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

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

Reference
DTS/RRS-03012

Keywords
security, software

ETSI

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

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

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

Contents

Intellectual Property Rights

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

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

Foreword

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

Modal verbs terminology

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

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

1 Scope

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

2 References

2.1 Normative references

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

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

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

The following referenced documents are necessary for the application of the present document.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

[i.1] ETSI TR 103 087: "Reconfigurable Radio Systems (RRS); Security related use cases and threats in Reconfigurable Radio Systems".

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

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

[i.3] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

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

4 Review of objectives and high level requirements

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

Table 1: Review of security objectives

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

Id	Text of objective	Countermeasure	Strategy
11	The RRS framework should ensure measures are provided to prevent installation of malicious RAPs (see note 4)	Testing and distribution network should verify, as far as reasonable, the functionality of every RAP	Liability framework
12	The RRS framework should ensure measures are provided to prevent modification of an RAP after installation (see note 5)	Run time attestation of integrity	Attestation
13	The RRS framework should provide means to verify the legitimacy of the Declaration of Conformity (DoC) and CE marking (see note 6)	Cryptographically strong document signature verification.	Digital signature
		Maintenance and distribution of blacklist of invalid DoC identities	PKI
		Online verification of signature of DoC	PKI
14	The RRS platform should provide means to be able to uniquely identify the master copy of the DoC (see note 7)	The DoC should be identifiable using a URI or equivalent	Identity management
		Master copy should be named distinctly from any copy and signed as such. In addition copies should be signed/verifiable as legitimate copies and point (URI/URL) to the master copy	Digital signature
15	Where CE marking and DoC are provided for display of the radio equipment by means of user interaction the RRS platform should provide means to assure that the marking is resistant to tampering (see note 8)	This requires the hardware to have tamper-resistant storage to hold the DoC/CE data	Hardware tamper resistance
16	The RRS platform should provide means to validate data used to describe the installation requirements of the RAP (the RAP metadata) against the capabilities of the RE and prohibit installations where a mismatch is identified	The manifest of required platform capability should be covered in the signature and integrity check function	Integrity
17	The RRS platform should prevent an unauthorised third-party from determining that the DoC is being updated	Authentication of parties	Access Control, Identity Management
18	The RRS platform should prevent an unauthorised third-party from determining that the complete DoC is being retrieved from a simplified DoC over the network	Encryption of signalling	Confidentiality
19	The RRS platform should provide means to prevent modification of the DoC apart from installation and update, in particular at rest	Authenticated access control combined with change management control of the DoC	Integrity
20	When the DoC is being updated, or the complete DoC is being retrieved, the RRS platform should allow integrity protection of said DoC while it is in-transit between the relevant entities in the network and components on the device	The integrity measure here applies to data in transit and may be applied at the transport entity as opposed to the document level	Integrity
21	The RRS platform should prevent an unauthorised third-party to delete, install or otherwise alter a DoC on the RE (see note 9)	The DoC should always be available in read-only form on the RE but authorized 3rd parties shall be allowed to update the DoC. This may happen as a result of installation of a new RAP that requires modification of the stored DoC to support any new capability offered by the RAP	Access Control, Authentication, Identity Management
22	When there is only a digital DoC and no paper DoC provided with the RE, the RRS platform should provide means towards tamper-resistance of the DoC at rest on the RE	This requires the hardware to have tamper-resistant storage to hold the DoC/CE data	Hardware tamper resistance
23	When the complete DoC is requested over the network based on a simplified DoC residing on the RE, the RRS platform should provide means towards the availability of complete DoC to the RE	The checksum for proof of integrity shall be measured across the set of elements that compose the DoC	Integrity
24	When the DoC is being updated, or the complete DoC is being retrieved, the RRS platform should allow for identification and authentication of relevant entities in the network and components on the device	Authentication of parties	Access Control

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

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

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

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

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

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

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

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

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

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

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

5 Countermeasure framework

5.1 Notes for interpretation

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

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

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

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

5.2 Identity management and authentication

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

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

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

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

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

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.

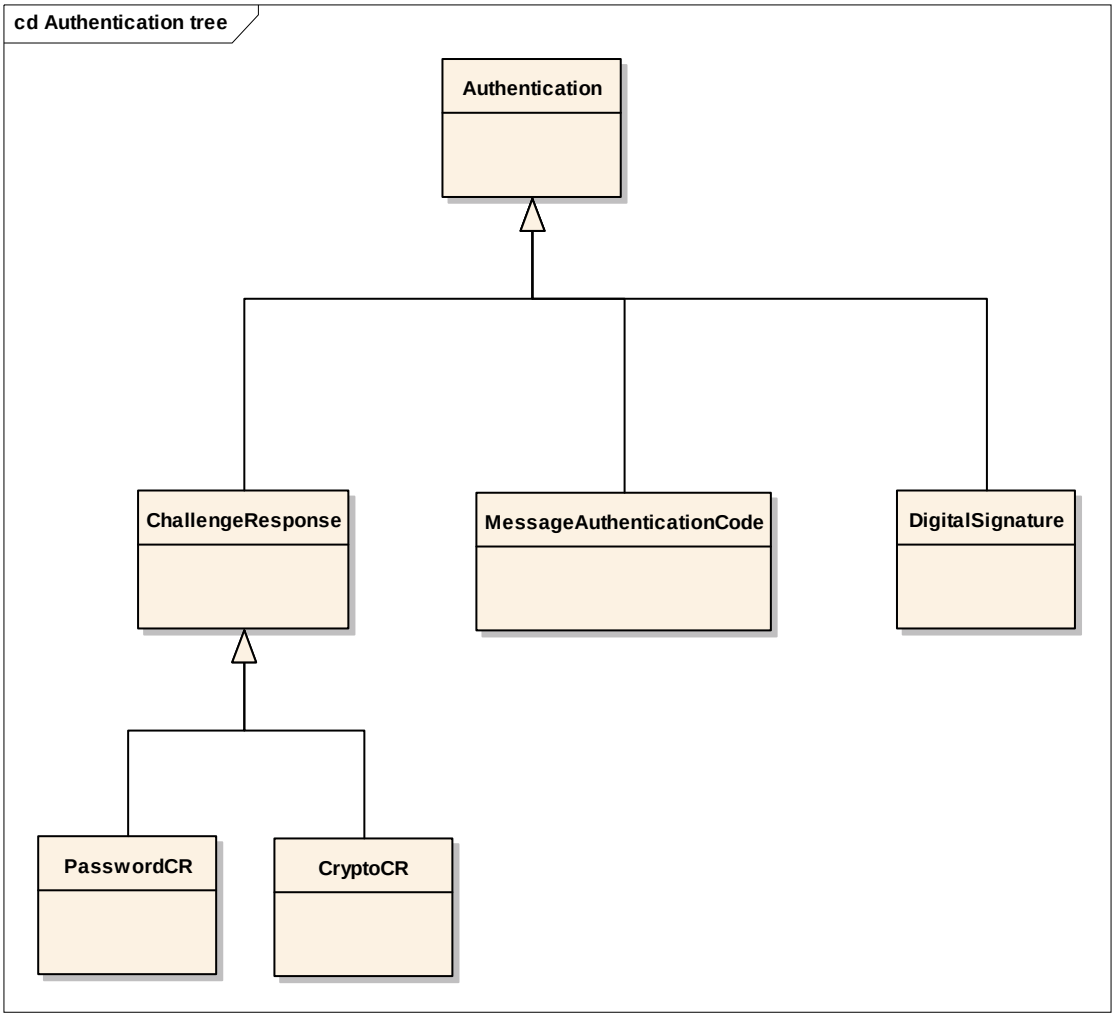

Figure 1: Authentication countermeasure specializations

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).

5.3 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.

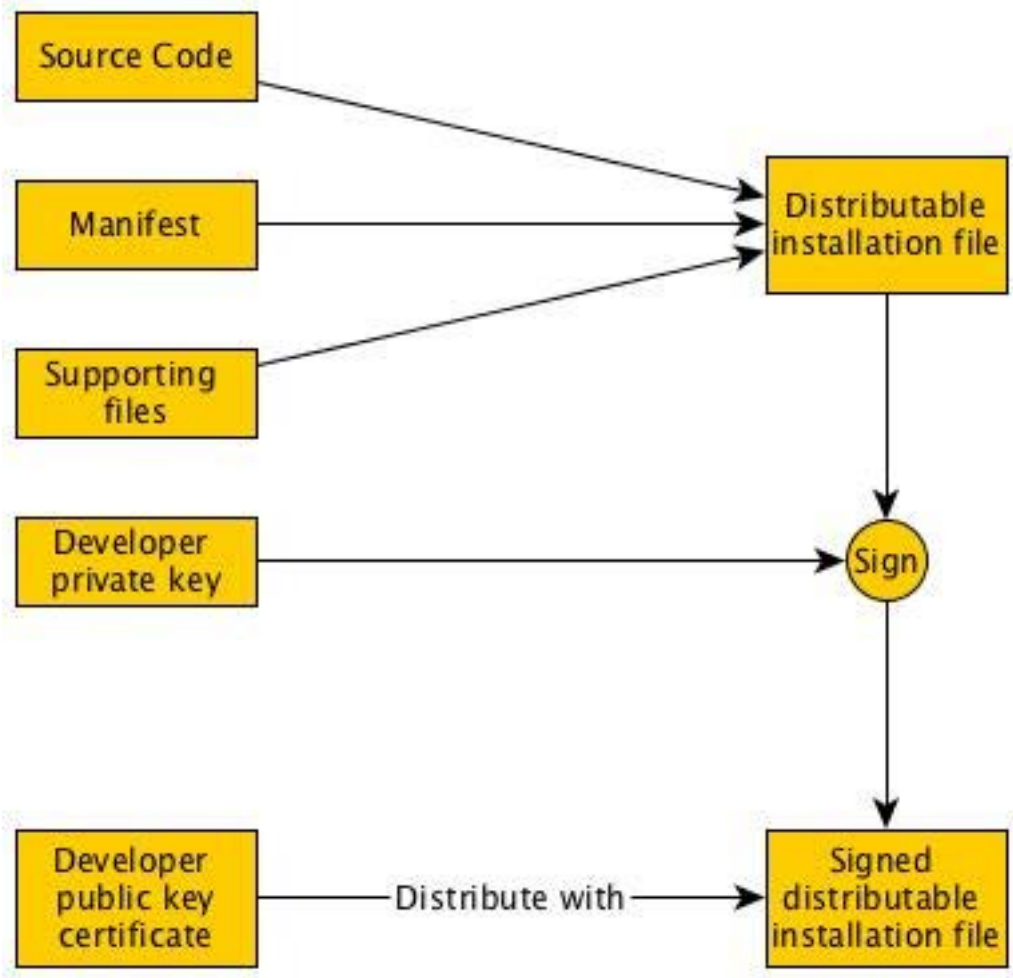

Figure 2: Simplified distribution of signed RAP

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-103-346 (3346) rrs-rap (0)

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

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).

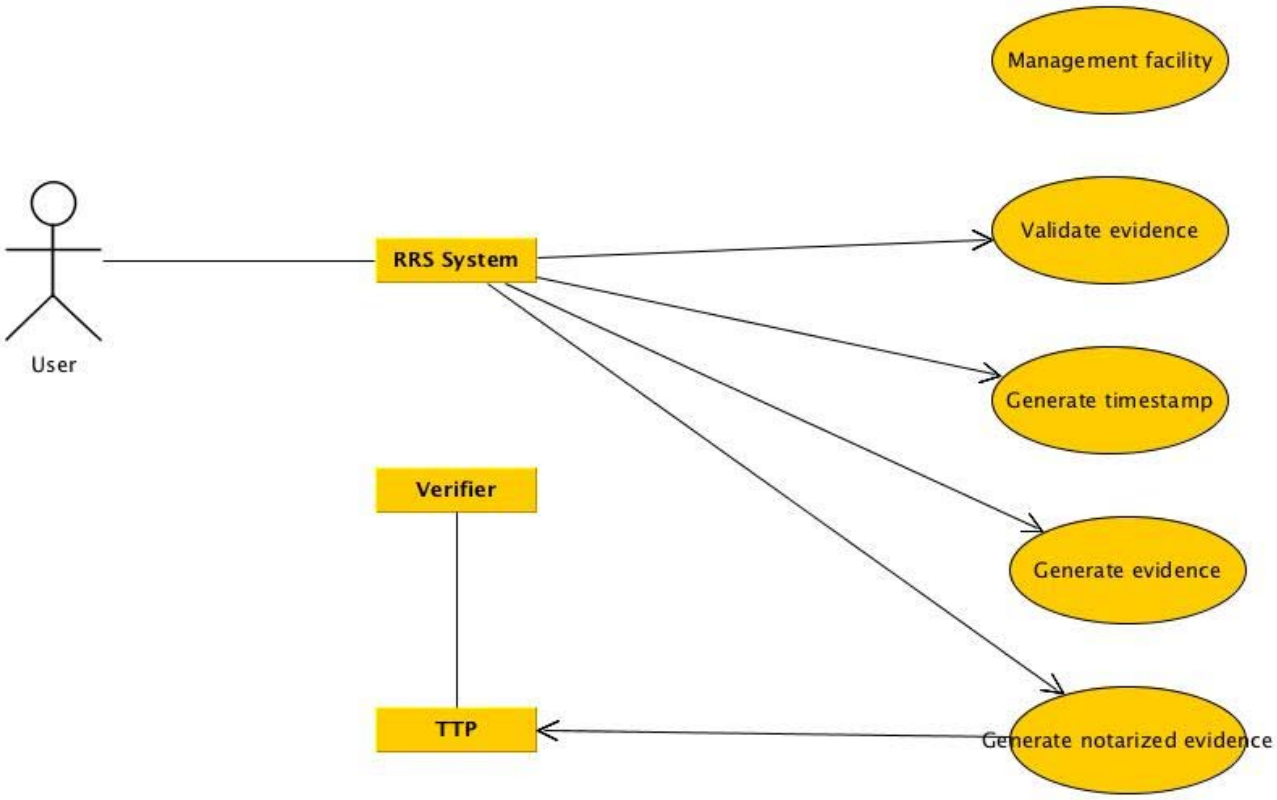

Figure 3: Simplified architecture of use of non-repudiation facilities in NGN

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 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.

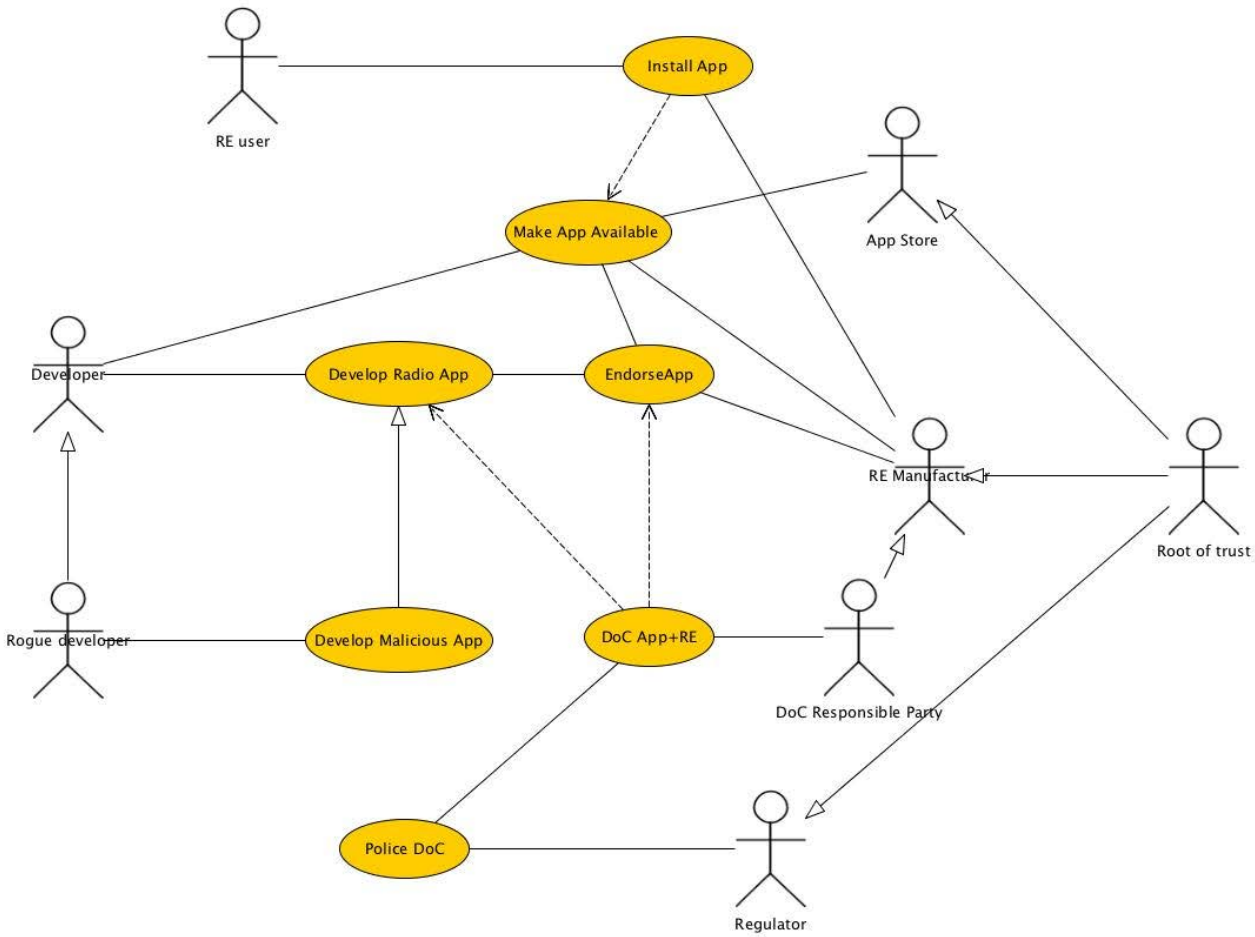

Figure 4: Use cases and actors for RRS application deployment from ETSI TR 103 087 [i.1]

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

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

The Functional model derived from objectives 1 and 18 is as shown in figure 3 and in table 3.

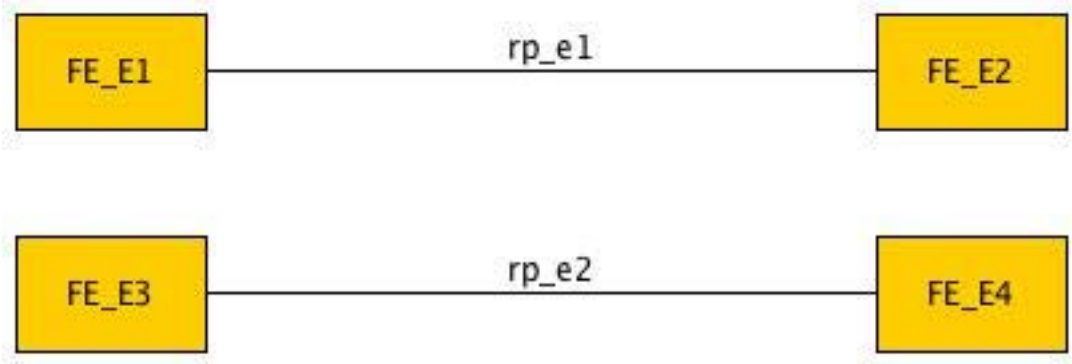

Figure 5: Functional entity model for "Encryption" strategy

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	

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

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 shall be identified by association to a specific RE type (see clause 7.5.2.1.1 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]).

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: ISO/IEC 15408-2 [10] Functional capabilities (Communication class (non-repudiation))

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.

Shortname	Definition	Measure in RRS
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.
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 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 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.

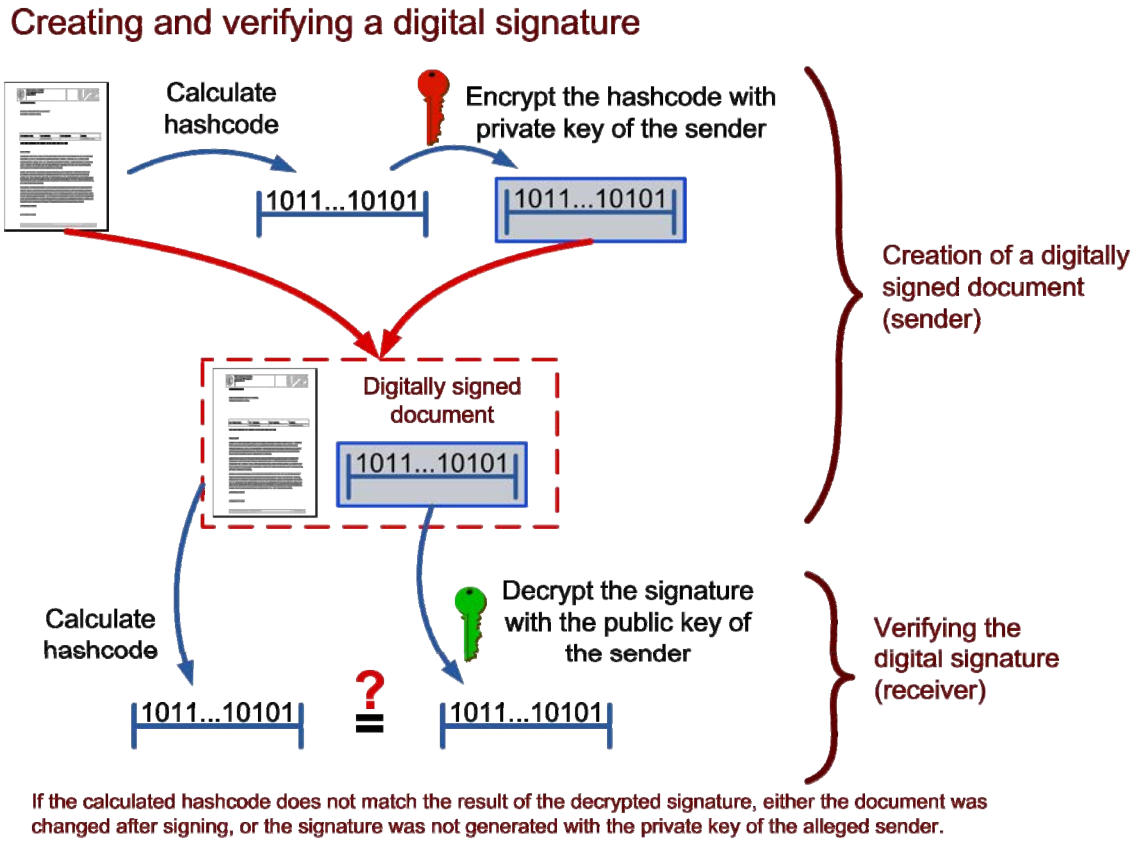

Figure 6: Digital signature process

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.

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 of themselves digital signatures are well understood and the process of adding them to the standards (this 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 analyzed. 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 here: http://www.keylength.com/en/3/ [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 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].

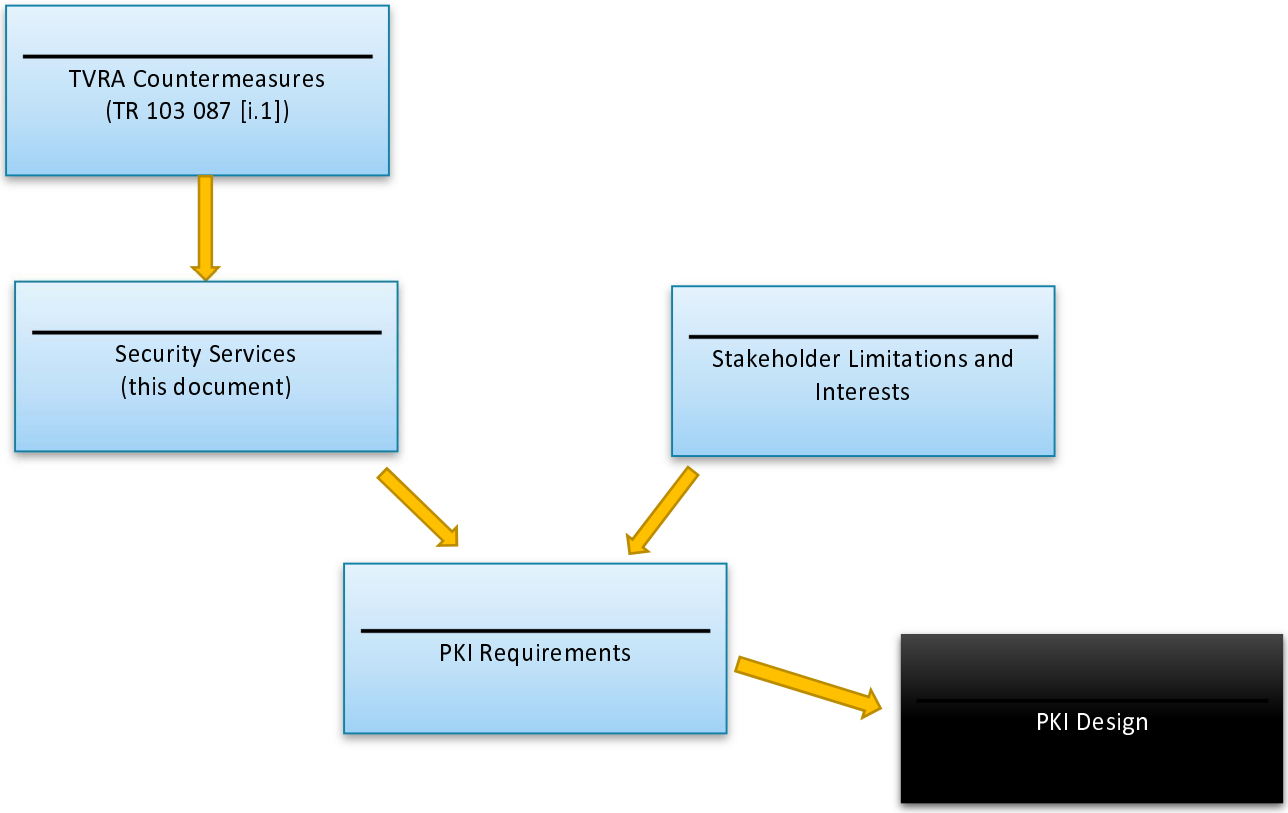

Figure D.1: Steps in the PKI design process

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.

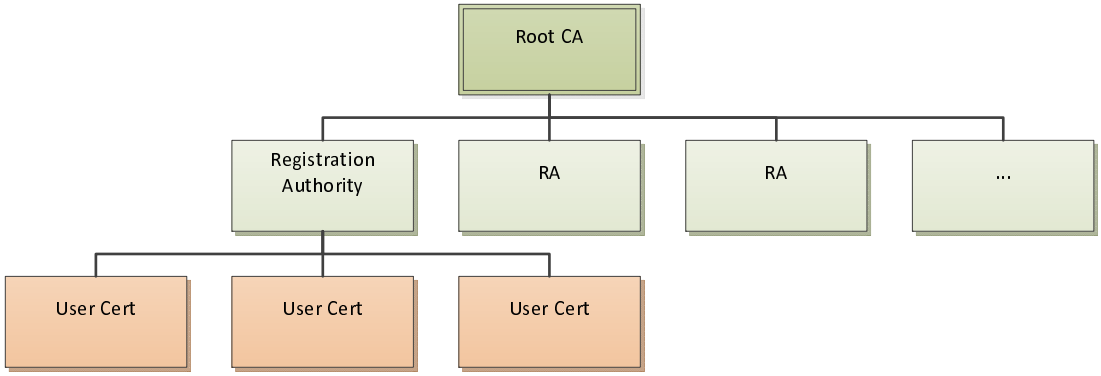

Figure D.2: Conventional PKI hierarchical structure

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.

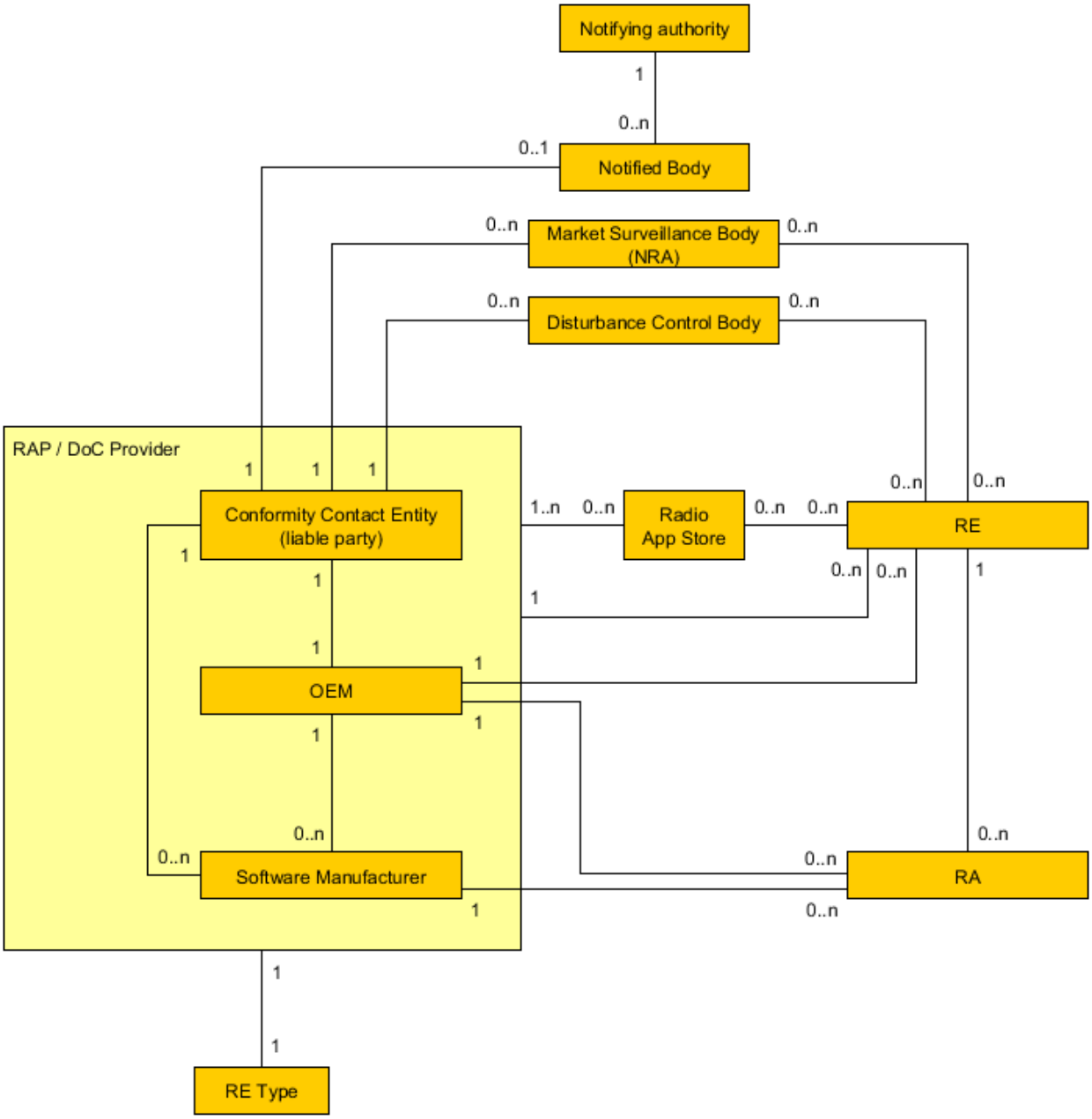

Figure D.3: Cardinalities of stakeholders and assets in RRS from ETSI TR 103 087 [i.1]

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.

History

Document history		
V1.1.1	August 2016	Publication