in an XACML policy shall contain code sufficient to verify the <<to be installed>> RAP exists in the RE Configuration policy. If the <condition> is evaluated as true then the rule and its containing policy, depending on the setting of the policy combination algorithm, shall be evaluated as PERMIT.

The definition of target in XACML for RRS is the platform identified in the DoC.

Figure 8: Void

In XACML whilst there are 4 possible decisions (Permit, Deny, NotApplicable, and Indeterminate) in the RRS context every attempt should be made to disallow the NotApplicable and Indeterminate decisions and thus only allow for Permit or Deny decisions. In the case the rule combining algorithm shall be one of the following:

- urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:deny-unless-permit
- urn:oasis:names:tc:xacml:3.0:rule-combining-algorithm:permit-unless-deny
- urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:deny-unless-permit
- urn:oasis:names:tc:xacml:3.0:policy-combining-algorithm:permit-unless-deny

In all cases the rules in any policy shall all be evaluated, thus in an RRS context the combining algorithms of type first-applicable should be avoided.

NOTE: A policy containing only 1 rule with a combining algorithm of type first-applicable will meet this requirement but if extended without modification of the combining algorithm would subsequently fail the requirement.

11.3.2 TCG TPM Model

The policy enforcement model described by the TCG in the TPM architecture is one of extended authorization built around the content of the various TPM elements. Examples cited in [25] include:

- limitations to the use of a key unless selected PCR have specific values;
- limitations to the use of a key after a specific time;
- limitations to modification of (say) an NV Index be provided by independent authorization grants from two different entities; or
- limitation of scope of a particular signing key to attest to PCR values but not to certify another TPM key.

11.4 Remote configuration control service

The remote configuration control service shall enable configuration enforcement of the RE by an external entity and is introduced in clause 10 of ETSI TR 103 087 [i.1].

The root of trust defined in clause 9 shall provide secure storage of the following:

- the digest of the APDU authorized sender manifest;
- the digest of the safe mode manifest;
- the digest of the snapshot list manifest.

The remote configuration control service should be implemented as a command and control protocol at the application layer of the OSI stack.

Details of the configuration control service and its command structure when operated remotely shall be identical to local operation with the source of the command being a trusted proxy of the configuration control management entity on the RE. Thus prior to delivery of any remote configuration control commands the local control management entity of the RE shall validate the authority and identity of the remote controller. The remote control entity shall provide proof of its identity and authority by signing all configuration control commands to attest to its identity and shall provide its authority in the form of an additional attribute certificate.

NOTE 1: The details of the configuration control command suite are not defined but an illustration of the command set that may be enforced is given in ETSI TR 103 087 [i.1]. When the capabilities of the command suite are defined the provisions in the present document may be updated.

The application layer protocol is not defined in detail but shall support the following requirements:

- The configuration enforcement command and its required proof of source and authority shall be embedded in the payload of the Application Protocol Data Unit (APDU).
- The APDU shall be composed of a transmission header, a payload, and a trailer containing a digital signature attesting to the source and integrity of the content.
- The APDU header shall allow each APDU to be uniquely identified to allow the receiving entity to reject an APDU if it determines that an APDU with the same identification information has already been received in order to prevent replay attacks. The APDU identification may be carried en clair to allow replay processing before performing the signature verification.

NOTE 2: The parsing of the ADPU can be made more secure against error by following the language theoretic security (langsec) principles outlined in annex A of ETSI TR 103 502 [i.12] and whilst the ADPU syntax and semantics are not defined in the present document it is recommended that this langsec approach is followed in future work.

- The APDU payload shall be encrypted using AES in CBC mode:
  - The minimum encryption key size shall be 128 bits or as determined by national security policy.

NOTE 3: The minimum key size specified for AES is 128 bits.

- The sender of the APDU shall provide the payload encryption key in a protected manner:
  - The key transport mechanism should be KTS-OAEP as specified in NIST SP 800-56B [i.22].
- The signature trailer shall contain a digital signature according to clause 8.2 of the present document, where the message (m) shall be the concatenation of the APDU header and payload.
- The APDU header shall contain the identifier of the public key allowing verification of the digital signature.

11.5 Long-term management service

The long-term management service enables the transfer of Conformity Contact Entity, and the associated authority responsible for maintenance of the RE Configuration Record, for the RRS Platform from one entity to another. The RE, and the supply chain associated to it, shall be able to demonstrate the identity of the current Conformity Contact Entity. The proof of transfer of authority shall be contained in the Transfer of Authority Document (TAD). The identity of the RRS-CP shall be contained in the RRS-CP Profile. Identities of other actors shall be contained in the RRS Configuration Profile. The outline of the service is described in ETSI TR 103 087 [i.1], clause 11. The security requirements to be met by the RE when the ToA service has been implemented are described in this clause.

The RRS Configuration Provider (RRS-CP) is responsible for provision of configuration parameters for the RE and is closely associated to the RRS Configuration Authority (RRS-CA) which manages authoritative power over the RE. The RRS-CP is identified using an X.509 identity and attribute certificate as specified in clause 5.2.1.

The essential assets of the long term management service shall be maintained in secure storage using the RTS and RTV facilities described in clause 9:

- A PCR shall be reserved for the following:
  - the DoC;
  - the RRS-CP identifier certificate and the RRS-CP Profile;
  - the RRS Configuration Profile; and
  - the TAD installation log.
- At run time the following shall be verified:
  - RRS-CP identity;
  - RRS Configuration Profile.

In terms of Identity Management (see clauses 6.4 and D.2 of the present document) the relying party for the Conformity Contact Entity (acting as the principal) is one of the Market surveillance body, the Disturbance control body or the Notified body. In each case the relying party has to be assured that if the conformity contact entity is changed by invocation of the procedure outlined in clause 11 of ETSI TR 103 087 [i.1] that the transfer is legitimate and is visible to the relying parties. The conformity contact entity shall always be recorded in the DoC (see annex E for examples of how this has been done for example DoCs under the R&TTE directive).

NOTE 1: The DoC is not described as a machine readable document with a syntax that allows for direct identification of the Conformity Contact Entity format but the RRS Configuration Profile, whilst not defined in the present document, is expected to explicitly identify the Conformity Contact Entity.

Where the conformity contact entity has been changed the DoC held or linked to on the RE shall be marked as "modified". The TAD shall be in the form an attribute certificate according to Recommendation ITU-T X.509 [5] and shall contain the following fields defined as attributes:

- one "effectTime" attribute indicating the time at which the TAD comes into effect (this attribute shall be presented in the syntax of the Recommendation ITU-T X.520 [28] GeneralizedTime type);
- one public key certificate acting as trust anchor for the authentication of the RRS-CA by the RRS-CM for communication security;

- one public key certificate with key usage constrained to digital signature, for the RRS-CA to sign RRS-CP Profiles (defined as the RRS-CA Asset Signature Key);
- the "issuer" field of the TAD shall identify the RRS-CA from which the TAD originates (the origin RRS-CA);
- the "holder" field of the TAD shall identify the RRS-CA to which the TAD applies to;
- The "attrCertValidityPeriod" field shall indicate the time period during which the TAD is valid for processing by the RRS-CM.

NOTE 2: this does not hold the same meaning as the "effectTime" field.

- the TAD shall be signed in accordance with annex A of Recommendation ITU-T X.509 [5] where the private key shall the Asset Signature Key of the origin RRS-CA.

The RRS-CP Profile shall be in the form an attribute certificate according to Recommendation ITU-T X.509 [5] and shall contain the following fields defined as attributes:

- one or more name identifier of RRS-CP (the attribute should build on the Recommendation ITU-T X.509 [5] GeneralName type);
- one public key certificate identifying the RRS-CP as defined in clause 5.2.1 of the present document, for communication security;
- one public key certificate with key usage constrained to digital signature, for the RRS-CP to sign RRS Configuration Profiles (defined as the RRS-CP Asset Signature Key).

The RRS-CP Profile shall contain an empty "holder" field.

NOTE 3: This is because attributes are used to name one or more RRS-CP.

The RRS-CP Profile shall be signed in accordance with annex A of Recommendation ITU-T X.509 [5] where the private key shall be the Asset Signature Key of the currently valid RRS-CA. The "issuer" field of the RRS-CP Profile shall match the identity of the currently valid RRS-CA.

The RRS-CA should provide an RRS-CP Profile revocation mechanism is the form of Recommendation ITU-T X.509 [5] Attribute Certificate Revocation List.

The present document places no requirement on the format of the RRS Configuration Profile.

The RRS Configuration Profile shall be subject to a digital signature from the RRS-CP, where the private key shall be one of the Asset Signature Key of the RRS-CP.

Where the ToA and the change of configuration control entity results in a change to the RE Configuration Record the processes that secure the authority and integrity of the RE Configuration Record described in clause 6 of the present document apply.

Annex A (informative): Cost benefit analysis for countermeasure application

A.1 Sample calculation

The calculation method and the metrics for the cost benefit analysis of the application of countermeasures is defined in ETSI TS 102 165-1 [i.3]. The analysis has been applied to the core countermeasure strategies given in the present document. Thus the digital signature strategy which includes provision of authenticity, integrity and confidentiality countermeasures, and the non-repudiation strategy that extends the digital signature strategy with additional evidence of the delivery and receipt of the DoC or RAP.

Table A.1: Costs benefit analysis for selected countermeasures in RRS

Countermeasure	Cost		Benefit			Result
	Category	Value	Risk Level	Original Count	Revised Count	
Digital signature based authentication and integrity measures	**Standards design**	Low Impact	**Minor**	0	0	**4**
	Implementation	Medium Impact	**Major**	0	0	
	Operation	Medium Impact	**Critical**	6	0	
	Regulatory Impact			Significant Positive Impact		
	Market Acceptance			Positive Impact		
Non-repudiation extension of digital signature based authentication and integrity measures	**Standards design**	Low Impact	**Minor**	0	0	**3**
	Implementation	Medium Impact	**Major**	0	0	
	Operation	No Impact	**Critical**	6	0	
	Regulatory Impact			Positive Impact		
	Market Acceptance			Positive Impact		

For the above analysis each factor has been assessed using the criteria given in ETSI TS 102 165-1 [i.3] and interpreted for the RRS environment as discussed in clauses A.2, A.3, A.4, A.5 and A.6.

The "Original Count" column in the "Benefits" section of the sheet shows the number of critical, major and minor risks related to the countermeasure calculated before its implementation, from the tables given annex E of ETSI TR 103 087 [i.1]. The "Revised Count" column shows the appropriate numbers of risks calculated after the countermeasure has been implemented.

A.2 Standards design

Introducing countermeasures to a standard under development or an existing standard (published) may impose changes affecting the time schedule and resulting in additional effort and cost. The level to which a countermeasure affects the standard design is measured according to the scale in table A.2.

Table A.2: Standards design evaluation

Scale	Description	Assigned value
No Impact	No effect on the time schedule and resources needed of standards under development or no changes needed on existing and published standards.	0
Low Impact	No significant time delay or additional resource demand for standards under development or changes needed on existing and published standards.	1
Medium Impact	Significant time delay and additional resource demand for standards under development and significant changes needed on existing and published standards.	4
Major Impact	Unacceptable time delay and additional resource demand for standards under development and unacceptable changes needed on existing and published standards.	9

Adding digital signature has been assessed as of low impact, as by themselves digital signatures are well understood and the process of adding them to the standards (the present document in particular) is relatively low. However, there is some impact on the overall RRS standards work with the inclusion in the architecture of signature creation and verification objects.

A.3 Implementation

Adding countermeasures to standards may affect its adoption and implementation in the targeted user community. This is an important aspect of standards adoption and crucial for countermeasure cost-benefit analysis. The level to which a countermeasure affects implementation of the standard is measured according to the scale in table A.3.

Table A.3: Implementation evaluation

Scale	Description	Assigned value
No Impact	No effect on standards adoption in the targeted user community.	0
Low Impact	No significant effect on standards adoption in the targeted user community.	1
Medium Impact	Significant effect on standards adoption in the targeted user community.	4
Major Impact	Unacceptable effect on standards adoption in the targeted user community.	9

The cost of implementing digital signature is not insignificant as the set of actors needing to be involved in the signature chain are not all in the position to adopt such measures. For most developers of "Apps" such measures are already applied for a number of application stores. The implementation assumption here is that the existing application stores may not be applicable to RRS.

A.4 Operation

Countermeasures may impact the ongoing operation of standardized products or systems once they have been deployed into an operational environment. The level to which a countermeasure affects the operation of standardized products is measured according to the scale in table A.4.

Table A.4: Operation evaluation

Scale	Description	Assigned value
No Impact	No effect on operation of realized standards design and targeted operational environment.	0
Low Impact	No significant effect on operation of realized standards design or targeted operational environment.	1
Medium Impact	Significant effect on operation of realized standards design and targeted operational environment.	4
Major Impact	Unacceptable effect on operation of realized standards design and targeted operational environment.	9

As with implementation the assessment is of medium impact as documents are now exchanged electronically and the entire supply chain and dependencies have to become familiar with modifications to operation.

A.5 Regulatory impact

Regulatory impacts concern the influence that the countermeasure may have on ensuring regulatory compliance. Regulatory impact is evaluated according to the scale in table A.5. The impact on regulation is assessed as very favourable as the supply chain is now bound together with a set of cryptographic proofs of delivery and assignment. Assuming the burden of Implementation and Operation are overcome this is the primary rationale for adoption of the methods given in the present document.

Table A.5: Regulatory impact evaluation

Scale	Description	Assigned value
Severe Negative Impact	Unacceptable effect on regulatory compliance requirements.	-9
Negative Impact	Significant negative effect on regulatory compliance requirements.	-4
No Impact	No effect on regulatory compliance requirements.	0
Positive Impact	Significant positive effect on regulatory compliance requirements.	4
Severe Positive Impact	Very favourable effect on regulatory compliance requirements.	9

A.6 Market acceptance

Adoption of a standard into industrial products and its acceptance by the targeted user community determine the success of a standard. Therefore, countermeasures with negative predicted effect on market acceptance should be carefully analysed. The level to which a countermeasure affects market acceptance of the standard is measured according to the scale in table A.6.

Table A.6: Market acceptance evaluation

Scale	Description	Assigned value
Severe Negative Impact	Unacceptable effect on market acceptance.	-9
Negative Impact	Significant negative effect on market acceptance.	-4
No Impact	No effect on market acceptance.	0
Positive Impact	Significant positive effect on market acceptance.	4
Severe Positive Impact	Very favourable effect on market acceptance.	9

The assessment of positive impact is made with the understanding that a radio with the features recommended in the present document will have a longer planned life, be more secure in general and the supply chain for its support more trusted.

Annex B (informative): Password policy guide

Whilst the weak security of username-password is advised against in RRS deployment it is recognized that it is a simple and straightforward countermeasure to deploy. The present annex is therefore a guide to the selection of a password and the integration into a system policy to avoid most of the pitfalls of unsafe or poor passwords.

Password security, measured by the time an attacker will need to guess it, is proportional to the length of the password and the size of the alphabet used to create it. An alphabet of only digits (0,1,2,3,4,5,6,7,8,9) to create an 8-digit PIN would only give 10^8 possible combinations, using only lower case letters an 8-character password would give 26^8 possible combinations, and obviously using a mixed combination of upper and lower case letters and characters would give a dictionary of 62 characters and thus 62^8 combinations, then adding in either more allowed characters or a longer minimum length extends the size even further. The recommendation given in the present document of cryptographic strength is 128 bits. It is possible to identify the number of possible passwords using a particular alphabet and password length in similar way to a typically random key (e.g. AES128 has a possible 2^{128} random keys (the alphabet size is 2, the length is 128)). Thus whilst standard English with 26 letters may have 26^4 possible 4 letter words the actual vocabulary of English has a significantly smaller number of actual 4 letter words (for example English does not allow for repeated letter patterns with more than 2 letters). A password does not need to have linguistic meaning, i.e. the password does not have to be in any vocabulary. Thus a truly random password of length *l* from a symbol set (alphabet) of size *k* has k^l possible values, e.g. an 8 character password from a 64 character alphabet has 64^8 possible values (or $(2^6)^8$ or 2^{48} giving nominal strength of 48 bits).

A good password has to have a high level of entropy, i.e. the measure of randomness should be high, thus for a number of calculations a password of 16 characters has an entropy of between 30 and 40 bits depending on how entropy is assigned to a character in the password, an 8 character password has an entropy of between 18 and 30 again depending on how entropy is assigned to a character, which itself depends on the way the password is generated.

Entropy is closely related to randomness and the rule of thumb for randomness is that if an attacker that can get access to all the historic random elements (all N values) this has to give zero information to correctly guess the value of the $(N+1)^{th}$ element. If this condition is met then the element can be considered as having a random value - but only with respect to the previous elements. However it has to be determined if the randomness can be emulated so that even if prior knowledge gives no greater likelihood of guessing the (N+1)th element a stakeholder has to be assured that knowledge of the context does not allow an observer to guess the (N+1)th element. Message entropy is discussed in a number of mathematical sources but at the root is Shannon's "A Mathematical Theory of Communication" [i.5] although linguistic entropy is addressed in many more texts including [i.6]. Essentially if the attacker knows or guesses that the message can take a small set of values the probability of correctly guessing bit N+1 after receiving bit N tends towards 1 whereas for a random binary alphabet the probability of a correct guess should always be 0,5. In a cryptographic context, where Alice is sending a message m to Bob in the form of a binary string the rule of thumb is that the bigger the entropy of the message *m* the more guesses required by an attacker to guess *m*. Thus in developing a password the target should be to maximize entropy, and also to maximize the number of possible passwords by maximizing either the length of the password or the size of the alphabet. As explained above it is also critical to ensure that all elements of the alphabet have the same chance of being selected in the password and that there is no relationship between elements of the alphabet that would statistically influence the selection process.

Choice of password is often poor and given that it is estimated that there are 220 000 dictionary base words for passwords it would not take an attacker long to work through all of them, and not much longer if all of these base words were "strengthened" using substitution of (say) "a" with "@" or "s" with "5". Attackers will develop and exchange password dictionaries containing all of these common combinations, alongside their hashes using the common hashing algorithms (MD5, SHA, etc.). In practice password dictionaries, pre-calculated rainbow tables, password attack networks, the use of botnets to capture transferred hashes, make immunity from password attacks difficult over a long period and passwords should be routinely changed to minimize exposure. Even using protocols that send the hash of the password such that the password is not easily visible in the clear does not guarantee safety. What the well prepared attacker will do is look up the hash in his dictionary of password hashes and if a match is found he will have the password. This does not require any breaking of the hash function, or direct "guessing" of the password. In part this is because the hash is much longer than the password and most methods simply concatenate copies of the password to an arbitrary length and then has the result. The attacker will adopt the same strategy in building a password dictionary. The resulting dictionaries are still relatively small and easy to exchange.

In order to mitigate the risk from pre-computed password hash dictionaries, it is advisable to use salt-based password hashing functions in which the salt value can span a very large range. If the attacker is able to obtain such a hash and has not pre-computed a dictionary with the salt, they will be forced to brute-force the hash by trying all possible password values until the hashed guess matches the obtained hash. In such situation the security of the password partly relies on the resilience of the hashing function against parallel and hardware-based calculation, as well as on the size of the salt space.

In case the attacker has not obtained the password hash but has access to a device against which they can test password guesses, it is advisable to implement measures such as temporary locking the authentication process or gradually throttling the number of incorrect attempts the attacker can perform over time. Another mitigation consists in limiting exposure of the password hash function to passive and invasive measurement attacks so that the attacker cannot easily gather information which would help reducing the space of password candidates.

Annex C (informative): Key lifetime and verification guidelines

C.1 General

The key size and key lifetime should address 2 major factors of the risk calculation: Access and Time. The access factor is used to determine the likelihood of an adversary gaining access to secured material and time is used to determine how long data has to remain confidential once accessed. A general evaluation of key-lengths for cryptographic operations across a number of standards and government bodies is found in [i.2].

The overall target for RRS deployment in the period to 2030 is that the cryptographic security level should not be less than 128 bits.

C.2 Symmetric cryptography

Where symmetric cryptography is to be used the key lifetime should not exceed 20 years in general if the keys are distributed in tamper resistant hardware. Where keys are not distributed in tamper resistant hardware the key lifetime should be significantly reduced.

C.3 Asymmetric cryptography

Within the context of asymmetric cryptography the private part of the key should be maintained in secure storage, ideally tamper proof hardware, and measures be taken to minimize any exposure of the key as any uncertainty regarding the storage of the private key has a consequential impact on any assertions made with it.

The distribution of keys using a Public Key Certificate requires that the certificate expiry time is embedded in the certificate and verified on each use.

C.4 Export control

Almost all uses of cryptography are subject to export control restrictions. Many countries in which RRS is deployed, developed or manufactured control the export of cryptography in the interests of national security. The present document does not define which parts of the RRS will be subject to such controls but it is useful to note what is generally exempted. Thus the following notes may be used to guide in determining what is exempt, although it is strongly recommended that advice is sought from the appropriate national authority:

- the item is generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of over-the-counter transactions, mail order transactions, electronic transactions or telephone order transactions;
- the cryptographic functionality cannot easily be changed by the user;
- the item is designed for installation by the user without further substantial support by the supplier; and
- when necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in the three points above.

All 4 conditions have to be met for the decontrol to apply (where decontrol refers to the non-applicability of export controls). It is essential to note that items marketed over the internet are subject to the same criteria. For example, cryptographic software and hardware products used to provide high-end backbone infrastructure services - such as high-capacity backbone routers - do not qualify as these items would normally require substantial support by the supplier.

The following interpretations of the main phases are taken from the UK but similar interpretations can be found from most countries:

- "Retail selling points" are places where cryptographic items are readily available - e.g. high street and warehouse shops which facilitate over-the-counter sales, or companies which make sales via mail order, telephone, fax or internet transaction. Purchases from such companies are made by reference to a mail order catalogue, magazine or newspaper advertisement, website, etc. - media which are generally available in their own right.

- "Without restriction" means that a buyer may acquire a product by paying a standard fee to the seller. "Restriction" in this context means either that some persons are excluded from being allowed to buy, or that they are subject to conditions or limitations at the time of purchase, other than those normally arising from copyright - e.g. conditions imposed in a software licence. Other examples of forms of "restriction" include a requirement to be an EU member state resident before purchase can be authorized, or a requirement for the purchaser to undertake that the goods will not be re-sold or given to any person or company from or in a particular country, or that installation can only be undertaken only by authorized engineers.

- "The cryptographic functionality cannot easily be changed by the user" means that the manufacturer has taken reasonable steps to ensure that the cryptographic functionality in the product can only be used according to their specification.

- Installation by the user without further substantial support" - most mass-market products meet this requirement. "Substantial support" does not include purely nominal installation support, such as provision of a telephone or an email helpline to resolve user problems.

Annex D (informative): PKI considerations for RRS

D.1 What is a Public Key Infrastructure?

Asymmetric cryptography allows for the public key to be freely distributed with no impact on system security. At a very simple level a public key is stored as a tuple of {*entity*, *public-key*} but as the number of entities that information is shared with grows there is a reasonable likelihood that the parties do not know each other, thus the simple tuple no longer scales. In addressing the wider use and distribution of public keys there has to be some consideration of trust (see ETSI TR 103 087 [i.1], annex G) to be able to give authority to the underlying relationship expressed in the tuple. The public key can be distributed in a Public Key Certificate (PKC), such as defined in Recommendation ITU-T X.509 [5], to give information to the holder of the public key regarding the owner of the public key and what the key can be used for. A PKC can be attested by a third party as belonging to the entity and the purpose of the Public Key Infrastructure (PKI) is to manage the set of entities that attest for each other. The steps in the design of the PKI are outlined in figure D.1. The first 2 steps have been completed in the present document and in the use cases of ETSI TR 103 087 [i.1].

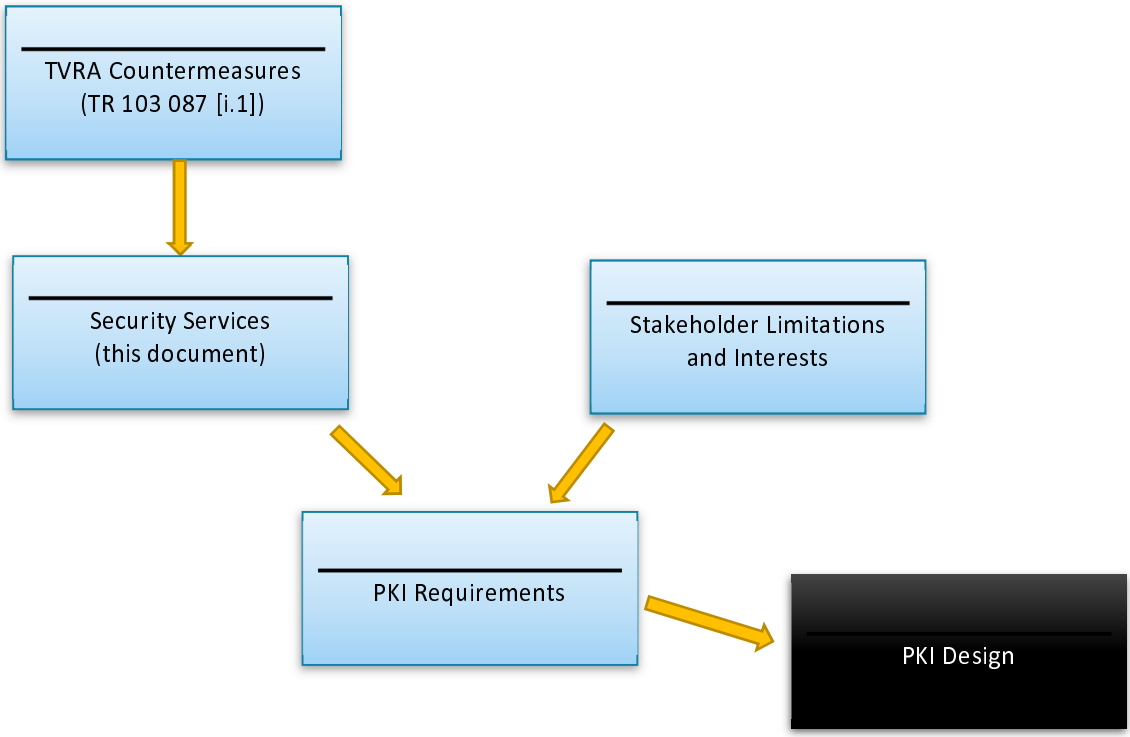

Figure D.1: Steps in the PKI design process

The most common model of PKI structures is a simple hierarchy. The model for certificate trust is conceptually simple: Party A (Alice) certifies that they trust a claim of Party B (Bob) and signs a certificate that proves this and identifies the context for which that trust is given. Bob can then exchange this trust certificate with his correspondents (Eve) and if Eve also trusts Alice they may choose to trust the claim of Bob without having to know anything about Bob other than what has been certified by Alice. The content of the certificate includes the public key belonging to Bob.

The relationship of Alice to Bob and Eve to a large extent determines the level of trust afforded by Eve to any communication from Bob. If all of Alice, Bob and Eve are peers the scalability of the trust model is low, whereas when Bob and Eve are peers but Alice is a higher level authority acknowledged as such by each of Bob and Eve the potential for the scheme to scale is increased. This use of higher level authorities in the PKI leads to the hierarchical nature of most PKIs and their ability to scale across large populations.

When generating an asymmetric key pair the role of the public key certificate is multi-fold:

- It verifies that the authority (Alice) has proven the relationship of the public key to the private key.

- It identifies the operations which the key pair is allowed to be associated with (e.g. encryption, integrity, digital signature).
- It identifies the context in which operations are allowed.
- It may identify the holder of the key pair (key pair association to a person).
- It may identify a specific role (key pair association is to the role).

Each PKC therefore gives qualified claims regarding the use of the key pair.

In the conventional PKI structure such as that shown in figure D.2 everyone trusts the Root CA, but essentially trust has only to be of the layer immediately above where one is operating. So with a 4 layer PKI with layer 1 being the root, then L4 trusts L3 and does not need to have knowledge of L2 or L1, similarly L2 does not have to have any knowledge of the L4 entities that an L3 entity certifies. For RRS it is reasonable to have as few layers in the hierarchy as possible whilst allowing a reasonable management load to be carried.

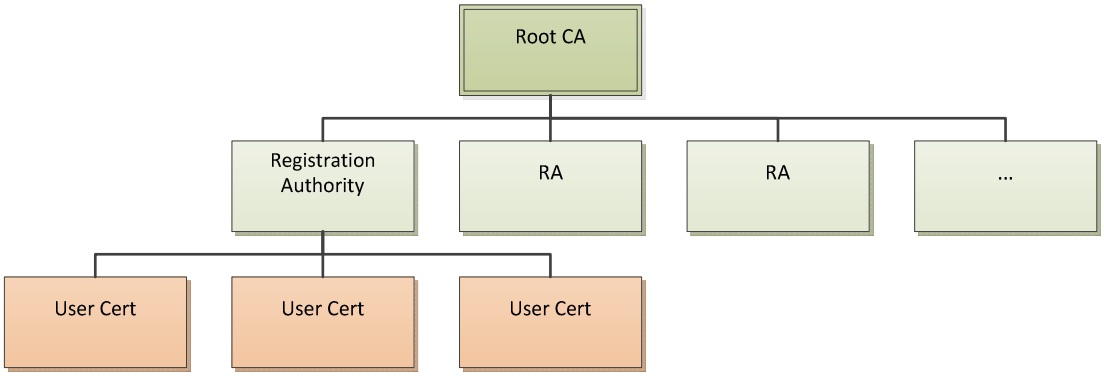

Figure D.2: Conventional PKI hierarchical structure

In summary therefore the PKI allows for the management of PKCs by distributing the trust across layers in a hierarchy.

D.2 Authorities in RRS and their PKI role

The set of authorities, assets and the nature of their relationships are summarized in ETSI TR 103 087 [i.1] and copied in figure D.3.

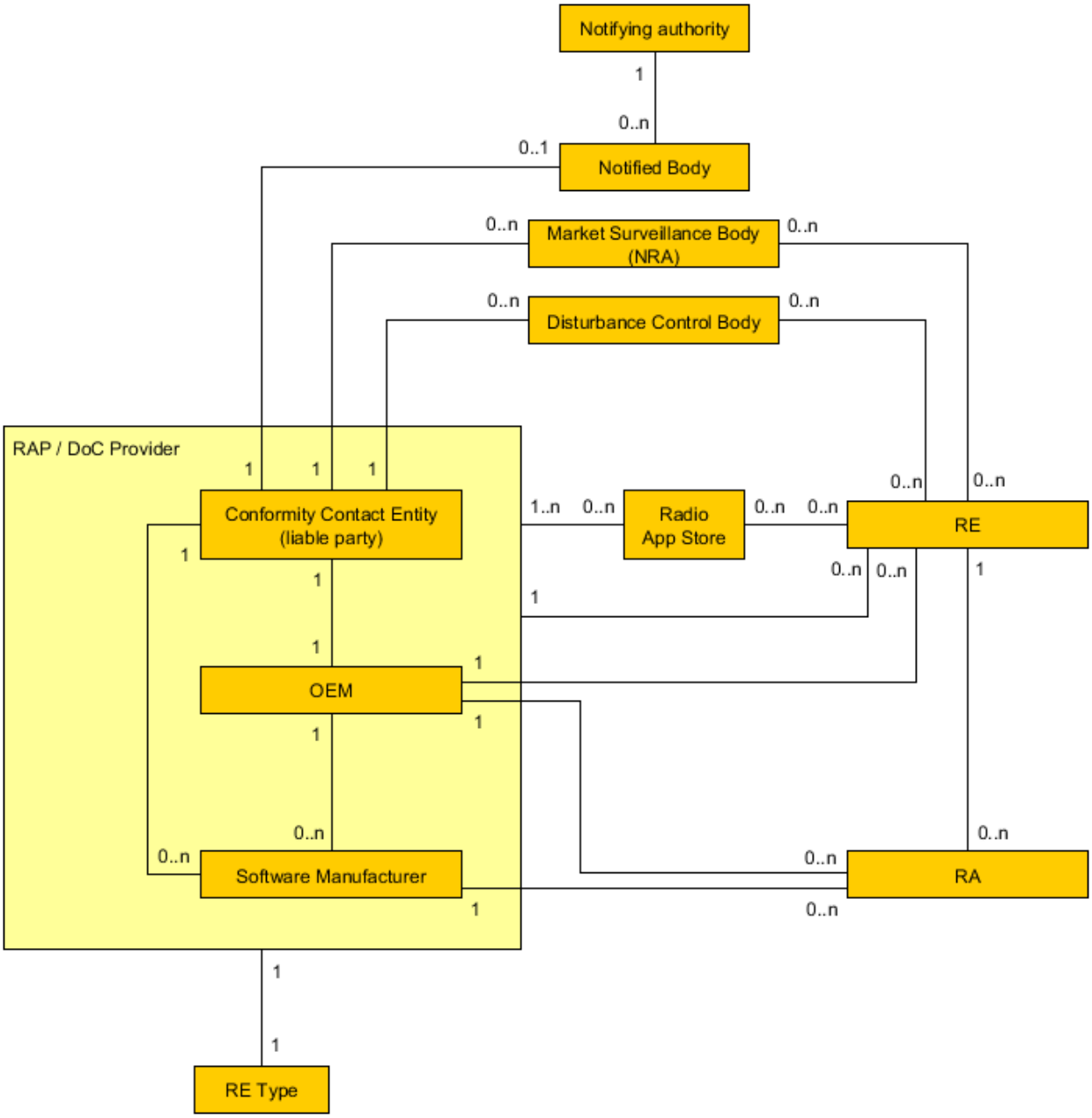

Figure D.3: Cardinalities of stakeholders and assets in RRS from ETSI TR 103 087 [i.1]

As defined in the body of the present document a software developer is expected to attest to the ownership and integrity of the software package (the RAP). The hardware manufacturer is expected to attest to the operation of the RAP on his hardware by countersigning the RAP. In addition, the RAP has to be attested by the DoC Contact Entity by countersigning the countersigned RAP. The DoC Contact Entity is identified as the liable party with respect to the relationship to the market surveillance authority.

The RE requires assurance that the RAP is from a trusted source and that the DoC of their device is a true statement of the legality of the device. Thus the RE user requires to be able to verify the RAP's integrity and the authenticity of the source, and that it has been allowed on their specific RE by verifying the attestation of the RE manufacturer.

With regard to the regulatory authorities the relationships are similar to those of the RE but with the emphasis on verifying that the capabilities of the equipment are within the bounds established in the DoC. The DoC may represent a super-set of RE capability, as it is not mandatory for all the RAPs available to be installed. So a regulatory authority does not need to sign the DoC, or to sign the RAP, but needs to verify the platform both before entry to the market (pre-sale) and when in use to verify the device is still in compliance.

D.3 Assignments of RRS roles to PKI

D.3.1 Model 1: New Root Authority for RRS in the EU

In this model a new entity, the RRS Root Authority, is established. This model is similar to that used in the EU Digital Tachograph model in which the root authority has been established in the JRC.

Pros: RRS is established as a distinct security domain.

Cons: Identification and management of the root authority may be protracted to establish. Protocol and processes for the signature of developer and RE manufacturer certificates have to be established.

D.3.2 Model 2: Existing authorities assigning one entity as root

The core entities involved in the signature creation are the Software Developer for the original RAP, and the RE manufacturer in endorsing the RAP. For the DoC the involved entities in the signature creation are the RE manufacturer and the DoC responsible party (of the RE). There is some potential to have a shared application store that acts as the root, thus the application store acts as the root for all RE manufacturers and their software developers.

The entities involved in validation of the signature are the RE (the equipment), and the regulatory entities.

Pros: A distinct security domain is established within the RRS world.

Cons: Difficult to prove who should be the root in an open market model (a closed market model of a single RE manufacturer managing the entire RRS lifecycle suggests that the RE manufacturer is root).

D.4 Alternative models to PKI for key management

D.4.1 General considerations

The rule of operation in asymmetric cryptography is that one can freely share the public key and there are many means to achieve this including publishing on a public web site, use a keyserver, distribution with message content (email) and X.500/LDAP directories. Sharing the public key does not damage the security of the system as there is no non-trivial means of identifying the private key from knowledge of the public key (as currently known).

Whilst formally a PKI is the most structured it is also the most complex in terms of management. For small projects the web of trust model may be sufficient. Simply RRS is not a small undertaking and justification for anything other than a true PKI is difficult to make.

D.4.2 Self signed certificates

It is possible for an entity to sign their own X.509 certificates. This removes the PKI but assumes no trust hierarchy.

Annex E (informative): The electronic signature regulation (eIDAS)

E.1 Overview

The original Electronic Signature Directive (ESD), 1999/93/EC [8], established a framework across the EU Member States in order to facilitate the use of electronic signatures and to contribute to their legal recognition. The update of the ESD to a full regulation was established in EU Regulation No 910/2014 [9] of 23 July 2014 that came into force in July 2016. The difference between the scope and impact of a directive and a regulation is that the directive requires the creation of law, in this instance to create an electronic signing system within the EU, whereas the regulation is legally binding on all Member States to accept and process complying signatures.

E.2 eIDAS elements

The eIDAS Regulation provides the regulatory environment for the following:

- Advanced electronic signature:
  - Characteristics of an advanced electronic signature are that it provides authentication and identification of the signatory on the assumption that only the signatory has control of the data used to create the electronic signature. In addition the signature has to be constructed in such a way that it makes any tampering of the signed message evident.
  - The technical implementation of advanced electronic signatures is described in the relevant ETSI standards for digital signature for each of XML, PDF and generalized digital documents.
- Qualified electronic signature:
  - Differs from an advanced electronic signature only in respect that it is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures (that is a certificate that attests to a qualified electronic signature's authenticity that has been issued by a qualified trust service provider).
- Trust service:
  - An electronic service that creates, validates and verifies electronic signatures, time-stamps, seals and certificates. Additionally, a trust service may provide website authentication and preservation of created electronic signatures, certificated and seals. It is handled by a trust service provider.

Under the eIDAS framework any document which has been signed has the same legal validity as a conventional written signature. Furthermore where a qualified digital signature is used it is similar to a witnessed signature (i.e. the signature is recognized as explicitly belonging to the signatory by the attestation of a trusted third party).

E.3 Provisions required for eIDAS in RRS and digital variants of DoC

The DoC may be provided in an electronic format. The DoC may be accessed by the user of a smartphone through the user interface. It may also be provided through online resources of the manufacturer. At the time of preparing the present document digital copies of DoCs have been verified as available online (on the World Wide Web) from several manufacturers in PDF or XHTML formats, and can be found by using the search term "Declaration of Conformity" in association with the brand name associated to the manufacturer.

For such electronic versions of the DoC to be considered as legally binding documents in the context of eIDAS they should be signed in compliance with the eIDAS regulation (for the examples cited using the relevant ETSI standards for PDF [13] and XML documents [14] respectively). This is indicated in clause 7.2.2.1 of the present document.

In all instances of examples of the DoC that have been examined in the preparation of the present document the DoC is prepared by the manufacturer and is currently a self-asserted declaration without an apparent digital signature. The responsible party for the DoC is the manufacturer and the depending parties include the market surveillance authorities. These parties are described in clause D.2 as the DoC Contact Entity and the Market Surveillance Body.

The DoC is itself a composite declaration of all of the EMC, RF and other relevant harmonised standards that the device claims conformance to. The DoC does not have a defined syntax or semantic structure and thus has to be treated as a single document for the purposes of signature.

Annex F (normative): ASN.1 OID definitions

Object identifiers for RRS assets and entities shall be defined as follow:

```
DEFINITIONS IMPLICIT TAGS EXTENSIBILITY IMPLIED ::= BEGIN

-- Object Identifier definitions

rrs-rapROLE OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436)
rrs-rap (0)}
rrs-market-surveillanceROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-
103-436 (3436) rrs-market-surveillance (1)}
rrs-application-storeROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-103-
436 (3436) rrs-application-store (2)}
rrs-re-manufacturerROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-103-
436 (3436) rrs-re-manufacturer (3)}
rrs-disturbance-controlROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-
103-436 (3436) rrs-disturbance-control (4)}
rrs-ran-managerROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-103-436
(3436) rrs-ran-manager (5)}
rrs-rrs-caROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436)
rrs-rrs-ca (6)}
rrs-rrs-cpROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436)
rrs-rrs-cp (7)}
rrs-cceROLE OBJECT IDENTIFIER ::= {itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436)
rrs-cce (8)}


END
```

Annex G (normative): Implementation Conformance Statement

G.0 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the ICS pro forma in clause G.5 of the present |annex so that it can be used for its intended purposes and may further publish the completed ICS pro forma.

G.1 Introduction

NOTE: This annex contains a pro forma of an Implementation Conformance Statement to be completed by the supplier of capabilities to an RRS platform. Thus the roles addressed cover those identified in the main body of the document who have a direct impact on the functionality of the platform, hence the suppliers of hardware and software only.

G.2 Guidance for completing the ICS pro forma

G.2.1 Purposes and structure

The purpose of this ICS pro forma is to provide a mechanism whereby a supplier of an implementation of the requirements defined in relevant specifications may provide information about the implementation in a standardized manner.

The ICS pro forma is subdivided into clauses for the following categories of information:

- instructions for completing the ICS pro forma;
- identification of the implementation;
- identification of the protocol;
- ICS pro forma tables (for example: Major capabilities, etc.).

G.2.2 Abbreviations and conventions

This annex does not reflect dynamic conformance requirements but static ones. In particular, a condition for support of a Protocol Data Unit (PDU) parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the related protocol specification.

As a consequence, PDU parameter tables in this annex are not the same as the tables describing the syntax of a PDU in the reference specification.

The ICS pro forma contained in this annex is comprised of information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7 [24].

Item column

The item column contains a number which identifies the item in the table.

Item description column

The item description column describes in free text each respective item (e.g. parameters, timers, etc.). It implicitly means "is <item description> supported by the implementation?".

Reference column

The reference column makes reference to the main body of the present document except where explicitly stated otherwise.

Status column

The various status used in this annex are in accordance with the rules in table G.1.

Table G.1: Key to status codes

Status code	Status name	Meaning
m	mandatory	The capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).
o	optional	The capability may or may not be supported. It is an implementation choice.
n/a	not applicable	It is impossible to use the capability. No answer in the support column is required.
c.<integer>	conditional	The requirement on the capability ("m", "o", "n/a") depends on the support of other optional or conditional items. <integer> is the identifier of the conditional expression.
o.<integer>	qualified optional	For mutually exclusive or selectable options from a set. <integer> is the identifier of the group of options, and the logic of selection of the options.

Mnemonic column

The Mnemonic column contains mnemonic identifiers for each item.

Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7 [24], shall be used for the support column:

Y or y — supported by the implementation

N or n — not supported by the implementation

N/A, n/a or - — no answer required (allowed only if the status is N/A, directly or after evaluation of a conditional status)

References to items

For each possible item answer (answer in the support column) within the ICS pro forma there exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table.

EXAMPLE: A.5/4 is the reference to the answer of item 4 in table A.5.

G.2.3 Instructions for completing the ICS pro forma

The supplier of the implementation may complete the ICS pro forma in each of the spaces provided. More detailed instructions are given at the beginning of the different clauses of the ICS pro forma.

G.3 Identification of equipment and role

The present content of the ICS addresses mandates at stage 2 and detail definition of equipment and role is not given in the present version of the document.

G.4 Global statement of conformance

The implementation described in this ICS meets all the mandatory requirements of the referenced standard?

[ ] Yes

[ ] No

NOTE: Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the ICS, with an explanation of why the implementation is non-conforming. Explanations may be entered in the comments field at the bottom of each table or on attached pages.

In the tabulations which follow, all references are to the main body of the present document unless another numbered reference is explicitly indicated.

G.5 ICS pro forma tables

G.5.1 Security tier

Table G.2: Security tier

Item	Roles	Reference	Status	Support
1	Tier 1	3a	o.1	
2	Tier 2	3a	o.1	
3	Tier 3	3a	o.1	
o.1:	It is mandatory to support at least one of these items.			

G.5.2 Major capabilities

Table G.3: Major capabilities

Item	Roles	Reference	Status	Support
1	Signature validation	3a	M	
2	Signature creation	3a	o.1	
3	Trusted timestamp	3a	o.1	
4	Secure store	3a	o.1	
5	Remote attestation	3a	o.2	
6	Local configuration control	3a	o.1	
7	Remote configuration control	3a	o.2	
8	Non-repudiation of receipt of RAP	5	o.2	
o.1:	IF G.2/1 THEN n/a else m			
o.2:	IF G.2/3 THEN m ELSE n/a			

G.5.3 Trusted timestamp

Table G.4: Trusted timestamp

Item	Trusted Timestamp type	Reference	Status	Support
1	IETF RFC 3161 [20] trusted timestamp	3a	o.1	
2	ANSI X9.95 [21] trusted timestamp	3a	o.2	
o.1: IF G.2/2 THEN m else n/a o.2: IF G.2/3 THEN m ELSE n/a				

G.6 Tabulated mandates

NOTE: The following table is given for information only and is only present to assist in building the ICS tables.

Table G.5: Tabulation of mandates from main body of document

Requirement number	Text	Citation in main body	ICS citation
RQ-TS103436-001	Electronic signature validation shall be provided in all RRS platforms for the validation of the source and integrity of any downloaded Radio Application	3a.2	Table G.3
RQ-TS103436-002	The Radio Application shall be signed using the private key of the signing authority (see note 1)	3a.2	Table G.3
RQ-TS103436-003	The public key certificate of the signing authority, and any other identifying certificates used in the distribution chain, shall be provided along with the Radio Application	3a.2	Table G.3
RQ-TS103436-004	The RE shall be able to verify the signature applied to the distributed Radio Application	3a.2	Table G.3
RQ-TS103436-005	The RE shall only act on the content if the authenticity and integrity of the RAP is verified (see note 2)	3a.2	Table G.3
RQ-TS103436-006	If the RAP cannot be authenticated, or if the integrity validation fails, the RAP shall be discarded (see note 3)	3a.2	Table G.3
RQ-TS103436-007	The RE shall generate evidence of actions related to the use of RAs and sign the evidence (see note 4)	3a.3	Table G.3
RQ-TS103436-008	The RE shall sign the evidence of actions related to the use of RAs	3a.3	Table G.3
RQ-TS103436-009	For Tier#2 the RE shall act as Secure Signature Creating Device (SSCD)	3a.3	Table G.3
RQ-TS103436-010	For Tier#3 the RE shall act as a Qualified Signature Creation Device (QSCD)	3a.3	Table G.3
RQ-TS103436-011	For the non-repudiation service at Tier#3 the RE shall be able to generate evidence of the time any actions related to the use occurred	3a.4.1	Table G.3
RQ-TS103436-012	For the non-repudiation service at Tier#3 the RE shall include the timestamp in the evidence generated	3a.4.1	Table G.3
RQ-TS103436-013	For Tier#2 devices a Trusted Timestamp complying to IETF RFC 3161 [20] shall be generated	3a.4.2	Table G.3
RQ-TS103436-014	For Tier#3 devices a Trusted Timestamp complying to ANSI X9.95 [21] shall be generated	3a.4.2	Table G.3
RQ-TS103436-015	Tier 2 and Tier 3 systems shall maintain evidence generated by the non-repudiation service in secure storage	3a.5	Table G.3
RQ-TS103436-016	Tier 2 and Tier 3 systems shall maintain proof of RAP integrity in secure storage	3a.5	Table G.3
RQ-TS103436-017	Tier 2 and Tier 3 systems shall maintain proof of the binding of a RAP to the RE in secure storage	3a.5	Table G.3
RQ-TS103436-018	The RE Configuration Policy shall be made available to a policy enforcement entity	3a.7	Table G.3
RQ-TS103436-019	The RE shall have a unique application store access identity	4, table 1. Id#3	Table G.3
RQ-TS103436-020	The application store shall have an unique name (see note 5)	4, table 1, id#4	Table G.3

Requirement number	Text	Citation in main body	ICS citation
RQ-TS103436-021	The Developer of RAP shall be identified by an identity form of Public Key Certificate (PKC) according to Recommendation ITU-T X.509 [5]	5.2.1	Table G.3
RQ-TS103436-022	The Application store shall be identified by an attribute form of PKC according to Recommendation ITU-T X.509 [5] with a subjectDirectoryAttributes extension containing the attribute RRS_APPLICATION_STORE (see note 6)	5.2.1	Table G.3
RQ-TS103436-023	The RE Manufacturer shall be identified by both an identity form, and by an attribute form, of PKC according to Recommendation ITU-T X.509 [5] with a subjectDirectoryAttributes extension containing the attribute RRS_RE_MANUFACTURER	5.2.1	Table G.3
RQ-TS103436-024	The Conformity Contact Entity shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_CCE	5.2.1	Table G.3
RQ-TS103436-025	The Market Surveillance Body shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_MARKET_SURVEILLANCE	5.2.1	Table G.3
RQ-TS103436-026	The Disturbance Control Body shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_DISTURBANCE_CONTROL	5.2.1	Table G.3
RQ-TS103436-027	The Radio Network Manager shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_RAN_MANAGER	5.2.1	Table G.3
RQ-TS103436-028	The RRS-CA shall be identified by both an identity form and attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_RRS_CA	5.2.1	Table G.3
RQ-TS103436-029	The RRS-CP shall be identified by both an identity form and an attribute form of PKC according to Recommendation ITU-T X.509 [5], with a subjectDirectoryAttributes extension containing the attribute RRS_RRS_CP	5.2.1	Table G.3
RQ-TS103436-030	The developer of the RAP shall provide proof of the integrity of the package by digital signature of the entire package to be delivered	5.3.1	Table G.3
RQ-TS103436-031	When distributing a RAP the software shall be identified as of type RRS-RAP using the Object IDentifier (OID) itu-t(0) identified-organization(4) etsi(0) ts-103-436 (3436) rrs-rap (0)	5.3.1	Table G.3
RQ-TS103436-032	The developer of the RAP shall include a copy of the DoC for the target platform in the set of supporting files that are distributed with the RAP	5.3.1	Table G.3
RQ-TS103436-033	Basic data exchange confidentiality to provide protection from disclosure of user data while in transit shall be implemented using the TLS mechanisms defined in IETF RFC 5246 [7]	6.2	Table G.3
RQ-TS103436-034	The integrity service shall be implemented using the hash functions within digital signature	6.3	Table G.3
RQ-TS103436-035	Basic data exchange integrity protection to provide protection from manipulation of user data while in transit shall be implemented using the TLS mechanisms defined in IETF RFC 5246 [7]	7.3	Table G.3
RQ-TS103436-036	Cipher suite selection of TLS shall be "TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA"	7.1.1, 7.2.1, 8.1 and 8.2	Table G.3

Requirement number	Text	Citation in main body	ICS citation
RQ-TS103436-037	The RE Configuration record shall be provided by the manufacturer in a machine readable format consistent with that used in the Policy Enforcement Engine (PEE)	11.2	Table G.3
NOTE 1: This along with requirements 3 and 4 meet the requirements stated for objectives 6 and 7 in clause 4. NOTE 2: This partly meets the requirement stated for objective 11 in clause 4. The requirements stated in clause 5.3 are also met by the above. NOTE 3: This meets the requirement stated for objective 12 in clause 4. NOTE 4: This meets the requirement stated for objective 9 in clause 4. NOTE 5: This is complemented by the requirements from clause 5.2.1 to identify the application store as an application store by use of the attribute form of PKC. NOTE 6: This fulfils the requirement set for objective 4 in clause 4.			

Annex I (informative): Change History

CR number	Date	Category	Summary of change	Affected clauses of document	Input version of document	Status	Status date
1	06/02/2017	B (addition of feature)	Addition of new annex and cross reference from the DoC signature countermeasures	New annex E	V1.1.1	Approved	21/02/2017
2	08/02/2017	F (Correction)	Change OID to point to the subject document	5.3	V1.1.1	Approved	21/02/2017
3	06/03/2017	B (addition of feature)	Addition of security classes for RRS	New clause 3a	V1.1.1	Approved	27/03/2017
4	15/03/2017	B (addition of feature)	Addition of clause 9 "Provision of root of trust"	New clause 9	V1.1.1	Approved	27/03/2017
5	08/05/2017	All	Various editorial and technical modifications	All	V1.1.4	Approved	15/05/2017
6	10/05/2017	C (Functional modification of feature)	Extensions in a number of parts of the document. Identification of OIDs	2, 5, 6 and new annex	V1.1.4	Approved	15/05/2017
7	17/04/2017	B (addition of feature)	Addition of annex containing all mandates in document summarized in the form of an Implementation Conformance Statement	Annex F (new), 2.1 (normative references)	V1.1.4	Approved	15/05/2017
8	10/05/2017	C (Functional modification of feature)	Text addressing normative requirements for remote attestation service	10	V1.1.4	Approved	15/05/2017
9	10/05/2017	C (Functional modification of feature)	Text addressing additional requirements for local access control	11	V1.1.4	Approved	15/05/2017
10	31/05/2017	B (addition of feature)	Technical and editorial finalizations in document	All	V1.1.4	Approved	07/06/2017
11	17/06/2017	B (addition of feature)	Addition of tabulated mandates to ICS Annex	Annex G	V1.1.4	Approved by correspondence in course of RC	19/06/2017

History

Document history		
V1.1.1	August 2016	Publication
V1.2.1	February 2018	Publication