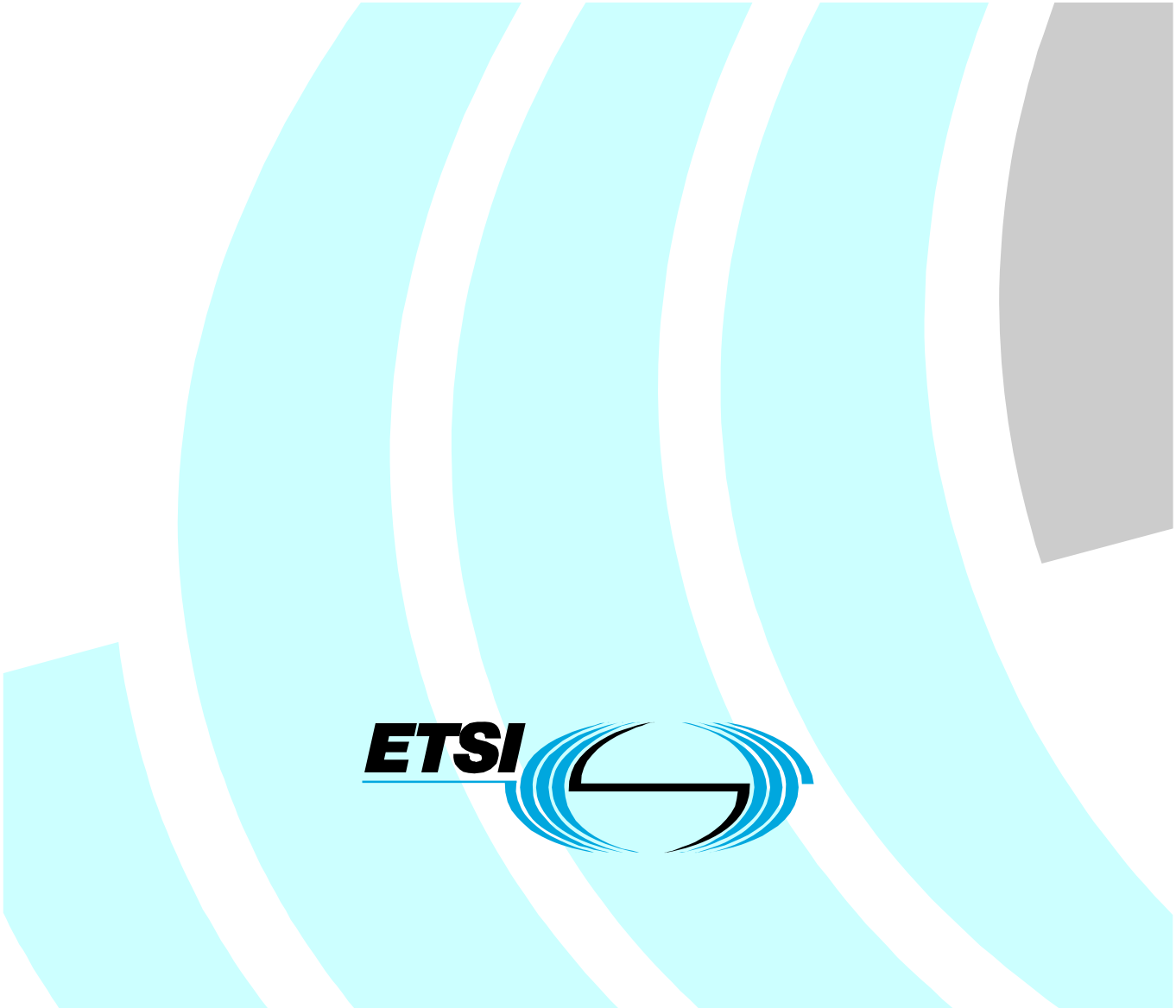
# ETSI TS 102 165-2 V4.2.1 (2007-02)

*Technical Specification*

**Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures**



Reference
RTS/TISPAN-07007-Tech

Keywords
IP, Protocol, Security, VoIP

***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 (http://webapp.etsi.org/IPR/home.asp).

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 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

# Introduction

The present document is one of a set of documents that addresses standardization of security protocols and mechanisms within the context of the *e*Europe 2005 programme. The suite of documents in this suite is composed as follows:

- ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".
- ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".
- ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".
- ETSI TS 102 165-1 [10]: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Method and proforma for Threat, Risk, Vulnerability Analysis".
- **ETSI TS 102 165-2: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protocol Framework Definition; Security Counter Measures".**
- ETSI TS 102 556: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Protection Profile".
- ETSI EG 202 549: "Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities".

These documents are developed based on the objectives of the *e*Europe programme and are also developed to ensure they comply with the overall objectives of the European regulatory framework as defined in the following documents:

- Directive 2002/19/EC of the European Parliament and of the council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities (Access Directive).
- Directive 2002/20/EC of the European Parliament and of the council of 7 March 2002 on the authorization of electronic communications networks and services (Authorization Directive).
- Directive 2002/21/EC of the European Parliament and of the council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

- Directive 2002/22/EC of the European Parliament and of the council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services (Universal Service Directive).
- Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

In particular the present document forms part of the standardization initiative for the Next Generation Network (NGN) platform to be used in *e*Europe and upon which the trust and viability of the *e*-enabled community will, to a very large part, depend on.

The *e*Europe 2005 action plan has been drawn up to focus on "*the widespread availability and use of broadband networks throughout the Union … and the security of networks and information, eGovernment, eHealth and eBusiness*" requiring a supporting infrastructure, which is truly pan-European. To quote COM(2002)263: "*By 2005 Europe should have … a secure information infrastructure*".

# 1 Scope

The present document defines by means of an information model and functional entity behavioural model, the security countermeasures for the ICT in general and where examples are shown they are shown with respect to the NGN. Countermeasures are grouped by their key feature, i.e. Authentication, Integrity.

The Unified Modelling Language (UML) is used to model the countermeasures as a semi-formal tool with verification and simulation capabilities deployed during development.

NOTE: This is in accordance with the goals of the *e*Europe project under objective Good practices (COM(2002) 263 page 18).

The countermeasures defined in the present document have been identified from an analysis of the NGN presented in TS 102 165-1 [10] and in TR 187 002 [9] as those most likely to be required for mitigation of risk in the NGN. The deployment of the countermeasures in the NGN is extrapolated from TR 187 002 [9] and defined in this document.

The present document is intended for designers of security countermeasures.

NOTE: The definition of cryptographic algorithms is not provided by this document but the invocation of algorithms in protocol sequences is shown.

The specific use of IPsec [11] in ESP mode [12], including IKEv2 [18] and is reviewed in annex B of this document as a specific stage 3 implementation of the stage 1 and stage 2 capabilities. The authentication countermeasures outlined as structural and behavioural patterns in the present document cover the following scenarios:

- Source authentication as defined for IPsec ESP.
- NASS-IMS bundled authentication including mechanisms for NASS authentication.
- Early IMS authentication (by reference to TR 133 978 [20]).

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication and/or edition number or version number) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version 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.

[1] ISO/IEC 10181-3: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Access control framework".

NOTE: Equivalent to ITU-T X.812.

[2] ISO/IEC 9798-2: "Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms".

[3] ISO/IEC 9798-3: "Information technology - Security techniques - Entity authentication - Part 3: Entity authentication using a public key algorithm".

[4] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[5] ITU-T Recommendation Z.100: "Specification and description language (SDL)".

[6] ETSI TS 187 001: "Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements".

[7] ETSI TS 187 003: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture".

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

[9] ETSI TR 187 002: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis".

[10] 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".

[11] IETF RFC 4301: "Security Architecture for the Internet Protocol".

[12] IETF RFC 4303: "IP Encapsulating Security Payload (ESP)".

[13] IETF RFC 4306: "Internet Key Exchange (IKEv2) Protocol".

[14] IETF RFC 4305: "Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)".

[15] IETF RFC 3566: "The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec".

[16] IETF RFC 3602: "The AES-CBC Cipher Algorithm and Its Use with IPsec".

[17] IETF RFC 3686: "Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP)".

[18] ETSI TS 133 210 (V7.0.0): "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); 3G security; Network Domain Security (NDS); IP network layer security (3GPP TS 33.210 version 7.0.0 Release 7)".

[19] ISO/IEC 13335-1 (2004): "Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management".

[20] ETSI TR 133 978: "Universal Mobile Telecommunications System (UMTS); Security aspects of early IP Multimedia Subsystem (IMS) (3GPP TR 33.978)".

[21] ISO/IEC 17799 (2005): "Information technology - Security techniques - Code of practice for information security management".

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

[23] ISO/IEC 15408 (2005) (all parts): "Information technology - Security techniques - Evaluation Criteria for IT security".

[24] ISO/IEC 10181-6: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Integrity framework".

NOTE: Equivalent to ITU-T Recommendation X.815.

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

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in ISO/IEC 17799 [21], ISO/IEC 13335-1 [19] and the following apply:

**asset:** anything that has value to the organization, its business operations and its continuity

**authentication:** ensuring that the identity of a subject or resource is the one claimed

**availability:** ensuring that authorized users have access to information and associated assets when required

**compromised evidence:** evidence that was, at one time, satisfactory but which no longer has the confidence of the Trusted Third Party or adjudicator

**confidentiality:** ensuring that information is accessible only to those authorized to have access

**counter-signature:** digital signature appended to a data unit which has already been signed by a different entity (e.g. a TTP)

**evidence generator:** entity that produces non-repudiation evidence

**evidence subject:** entity whose involvement in an event or action is established by evidence

**evidence user:** entity that uses non-repudiation evidence

**evidence verifier:** entity that verifies non-repudiation evidence

**evidence**: information that, either by itself or when used in conjunction with other information, may be used to resolve a dispute

**impact:** result of an information security incident, caused by a threat, which affects assets

**integrity:** safeguarding the accuracy and completeness of information and processing methods

**message authentication code**: cryptographic checkvalue that is used to provide data origin authentication and data integrity

**mitigation:** limitation of the negative consequences of a particular event

**nonce**: arbitrary number that is generated for security purposes (such as an initialization vector) that is used only one time in any security session

NOTE: Although random and pseudo-random numbers theoretically produce unique numbers, there is the possibility that the same number can be generated more than once.

**non-repudiation service requester:** entity that requests that non-repudiation evidence be generated for a particular event or action

**non-repudiation:** ability to prove an action or event has taken place, so that this event or action cannot be repudiated later

**notary:** Trusted Third Party with whom data is registered so that later assurance of the accuracy of the characteristics of the data can be provided

**originator:** in the context of data transfer, entity that originates the data in an action that is subject to a non-repudiation service

**recipient:** in the context of data transfer, entity that receives the data in an action that is subject to a non-repudiation service

**Residual Risk:** risk remaining after risk treatment

**risk:** potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization

**system data:** data that is generated or used by the system to control the operation of the system

**threat:** potential cause of an incident that may result in harm to a system or organization

**vulnerability:** weakness of an asset or group of assets that can be exploited by one or more threats

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| A2ApoA | Application to application point of attachment |
| A2SpoA | Application to service point of attachment |
| AH | Authentication Header |
| ApoA | Application point of attachment |
| AUPC | Authentication Port Claimant |
| AUPV | Authentication Port Verifier |
| CA | Certification Authority |
| CK | Cipher Key |
| ESP | Encapsulating Security Payload |
| FFS | For Further Study |
| ICT | Information and Communication Technology |
| IK | Integrity Key |
| IPsec | IP security |
| KMPC | Key Management Port Claimant |
| KMPM | Key Management Port Manager |
| KMPV | Key Management Port Verifier |
| KSG | Key Stream Generator |
| KSS | Key Stream Segment |
| MAC | Message Authentication Code |
| NGN | Next Generation Network |
| PKI | Public Key Infrastructure |
| S2SpoA | Service to Service point of attachment |
| S2TpoA | Service to transport point of attachment |
| SDU | Service Data Unit |
| SpoA | Service point of attachment |
| T2TpoA | Transport to transport point of attachment |
| TA | Authentication Timer |
| TOE | Target Of Evaluation |
| TpoA | Transport point of attachment |
| TVP | Time Variant Parameter |
| UML | Unified Modelling Language |

## 3.3 Notation

For the purposes of the present document, the following notation is used:

| | |
|---|---|
| A | denotes A's Private user ID |
| $P_A$ | denotes the public key encryption algorithm of A |
| $S_A$ | denotes A's signature mechanism |
| $r_A$ | a random number generated by A |
| $t_A$ | a timestamp generated by A |
| $A \rightarrow B: P_B(t_A, A)$ | denotes the transmission from A to B of elements $t_A$ and A protected using $P_B$ |
| $A \leftarrow B: P_A(S_B(r_B, t_B))$ | denotes the transmission from B to A of elements $r_B$ and $t_B$ signed by B and protected using $P_A$ |
| $A \rightarrow B: P_B(S_A(r_A, r_A))$ | denotes the transmission from A to B of elements $r_A$ and $t_A$ signed by A and protected using $P_B$ |
| SPI | Security Parameters Index |

ICV Integrity Check Value

# 4 Architecture considerations for security in ICT

A simplified architectural model of the ICT and NGN domains is given in figure 1 and serves as the abstract model for the security countermeasures defined in the remainder of the present document.

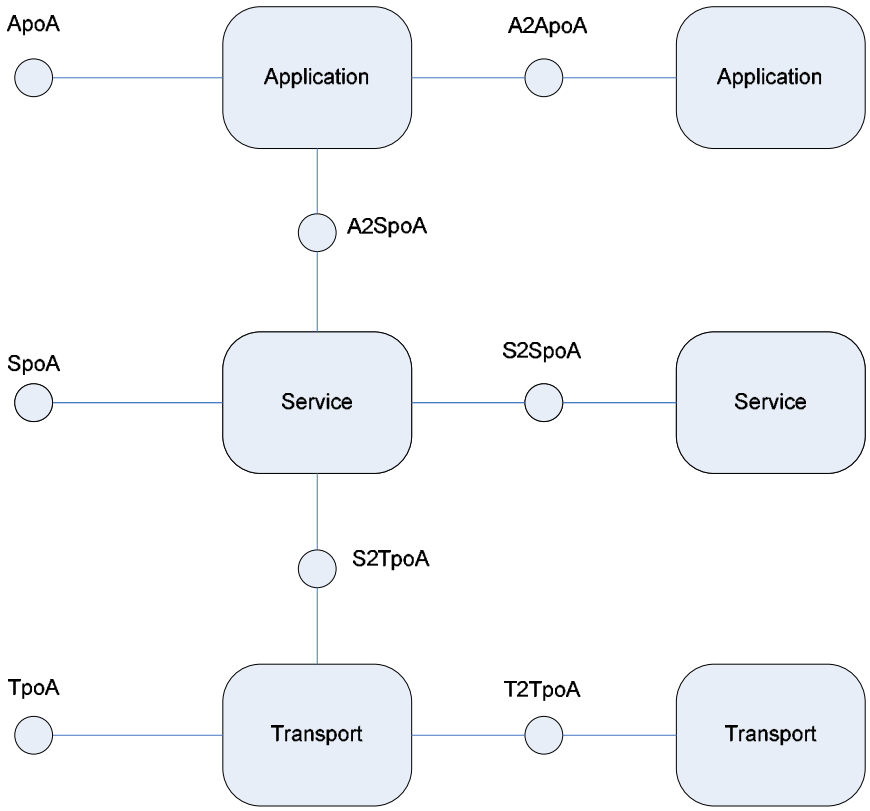



**Figure 1: Abstract architecture for security countermeasure application**

The user connects to each layer using a layer specific point of attachment:

- TpoA Transport point of attachment (TpoA reference point).
- SpoA Service point of attachment (SpoA reference point).
- ApoA Application point of attachment (ApoA reference point).

The countermeasures are described with respect to the user interaction with each layer:

- Inbound authentication at TpoA/SpoA/ApoA.
- Outbound authentication at TpoA/SpoA/ApoA.

NOTE 1: If an authentication exchange nests inbound and outbound authentication, it is termed mutual authentication. However if the exchanges are discrete and with different lifetimes the term mutual authentication is inappropriate.

- Integrity of communication at TpoA/SpoA/ApoA.
- Confidentiality of communication at TpoA/SpoA/ApoA.

Within the system the countermeasures are extended to cover interactions between layers both vertically and horizontally. The set of countermeasures thus include (where the term Service is used as a synonym for any of the three abstract layers of the ICT architecture):

- Service to Service authentication.
- Integrity of communication from Service to Service.
- Confidentiality of communication from Service to Service.

In an ICT environment, particularly where commercial services are offered, it may be required to provide a non-repudiation service (to counter denial of a transaction). An outline non-repudiation service is described in clause 9.

The services apply to the following points on figure 1:

- A2SpoA Application to Service reference point.
- S2TpoA Service to Transport reference point.
- A2ApoA Application to Application reference point.
- S2SpoA Service to Service reference point.
- T2TpoA Transport to Transport reference point.

NOTE 2: The model does not show a specific reference point between Application and Transport on the assumption that a Service layer always exists.

In addition to the countermeasures provided at the identified reference points a secure system may have to deploy other countermeasures to protect their assets. Such countermeasures may include billing controls, system auditing and event logging.

## 4.1 Mapping to 3GPP and NGN architectures

The $Z_A$ and $Z_B$ interfaces defined in TS 133 210 [18] map to the reference points T2TpoA where T2TpoA may be either internal to a network (transport) or between networks (transport).

## 4.2 Use of functions from ISO/IEC 15408

The use of classes and families defined in the requirements document of ISO/IEC 15408 [23] can be applied when defining and modelling the security countermeasure services and capabilities. As defined in TS 102 165-1 [10] clause 4.2, security objectives are related to a system design which is composed of assets, there is also a relation between assets and the countermeasures applied to them. The security classes and families functionality defined in ISO/IEC 15408-2 [23] help to satisfy several security objectives as defined in TS 102 165-1 [10], there is therefore a relation between the countermeasures and the functionality that the classes and families provide that is defined in the countermeasures clauses of the present document.

## 4.3 Requirements model in communications security

The root of communications security is in the balance between what the user is doing and what the service provider has to do to enable the user to do it.

Users wish to use a service and may wish to have some assurance of the confidentiality, integrity and reliability of the service. At some point the user is likely to pay a bill for use of the service. On the balancing side the service provider wishes to ensure that only known parties have access to the services (Access Control) which may invoke use cases that check identity and authenticate identity.

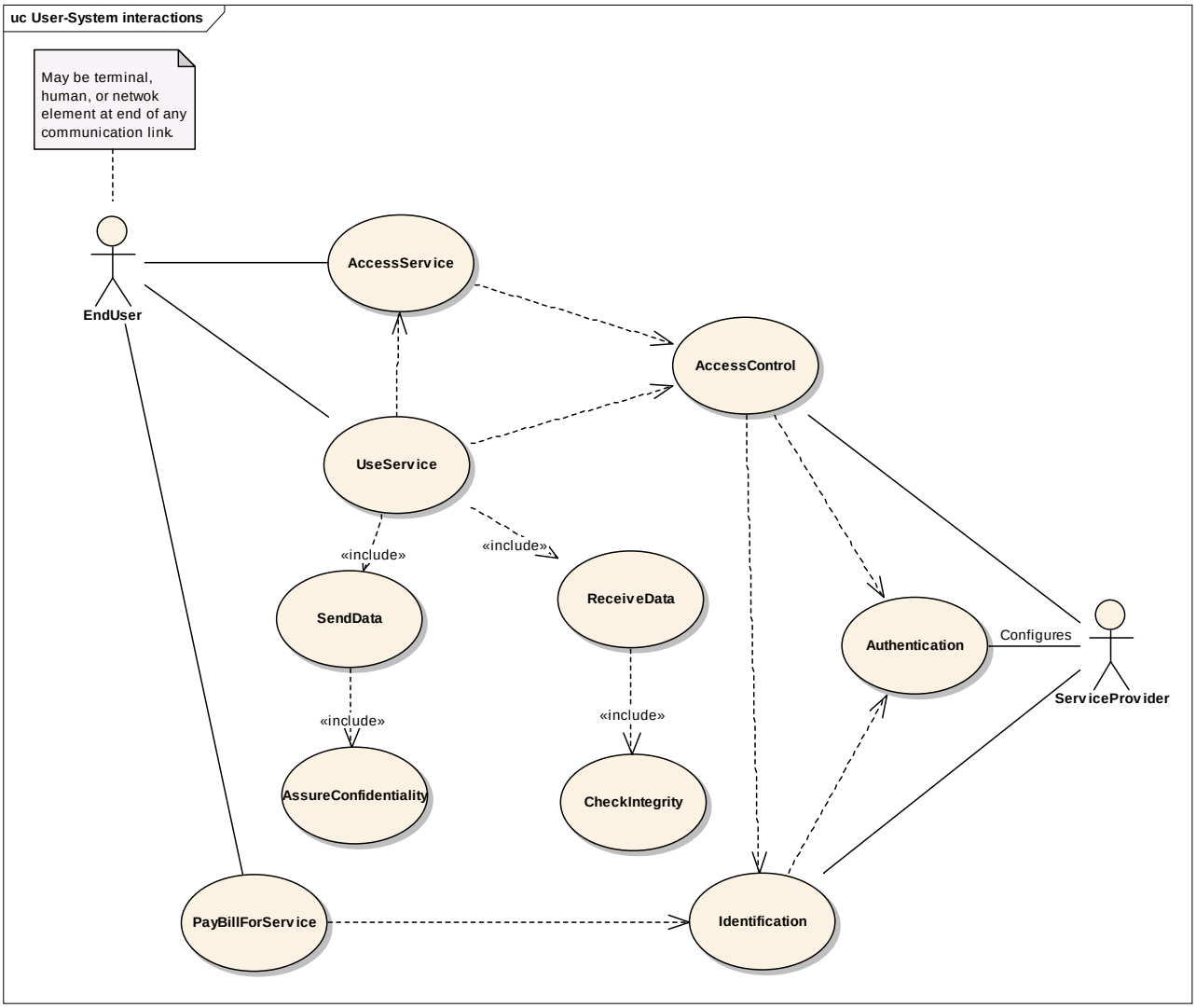



**Figure 2: Use cases and their interactions in Communications Security**

# 5 Authentication counter-measures

## 5.1 Introduction

The primary purpose of the authentication service is to counter masquerade attacks. This may prevent attack on the system by determining that the user is legitimate, and may prevent an attack on the user by determining that the system is legitimate. The authentication services when successfully performed may provide an element of an of access control mechanism.

The overall authentication framework is derived from ISO/IEC 10181-2 [8] and extended by modelling as UML with detail behaviour and information element definitions being provided.

In common with the framework from ISO/IEC 10181-2 [8] the models described in this document can be applied at any layer in a protocol stack or within any unique plane of the deployed NGN (i.e. they may apply at all the reference points described in clause 4).

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 3.

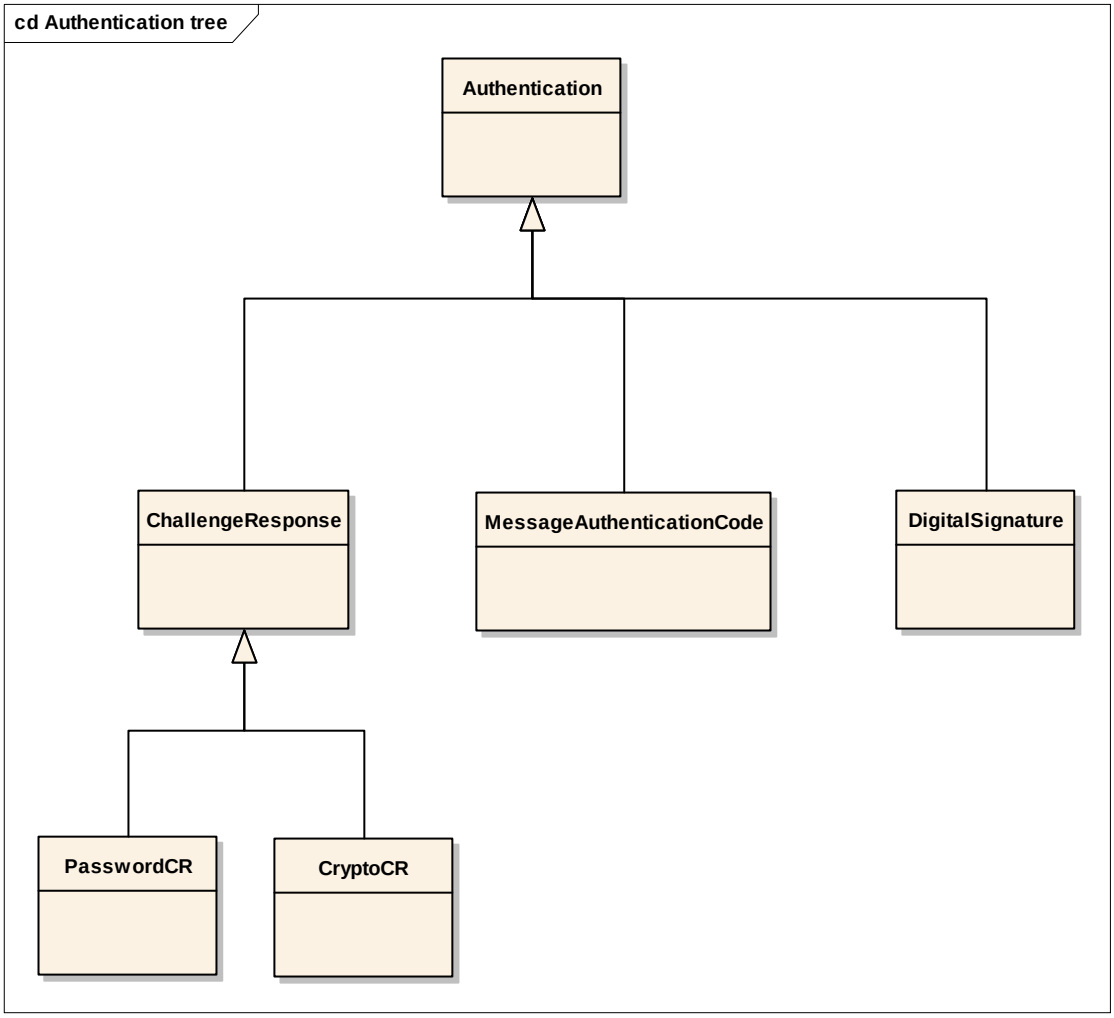



**Figure 3: Authentication countermeasure specializations**

Authentication requires that something is known to the parties authenticating each other. The fundamental concern of the verifying party is to be assured that the data requiring authentication belongs to the claiming party. In most communication systems the authentication service refers to a means of proving that an offered identity belongs to the claimant. This is achieved for the purposes of this document by combining the claimed identity with at least one other data element (key, password, etc.).

Two forms of authentication service are described in the present document:

- Challenge response based authentication.
- Message authentication code based authentication.

The outline models for authentication mechanisms (as distinct from the framework they exist in) are found in ISO/IEC 9798-2 [2] and in ISO/IEC 9798-3 [3] for the challenge response based authentication methods using symmetric and asymmetric keys respectively. The model for message authentication code forms is adapted from ISO/IEC 9798-4 [4].

Authentication may be realized in several ways:

- Weak authentication methods such as username/password where the user enters the credentials manually and this can authenticate directly using the terminal as a conduit.
- Strong authentication methods using cryptographic credentials the user cannot be an active part of the authentication process. In this case the terminal or a device connected to it (e.g. smartcard) may perform the generation of the necessary cryptographic tokens.

For the remainder of this document only strong authentication methods are described.

### 5.1.1 Single versus multi-factor authentication

Authentication methods rely upon something the principal **is**, **has** or **knows**, where is, has, knows are considered as classes of information. Authentication that uses attributes from only one of these classes is called single factor authentication, and if attributes from two or more of the classes is used in the authentication it is referred to as multi-factor authentication (2-factor if attributes from 2 classes are used, 3-factor if attributes from all 3 classes are used).

NOTE 1: The use of two attributes in a class does not make the authentication 2-factor.

Typically if a human is the principal he is identified by some form of biometric data and the assumption for authentication is that the biometric data is unique and not forgeable.

NOTE 2: If biometric data is compromised it is not likely to be replaceable particularly if the attribute is physical such as fingerprint or DNA (i.e. a human being cannot readily change physical characteristics).

When the authentication factor uses something the principal has it often refers to a specific hardware module containing some unique and non-forgeable secret. This is the model used in SIM cards where the key is contained on the SIM held by the user's phone. The third case is where the user has to have knowledge and covers passwords, PINs, and pass-phrases.

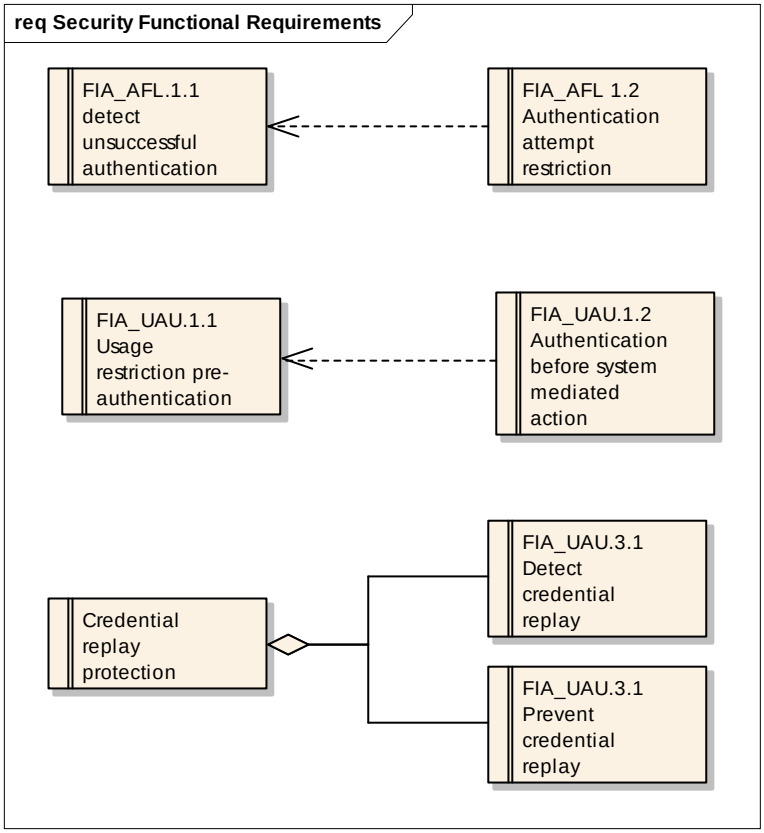
The mechanisms in the present document address only single factor authentication methods and in each case identify the principal and the nature of the credentials. The method of providing the credentials is not addressed.

#### 5.1.1.1 Behavioural extension for authentication models

In addition to the three classes (factors) described above a fourth class is sometimes considered that analyses behaviour of the entity being authenticated. For example when using an authenticated bank card (authentication by signature and/or PIN) the bank may require additional data to complete authorization if the behaviour of the authenticated party is divergent from previous behavioural patterns. The use of behavioural patterning is not covered in the present document.

## 5.2 Authentication service requirements

The authentication requirements may be stated using functional capabilities as defined in ISO/IEC 15408-2 [23]. These may also be shown graphically as in figure 4.




NOTE: Not all requirements are shown (FFS)

**Figure 4: Requirements for authentication in graphical format**

As a prerequisite for authentication the user identity has to be known and any key material used in the authentication protocol has to be distributed.

**Table 1: Detailed requirements statements for authentication countermeasures**

| Shortname | Definition |
|---|---|
| FIA_AFL.1.1 | The authentication protocol shall detect any unsuccessful authentication attempts. |
| FIA_AFL.1.2 | When the defined number of unsuccessful authentication attempts has been met or surpassed, the authentication protocol shall PROHIBIT further attempts using the same credentials. |
| FIA_UAU.1.1 | The system (ICT/NGN) shall allow only EMERGENCY CALLs and LOCATION UPDATEs on behalf of the user to be performed before the user is authenticated. |
| FIA_UAU.1.2 | The system (ICT/NGN) shall require each user to be successfully authenticated before allowing any other system-mediated actions on behalf of that user. |
| FIA_UAU.2.1 | The system (ICT/NGN) shall require each user to be successfully authenticated before allowing any other system-mediated actions on behalf of that user. |
| FIA_UAU.3.1 | The authentication protocol shall detect use of authentication data that has been forged by any user of the authentication protocol. |
| FIA_UAU.3.1 | The authentication protocol shall prevent use of authentication data that has been forged by any user of the authentication protocol. |
| FIA_UAU.3.2 | The system (ICT/NGN) shall detect use of authentication data that has been copied from any other user of the system (NGN). |
| FIA_UAU.3.2 | The system (ICT/NGN) shall prevent use of authentication data that has been copied from any other user of the NGN. |
| FIA_UAU.5.1 | The system (ICT/NGN) shall provide at least one authentication mechanism to support user authentication. |
| FIA_UID.1.1 | The system (ICT/NGN) shall allow no activity on behalf of the user to be performed before the user is identified. |
| FIA_UID.1.2 | The system (ICT/NGN) shall require each user to be successfully identified before allowing any other system (ICT/NGN)-mediated actions on behalf of that user. |

The present document assumes only symmetric keying methods are used. This method requires pre-arrangement between the authenticating entities but ensures that the authentication framework is able to provide a mapping to existing terminals which employ strong authentication (e.g. GSM, 3GPP-UMTS, DECT, TETRA).

The symmetric keying authentication methods are based upon the provisions described in ISO/IEC 9798-2 [2].

The authentication protocol should have the following properties:

- bi-directional challenge-response type;
- able to be initiated either explicitly or as part of the registration procedure;
- able to be initiated by the terminal or the network;
- the recipient of the first authentication demand may instigate mutual authentication by use of a mutual authentication indicator, and by sending its challenge together with the response to the first challenge; and
- where authentication is initiated as part of the registration the authentication timer TA shall always be less than or equal in value to any registration timer.

## 5.3 Overall stage 1 model for authentication

### 5.3.1 Procedures

#### 5.3.1.1 Provision/withdrawal

Authentication shall always be available.

#### 5.3.1.2 Normal procedures

Authentication shall always be activated.

##### 5.3.1.2.1 Invocation and operation

Authentication may be invoked on one or more of the following events:

- on registration to the CSP;
- on change of physical point of attachment;
- on change of logical point of attachment;
- on demand by the user through some terminal function; and
- on demand by the authentication centre.

#### 5.3.1.3 Exceptional procedures

##### 5.3.1.3.1 Activation/deactivation/registration/interrogation

Not applicable.

##### 5.3.1.3.2 Invocation and operation

If the expected response is not equal to the received response authentication is not proven and any dependent services shall not be invoked. A network may reattempt the authentication service, however repeated failure may be considered as an attack on the algorithms and should be deterred by denying access to the initiator of the authentication.

### 5.3.2 Interactions with other security services

The authentication services may be linked to the registration service and should be operated in parallel to them.

The authentication services may provide keying material for the confidentiality services.

The authentication services may provide the basis for the access control service.

### 5.3.3 Interworking considerations

The authentication algorithms used by each of the participant entities have to be matched.

## 5.4 Specific authentication models (stage 2 models)

### 5.4.1 Challenge response authentication

NOTE: The challenge response form is used in 3GPP-IMS for authentication of the IMS-user.

The generic model for challenge response authentication is given in figure 5 and illustrates the following primary elements:

- Key manager
  - Responsible for maintaining keys and distributing them securely to the active agents. In a Public Key Infrastructure (PKI) environment the Key manager may be considered as equivalent to the Certification Authority when X.509 certificates are used to distribute keys.
- Verifier
  - Responsible for initiating the authentication process and in charge throughout. An authentication proxy may assist in the carrying out of the verifier's role.
  - An entity which is (or which represents) the entity requiring authentication.
- Verifier proxy
  - An entity that may act on behalf of the true verifier (act as proxy for) which inherits the attributes and operations of the verifier but may extend either.
- Principal
  - An entity whose identity (or any other associated attribute) can be authenticated.
- Claimant
  - The representative of the principal for the purposes of authentication which acts as the entity being authenticated, responsible for supplying a correct response to the challenge.

A Trusted Third Party (TTP) may act as a special case of proxy for either the verifier of claimant.

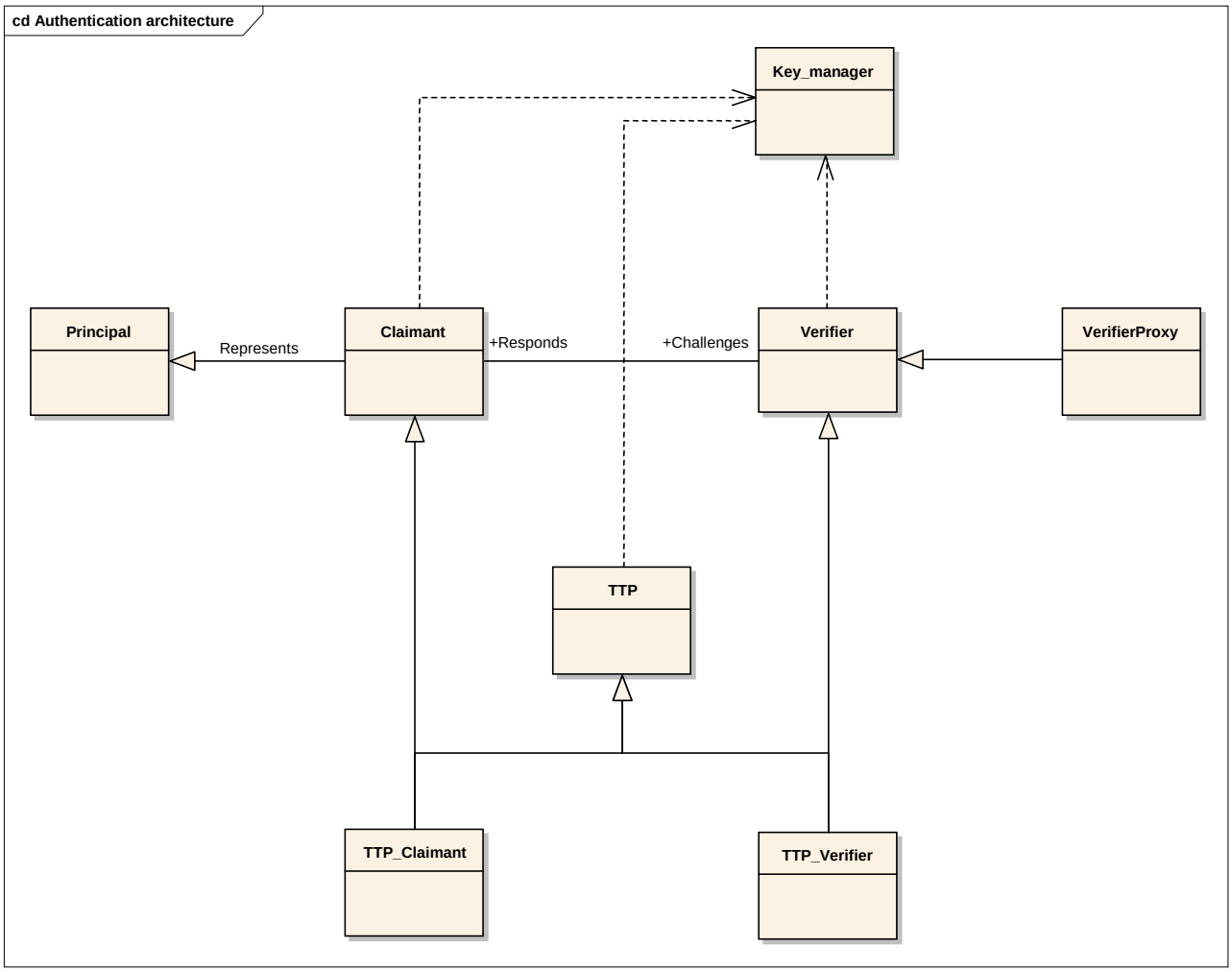
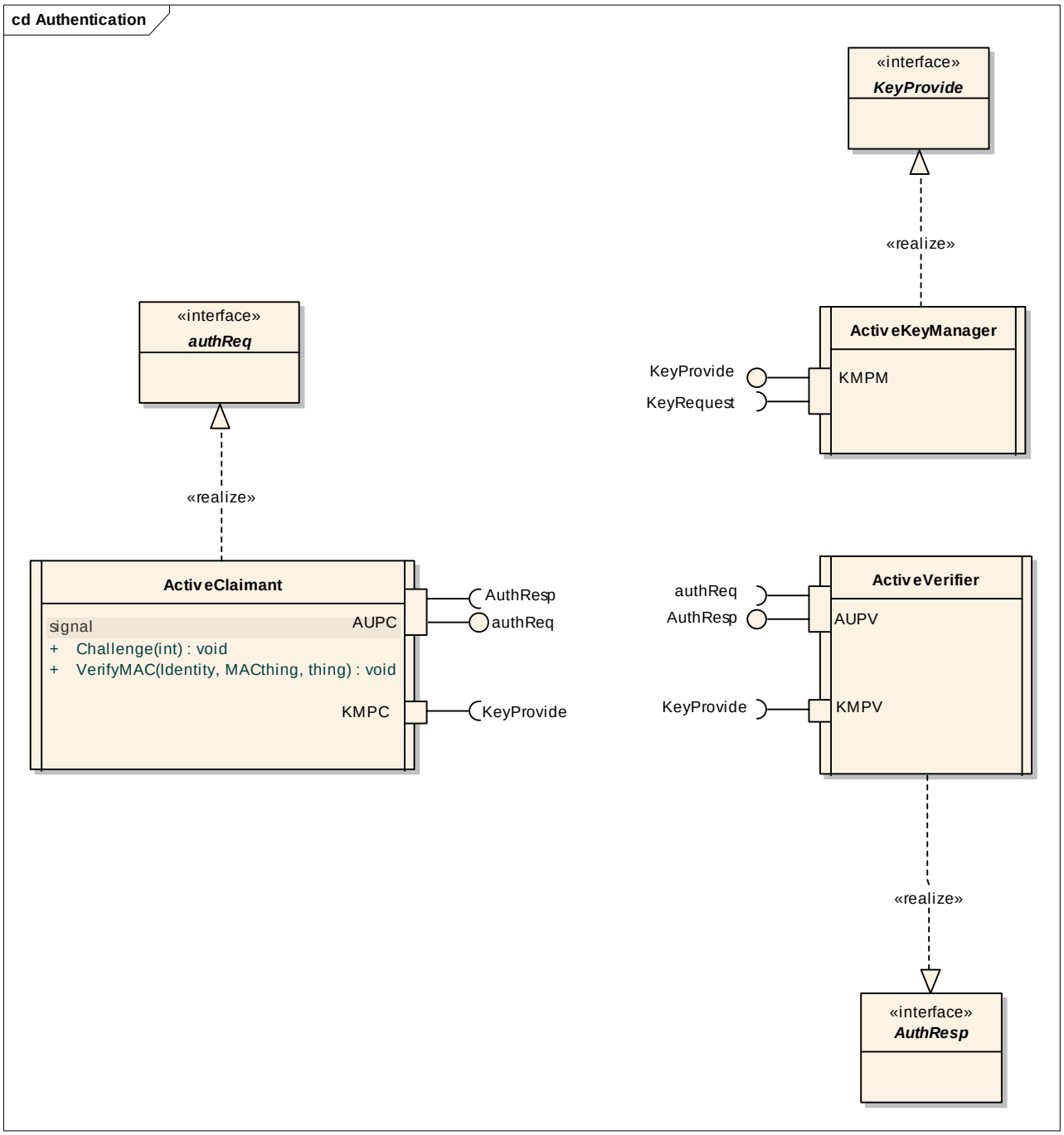



**Figure 5: UML pattern for challenge response authentication model**

For further analysis in UML2 the active model is shown in figure 6.




AUPC Authentication Port Claimant
AUPV Authentication Port Verifier
KMPC Key Management Port Claimant
KMPV Key Management Port Verifier
KMPM Key Management Port Manager

NOTE: The "Active" class construct is an UML2 concept that distinguishes between passive and active classes. The active classes are used for state-full type modelling wherein an active class indicates that, when instantiated, it will control its own execution. Rather than being invoked or activated by other objects, it can operate standalone, and define its own thread of behaviour. Countermeasures are modelled in the main as active rather than as passive classes.

**Figure 6: UML pattern for authentication using active classes**

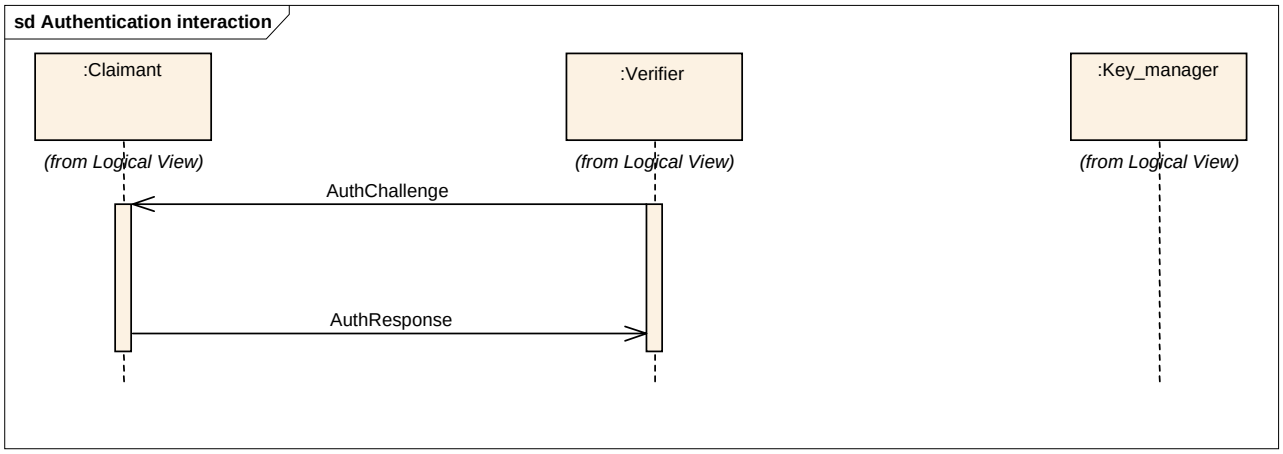



**Figure 7: Information flow interactions for authentication**

### 5.4.2 Authenticate service capability

The *authenticate* service capability is described by a set of capabilities allowing Challenge-Response authentication and Message Authentication Integrity Code authentication forms. These are shown in figures 9, 10, 11, and 12.

The service capability supports symmetric and asymmetric keying methods, single and multi-pass protocols, and both unilateral and mutual authentication.

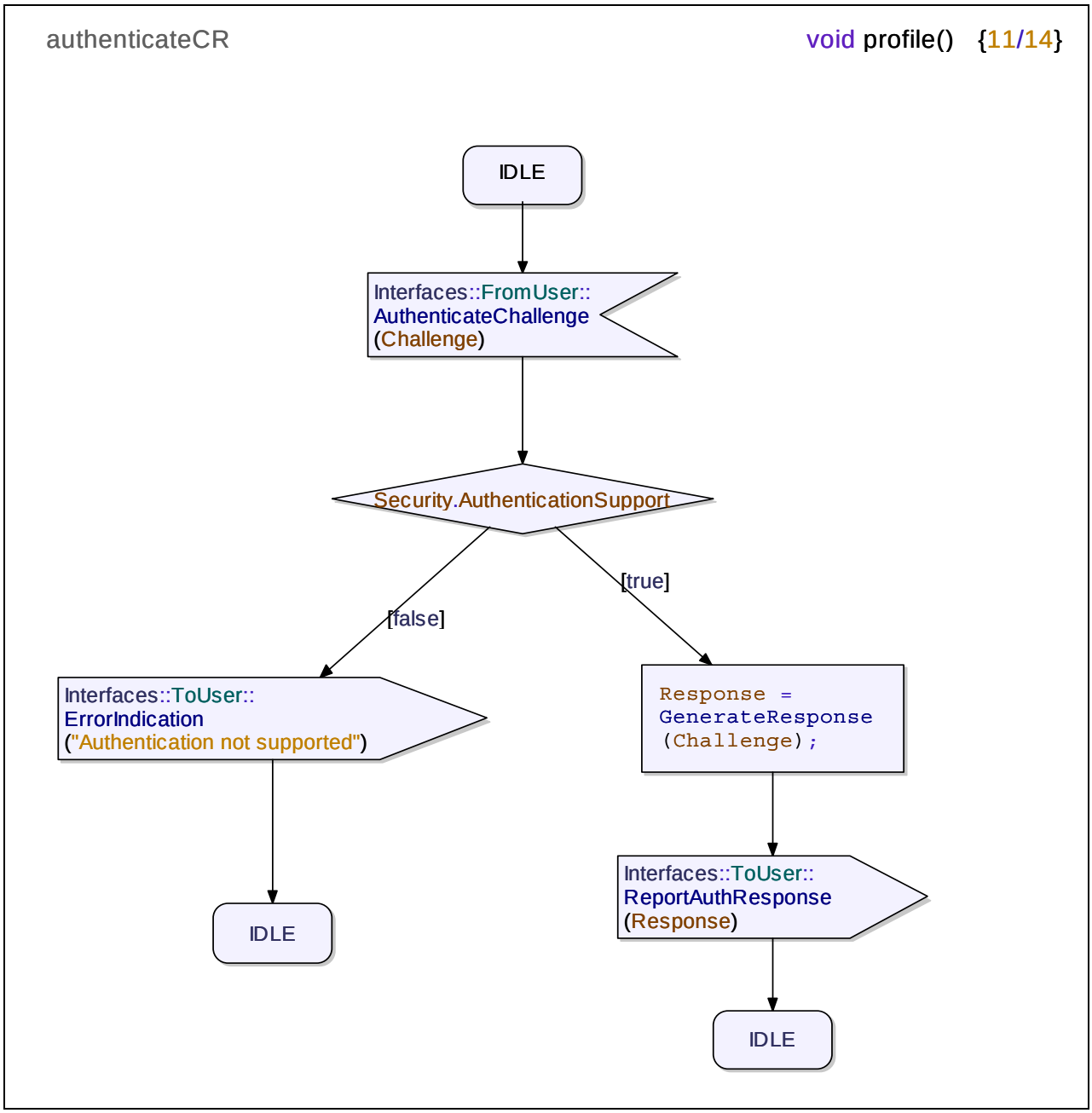



**Figure 8: State chart diagram for authenticate challenge response service capability**

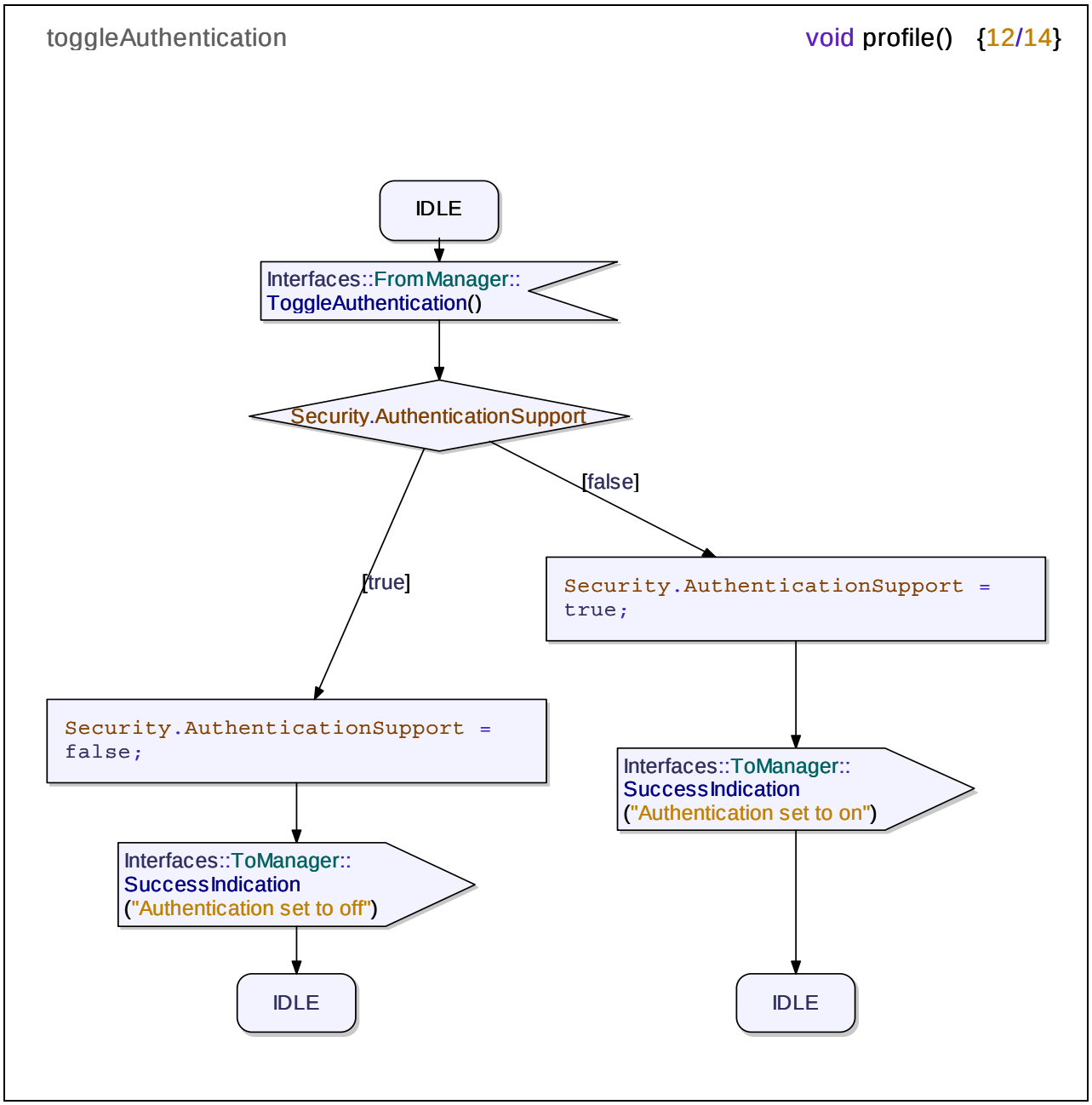



**Figure 9: State chart diagram for authenticate toggle service capability**

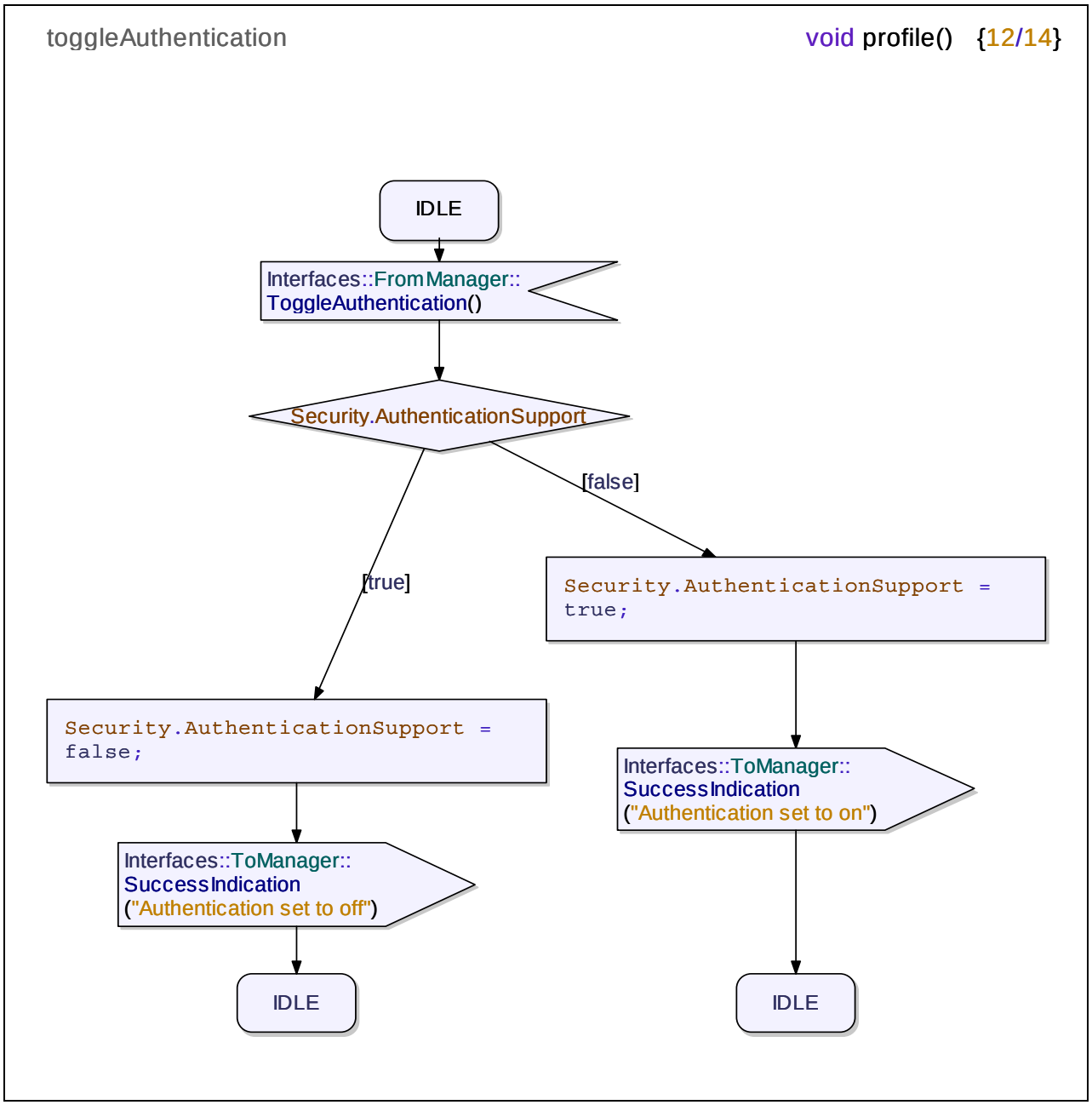



**Figure 10: State chart diagram for authenticate toggle service capability**

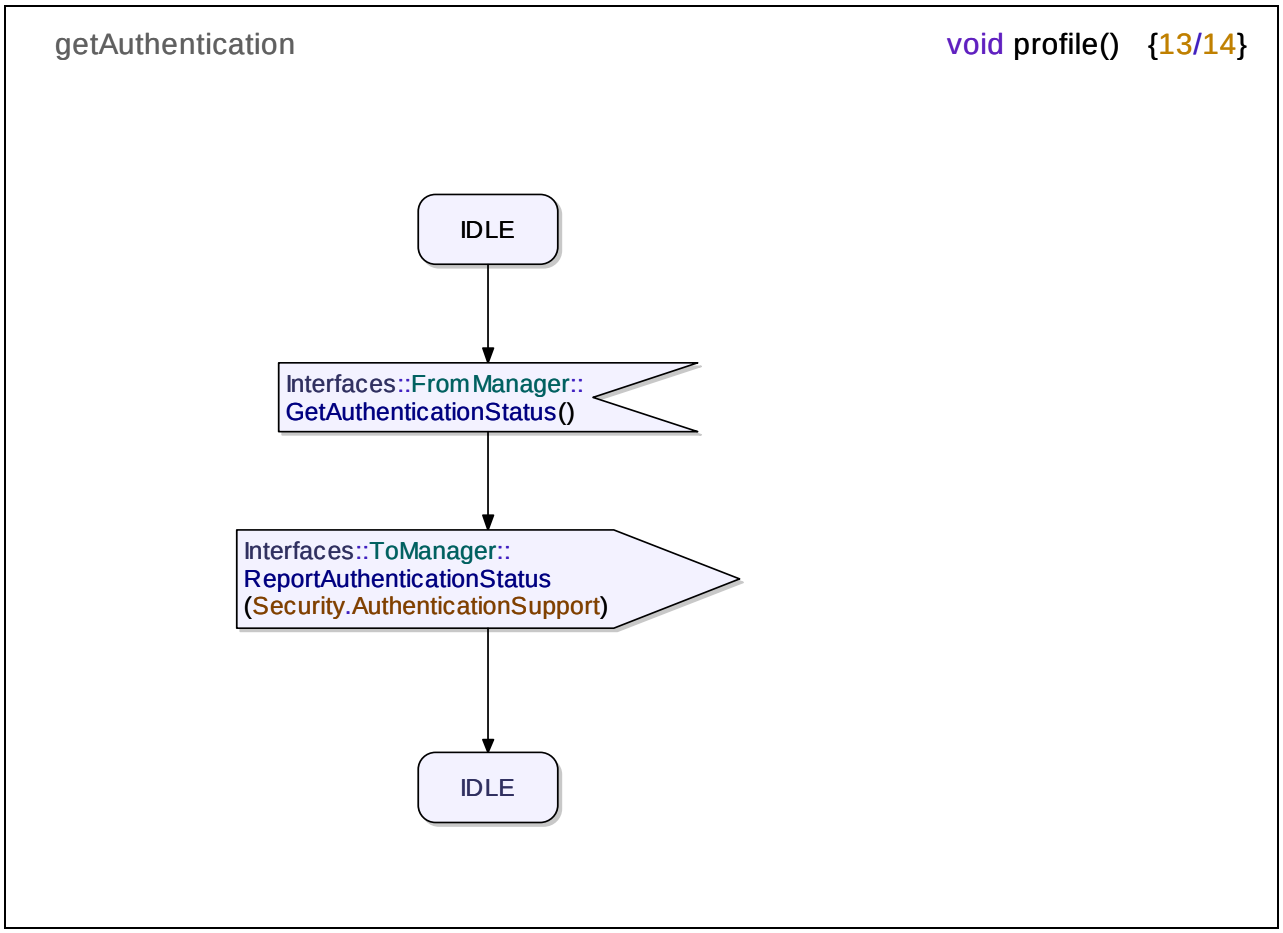



**Figure 11: State chart diagram for get authenticate status service capability**

### 5.4.3 Message authentication code model

NOTE: The MAC model is used in 3GPP for authentication of the infrastructure, and is the form used in IPsec for both ESP and AH.

The Message Authentication Code (MAC) model uses a significantly different method for authentication of the claimant than the challenge response method. A MAC is a cryptographic checksum obtained a secret key based one-way function applied to a message.

The MAC value protects both a message's integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

NOTE 1: Unlike digital signatures (see clause 5.4.5) MACs are computed and verified with the same key.

NOTE 2: MACs do not provide the property of Non-repudiation offered by signatures as the verifier can also act as claimant by generating MACs.

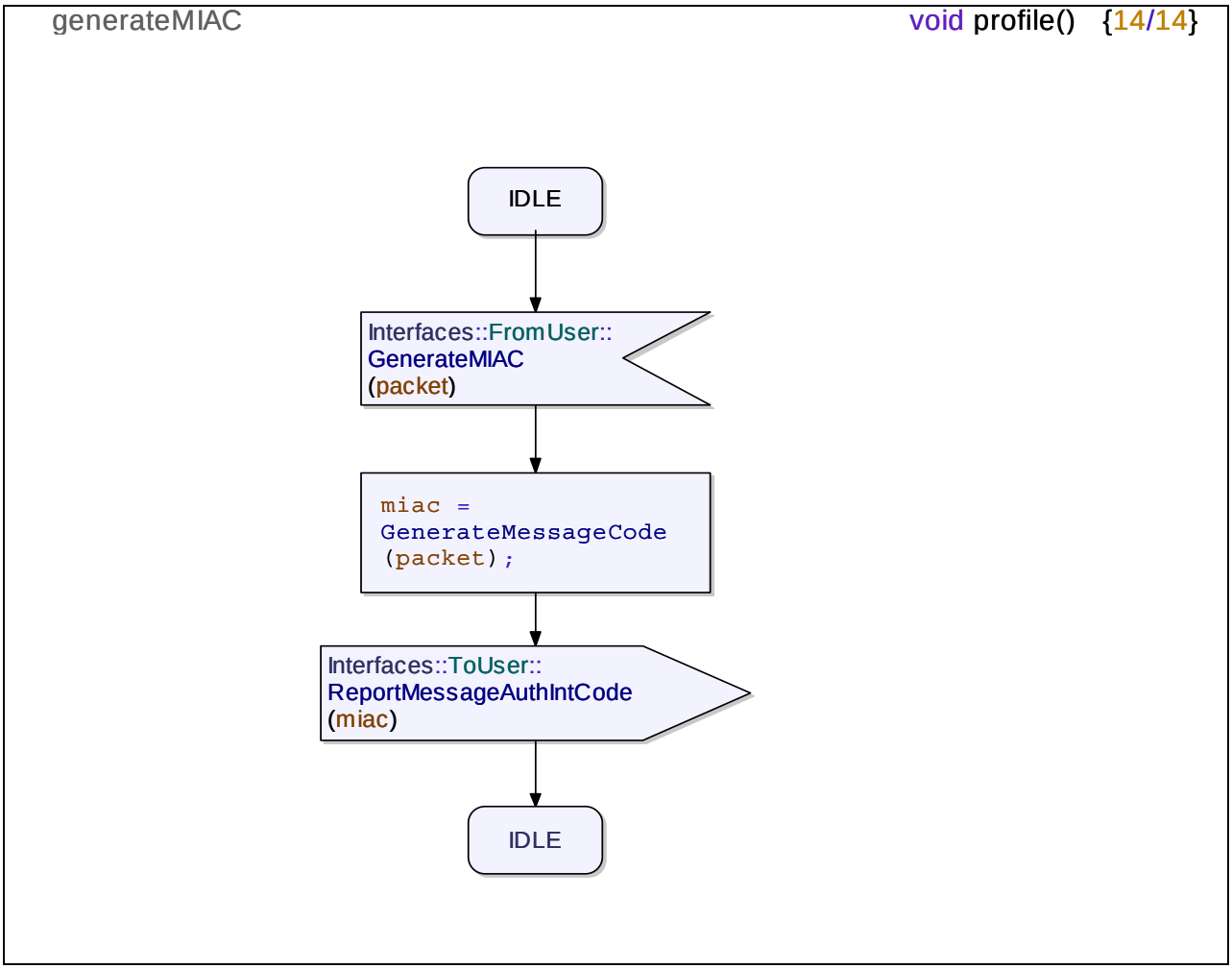



**Figure 12: State chart diagram for generate message integrity and authentication code service capability**

#### 5.4.3.1 Hash function-based MAC

Hash function-based MACs (HMACs) use a key or keys in conjunction with a hash function to produce a checksum that is appended to the message.

EXAMPLE: Keyed-MD5.

#### 5.4.3.2 Block cipher MAC

MACs can be derived from block ciphers.

EXAMPLE: DES-CBC MAC.

### 5.4.4 Digital signature

NOTE: Within the European Union Directive 1999/93/EC established the framework for electronic signatures based on three CEN Workshop Agreements as technical standards in accordance with the Directive. This is an active area of work within ETSI and CEN in the Technical Committee ESI.

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 13 illustrates the digital signature process.

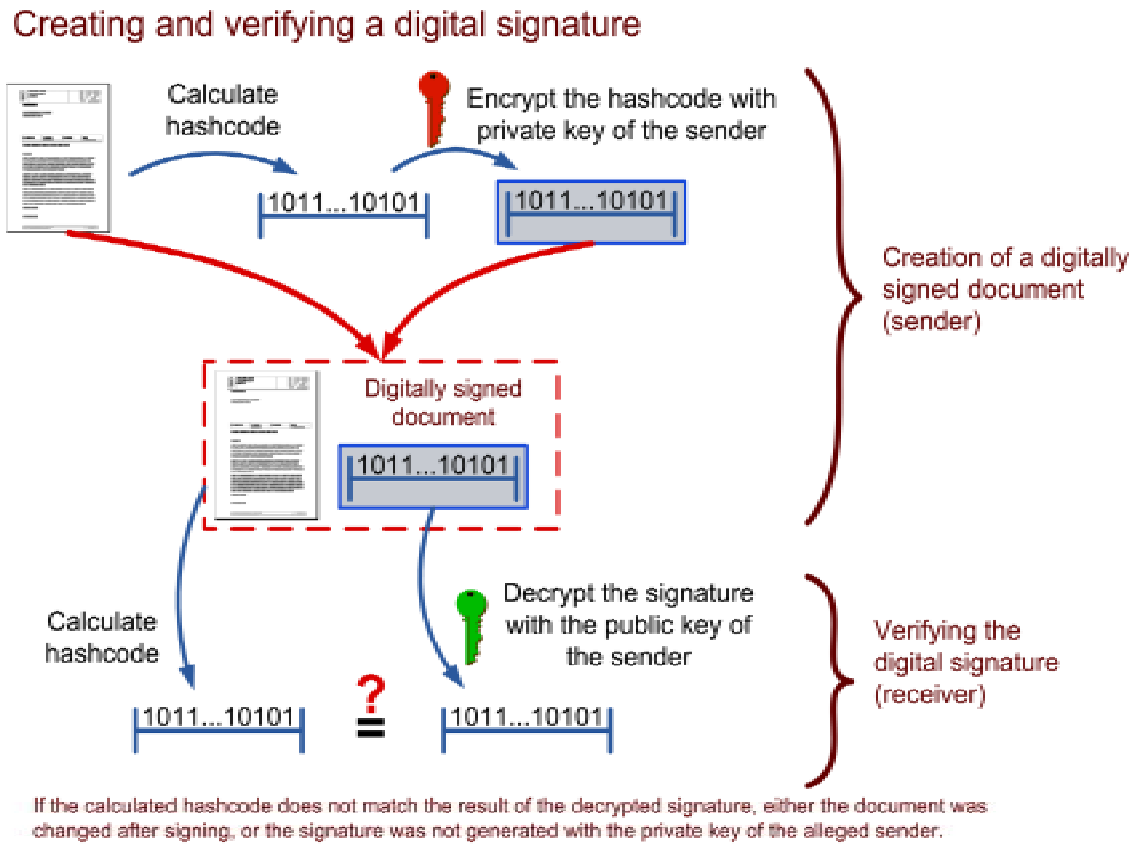



**Figure 13: Digital signature process**

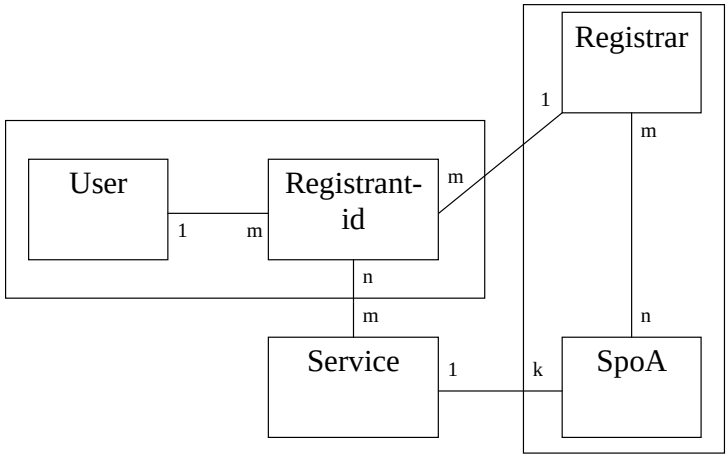
In the context of ICT and NGN digital signature is not generally applied for authentication but may be used within the application plane where commercial transactions occur. The present document does not define any digital signature schemes for use in authentication.

# 6 Access control counter-measures

## 6.1 Introduction

The primary purpose of the access control service is to counter the treat of unauthorized invocation of operations on the communications system. The use of access control is often considered to explicitly counter threats and their associated threat agents that lead to attacks of unauthorized use, disclosure, modification, destruction and denial of service.

Access control counter-measures act independently of authentication and confidentiality countermeasures but are used to determine if the identity (ideally confirmed through authentication) is authorized to use the service requested. Figure 14 shows a view of the access control problem wherein a user, represented by a registrant-id, is offered access to many services at potentially multiple attachment points.




NOTE 1: A single user may be associated with many registrant-ids.
NOTE 2: A registrant-id shall be associated with only one user.
NOTE 3: A registrant-id shall be associated with only one registrar.
NOTE 4: A registrar may be associated with many registrant-ids.
NOTE 5: A service may be associated with many SpoAs.
NOTE 6: In any registration instance a service shall be associated with only one SpoA.
NOTE 7: An SpoA shall be associated with only one Service.
NOTE 8: A registrant-id may be associated with many Services.

**Figure 14: Ordinal relations in ICT and the NGN**

## 6.2 Overall stage 1 model for access control

### 6.2.1 Procedures

#### 6.2.1.1 Provision/withdrawal

Access control shall always be available.

#### 6.2.1.2 Normal procedures

##### 6.2.1.2.1 Activation/deactivation/registration/interrogation

Access control shall always be activated.

##### 6.2.1.2.2 Invocation and operation

On receipt of a request to access a service from a known entity shall be validated against the access policy maintained for the service. The access policy may be applied in a number of ways:

- all requests conforming to a pattern have access;
- requests conforming to a pattern from authorized parties have access (white list);
- requests conforming to a pattern from known unauthorized parties are denied access (black list).

If the requestor is not allowed access to the named service access shall be denied.

#### 6.2.1.3 Exceptional procedures

##### 6.2.1.3.1 Activation/deactivation/registration/interrogation

Not applicable.

#### 6.2.1.3.2 Invocation and operation

In the event of any protocol failure no access shall be granted.

### 6.2.2 Interactions with other security services

In order to ensure the identity requesting service is valid the identity should be authenticated.

### 6.2.3 Interworking considerations

FFS.

## 6.3 Specific access control models (stage 2 models)

The generic model for an access control system consists of 3 functional elements:

- Access requestor
  - The entity requesting access to a specific network entity.
- Access policy verifier
  - The entity that checks to see if the requestor is allowed to access the specific network entity and which instructs the policy enforcer to enable/disable access.
- Access enforcer
  - The entity that enables or disables access to a resource for the access requestor under control of the policy validator.

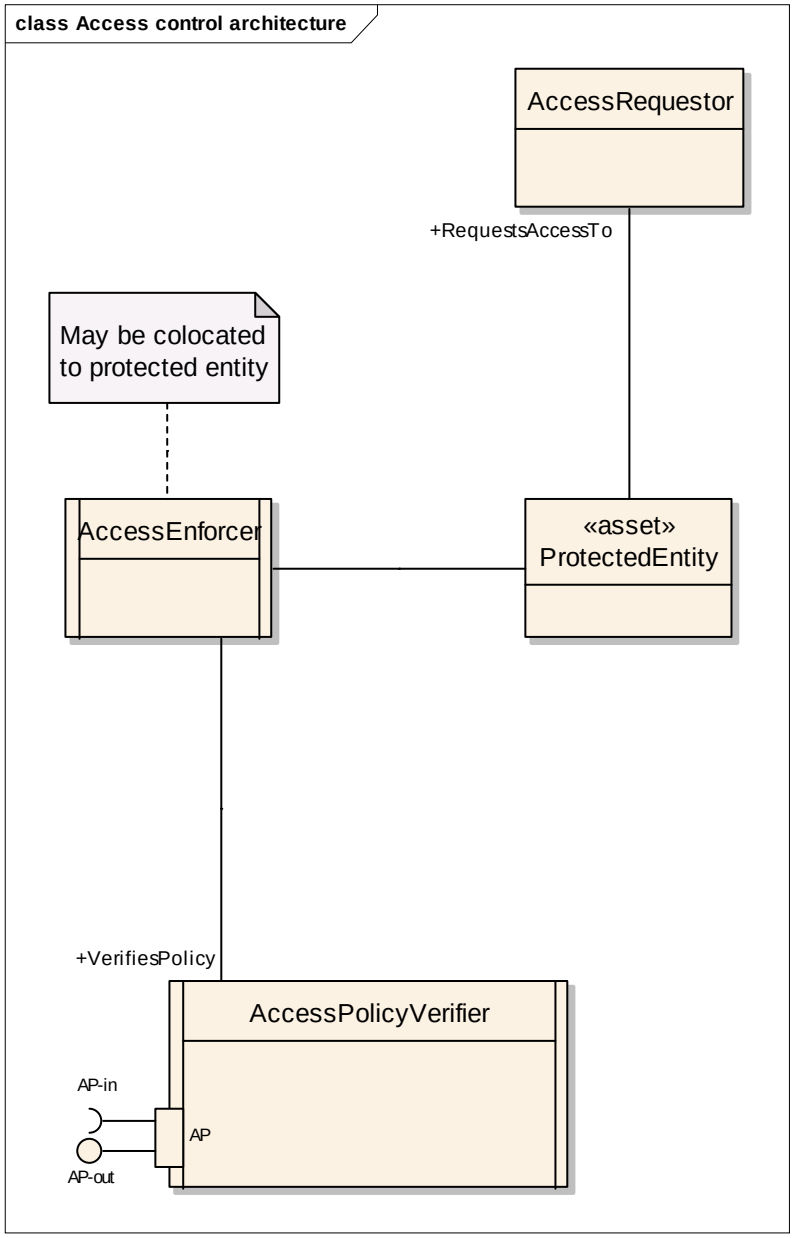



**Figure 15: Pattern for access control mechanism**

There are a number of deployment models that offer different protection and performance opportunities. The model offered in figure 16 places the access enforcer as a firewall-like entity that intercepts every input to the protected asset, validates it and either forwards it or rejects it.

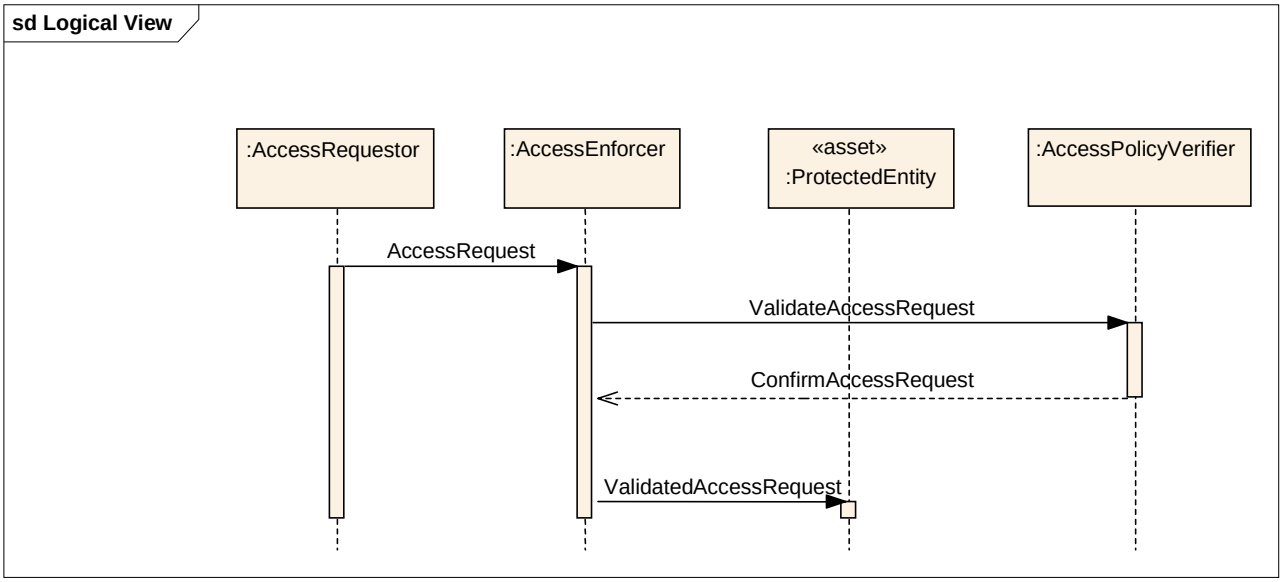



**Figure 16: Interaction diagram for access control pattern (firewall mode)**

The firewall model may be applied in a number of ways:

- all requests conforming to a pattern have access;
- requests conforming to a pattern from authorized parties have access (white list);
- requests conforming to a pattern from known unauthorized parties are denied access (black list).

# 7 Confidentiality service

## 7.1 Introduction

Cryptographic confidentiality services may be provided in one of 2 ways:

- Streaming ciphers
  - One bit of transmitted data encrypted at a time.
  - Errors in the transmission path affect only one bit (no error propagation).
  - There should be no processing delay due to the ciphering process.
- Block ciphers
  - A fixed length block of data encrypted at a time.
  - Errors in the transmission path may affect the entire block (error propagation).
  - The block to be encrypted has to be prepared prior to transmission and may incur some processing delay.

## 7.2 Provided services

### 7.2.1 Description

Confidentiality services are provisioned by use of an encryption service that lies between the service encoding unit and the transport service for the Service Data Unit (SDU).

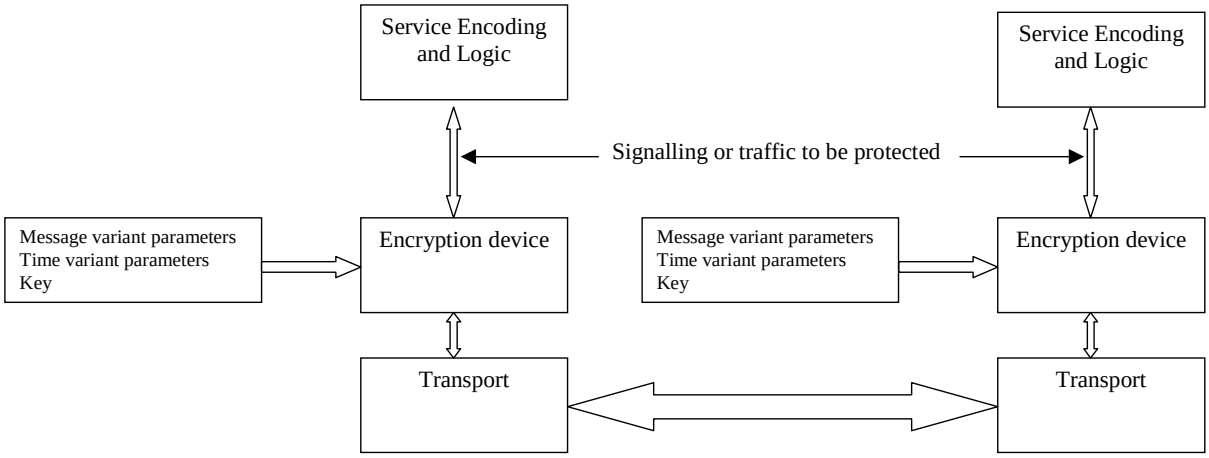
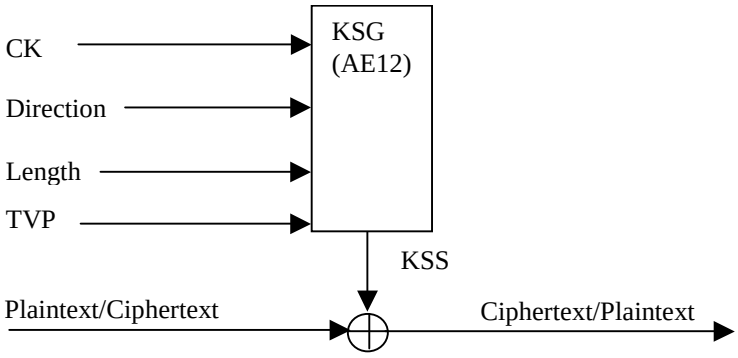



**Figure 17: Location of encryption in generic ICT model**

The encryption device shall be chosen to meet the error characteristics of the transmission medium, for example a streaming cipher device operating in a bit replacement mode (i.e. every bit of plaintext is replaced with a bit of ciphertext) is often used in a radio environment where single bit errors are common.

A terminal may have more than one algorithm but shall use the algorithm indicated by the SpoA at the time of registration.




CK: Cipher Key
KSG: Key Stream Generator
KSS: Key Stream Segment
TVP: Time Variant Parameter

**Figure 18: Speech and control information encryption**

## 7.2.2 Encryption mechanism

The KSS bits shall be modulo 2 added (XORed) with plain text bits in traffic and signalling Service Data Units (SDUs) to obtain encrypted cipher text bits. KSS(0) shall be XORed with the first transmitted bit of the first SDU, and so on. Any unused bits of KSS shall be discarded.

## 7.2.3 Implicit authentication

If authentication is used as the mechanism to generate (or derive) the confidentiality key (CK in figure 18) as happens in the TETRA system (EN 300 392-7, see Bibliography) every exchange of encrypted traffic or signalling using the generated/derived key is implicitly authenticated as the confidentiality key is generated/derived by the authenticating parties and known only to them.

# 7.3 Overall stage 1 model for confidentiality

## 7.3.1 Procedures

### 7.3.1.1 Provision/withdrawal

Confidentiality can optionally be available.

### 7.3.1.2 Normal procedures

#### 7.3.1.2.1 Activation/deactivation/registration/interrogation

Confidentiality can optionally be activated.

#### 7.3.1.2.2 Invocation and operation

Confidentiality may be invoked on one or more of the following interfaces referenced in the model in clause 4:

- Confidentiality of communication at TpoA/SpoA/ApoA.

Within the system the countermeasures are extended to cover interactions between layers both vertically and horizontally.

- Confidentiality of communication from Service to Service.

### 7.3.1.3 Exceptional procedures

#### 7.3.1.3.1 Activation/deactivation/registration/interrogation

Not applicable.

#### 7.3.1.3.2 Invocation and operation

Exceptional procedures should be invoked when some attacks take place such as man in the middle, differential attacks, weak keys, probabilistic or linear attacks, linear cryptanalysis, interpolation attacks, partial key guess and brute force attacks.

## 7.3.2 Interactions with other security services

The authentication services may provide keying material for the confidentiality services.

## 7.3.3 Interworking considerations

The authentication algorithms used by each of the participant entities have to be matched.

# 7.4 Specific confidentiality models (stage 2 models)

The generic model for an confidentiality system consists of 5 functional elements (ITU-T Recommendation X.814 taken into account):

- Confidentiality initiator agent
  - The entity requesting access to the confidentiality services and ciphering the massages.
- Key manager
  - Responsible for maintaining keys and distributing them securely to the active agents.

- Confidentiality responder agent
  - The entity granting access to the confidentiality services and deciphering the messages.
- Confidentiality policy verifier
  - The entity that checks to see if the initiator and responder are allowed to use specific confidentiality services and which instructs the confidentiality enforcer to enable/disable that use.
- Confidentiality enforcer
  - The entity that enables or disables the use of the confidentiality services for the confidentiality initiator and responder.

# 8 Integrity service

## 8.1 Introduction

Integrity mechanisms ensure the detection and prevention, and may provide recovery, of unauthorized modification of information.

The purpose of the integrity service is to protect the integrity of data and of their relevant attributes which can be compromised in a number of different ways as defined in ISO/IEC 10181-6 [24]:

1) unauthorized data modification;
2) unauthorized data deletion;
3) unauthorized data creation;
4) unauthorized data insertion;
5) unauthorized data replay.

## 8.2 Provided services

Integrity services as defined in ISO/IEC 10181-6 [24] are classified according to the following criteria:

1) By the type of violation they protect against. The types of violation are:
   a) unauthorized data modification;
   b) unauthorized data creation;
   c) unauthorized data deletion;
   d) unauthorized data insertion;
   e) unauthorized data replay.
2) By the type of protection they support. The types of protection are:
   a) prevention of integrity compromise;
   b) detection of integrity compromise.
3) By whether they include recovery mechanisms or not:
   a) with recovery the unshield operation may be able to recover the original data (and possibly signal a recovery action or an error for purposes such as audit) whenever the **validate** operation indicates alteration;

b) without recovery the unshield operation is unable to recover the original data whenever the validate operation indicates alteration.

The example algorithm from 3GPP is reviewed here as providing an example of a generic integrity algorithm with replay protection. The input parameters to the algorithm are the Integrity Key (IK), a time dependent input (COUNT-I), a random value generated by the network side (FRESH), and the data (MESSAGE). Based on these input parameters the user computes with the function f the message authentication code for data integrity (MAC-I) which is appended to the message when sent over the radio access link. The receiver computes XMAC-I on the messages received in the same way as the sender computed MAC-I on the message sent.

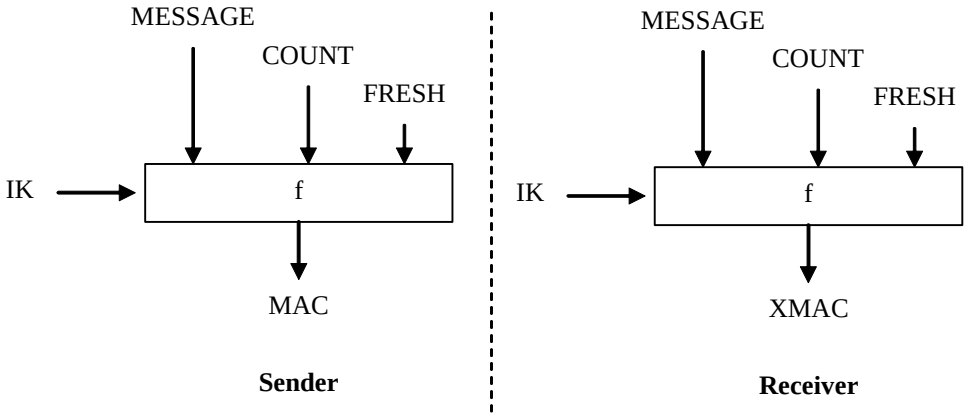



**Figure 19: Example of integrity algorithm**

## 8.3 Requirements statements for integrity service functional capabilities (ISO/IEC 15408-2)

The integrity service requirements may be stated using functional capabilities as defined in ISO/IEC 15408-2 [23] as shown in table 2.

**Table 2: ISO/IEC 15408-2 functional capabilities for integrity countermeasure**

| Shortname | Definition | Form of assignment in NGN |
|---|---|---|
| FPT_ITI.1.2 | The system (ICT/NGN) shall provide the capability to verify the integrity of all system (ICT/NGN) data transmitted between the system (ICT/NGN) and a remote trusted IT product and perform deletion and notification if modifications are detected. | The receiving entity will delete modified data and notify the receiving party. |
| FPT_ITI.2.2 | The system (ICT/NGN) shall provide the capability to verify the integrity of all system (ICT/NGN) data transmitted between the system (ICT/NGN) and a remote trusted IT product and perform notification if modifications are detected. | Notification of receiving party. |
| FPT_ITI.2.3 | The system (ICT/NGN) shall provide the capability to correct transmission errors of all system (ICT/NGN) data transmitted between the system (ICT/NGN) and a remote trusted IT product. | Transmission errors should be corrected. |
| FPT_ITT.1.1 | The system (ICT/NGN) shall protect system (ICT/NGN) data from modification when it is transmitted between separate parts of the TOE. | Data should be protected from modification. |
| FPT_ITT.3.1 | The system (ICT/NGN) shall be able to detect modification of data for system (ICT/NGN) data transmitted between separate parts of the TOE. | Modification. |
| FPT_ITT.3.1 | The system (ICT/NGN) shall be able to detect substitution of data for system (ICT/NGN) data transmitted between separate parts of the TOE. | Substitution. |
| FPT_ITT.3.1 | The system (ICT/NGN) shall be able to detect re-ordering of data for system (ICT/NGN) data transmitted between separate parts of the TOE. | Re-ordering. |
| FPT_ITT.3.1 | The system (ICT/NGN) shall be able to detect deletion of data for system (ICT/NGN) data transmitted between separate parts of the TOE. | Deletion. |
| FPT_ITT.3.2 | Upon detection of a data integrity error, the system (ICT/NGN) shall take the following actions: delete modified data and notify the receiving party. | The receiving entity will delete modified data and notify the receiving party. |

# 8.4 Overall stage 1 model for integrity

## 8.4.1 Procedures

### 8.4.1.1 Provision/withdrawal

Integrity can optionally be available.

### 8.4.1.2 Normal procedures

#### 8.4.1.2.1 Activation/deactivation/registration/interrogation

Integrity can optionally be activated.

#### 8.4.1.2.2 Invocation and operation

Integrity may be invoked on one or more of the following interfaces referenced in the model in clause 4:

- Integrity of communication at TpoA/SpoA/ApoA.

Within the system the countermeasures are extended to cover interactions between layers both vertically and horizontally.

- Integrity of communication from Service to Service.

### 8.4.1.3 Exceptional procedures

#### 8.4.1.3.1 Activation/deactivation/registration/interrogation

Not applicable.

#### 8.4.1.3.2 Invocation and operation

FFS.

## 8.4.2 Interactions with other security services

The authentication services may provide keying material for the integrity services.

## 8.4.3 Interworking considerations

The integrity algorithms used by each of the participant entities have to be matched.

# 8.5 Specific integrity models (stage 2 models)

The generic model for an integrity system consists of 5 functional elements:

- Integrity encoder agent
  - The entity requesting access to the integrity services and ciphering the massages.
- Key manager
  - Responsible for maintaining keys and distributing them securely to the active agents. In a Public Key Infrastructure (PKI) environment the Key manager may be considered as equivalent to the Certification Authority when X.509 certificates are used to distribute keys.

- Integrity decoder agent
  - The entity requesting access to the integrity services and deciphering the messages.
- Integrity policy verifier
  - The entity that checks to see if the encoder and decider are allowed to use specific integrity services and which instructs the integrity enforcer to enable/disable that use.
- Integrity enforcer
  - The entity that enables or disables the use of the integrity services for the integrity encoder and decoder.

## 8.6 Implicit authentication

If authentication is used as a key generation mechanism where a derived integrity key is used in the integrity service every proof of signalling integrity using the derived integrity key is implicitly authenticated as the integrity key is derived by the authenticating parties and known only to them.

# 9 Non-repudiation service

## 9.1 Overview

ISO/IEC 10181-4 [22] states:

QUOTE: *"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 20).

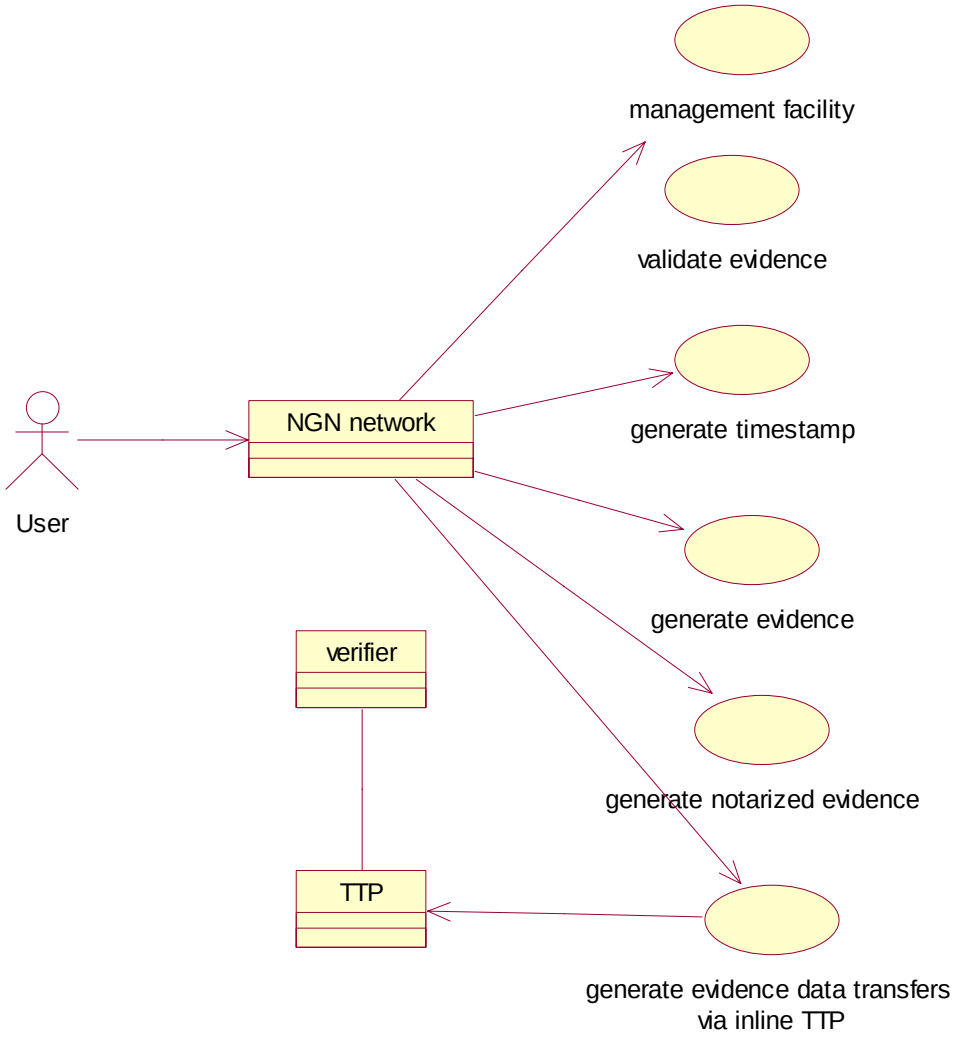



**Figure 20: Simplified architecture of use of non-repudiation facilities in NGN**

Using ISO/IEC 10181-4 [22] 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. Non-repudiation services may be requested by entities other than those involved in the event or action.

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

## 9.2 Requirements statements for non-repudiation service functional capabilities (ISO/IEC 15408-2)

The requirements for the non-repudiation service may be stated using functional capabilities as defined in ISO/IEC 15408-2 [23] and shown in table 3.

**Table 3: ISO 15408-2 Functional capabilities (Communication class (non-repudiation))**

| Shortname | Definition | Form of assignment in NGN |
|---|---|---|
| FCO_NRO.1.1 | The system (ICT/NGN) shall be able to generate evidence of origin for transmitted Billable events and messages at the request of the originator. | Billable events and messages |
| FCO_NRO.1.1 | The system (ICT/NGN) shall be able to generate evidence of origin for transmitted Billable events and messages at the request of the recipient. | Billable events and messages |
| FCO_NRO.1.3 | The system (ICT/NGN) shall provide a capability to verify the evidence of origin of information to originator, given [**assignment**: limitations on the evidence of origin]. | Originator and recipient |
| FCO_NRO.1.3 | The system (ICT/NGN) shall provide a capability to verify the evidence of origin of information to recipient given [**assignment**: limitations on the evidence of origin]. | Originator and recipient |
| FCO_NRO.2.3 | The system (ICT/NGN) shall provide a capability to verify the evidence of origin of information to originator given evidence of origin complies with FCO_NRO.1.1. | |
| FCO_NRO.2.3 | The system (ICT/NGN) shall provide a capability to verify the evidence of origin of information to recipient given evidence of origin complies with FCO_NRO.1.1. | |
| FCO_NRR.1.1 | The system (ICT/NGN) shall be able to generate evidence of receipt for received Billable events and messages at the request of the originator. | Billable events and messages by originator |
| FCO_NRR.1.1 | The system (ICT/NGN) shall be able to generate evidence of receipt for received Billable events and messages at the request of the recipient. | Billable events and messages by recipient |

## 9.3 Overall stage 1 model for non-repudiation

### 9.3.1 Procedures

#### 9.3.1.1 Provision/withdrawal

Non-repudiation can optionally be available.

#### 9.3.1.2 Normal procedures

##### 9.3.1.2.1 Activation/deactivation/registration/interrogation

Non-repudiation can optionally be activated.

##### 9.3.1.2.2 Invocation and operation

Non-repudiation is a composed countermeasure in the model of clause 4. The invocation and operation procedures of the other countermeasures defined in the present document can apply in this clause. In clause 9.3.2 below the interaction with other security services is defined.

#### 9.3.1.3 Exceptional procedures

##### 9.3.1.3.1 Activation/deactivation/registration/interrogation

Not applicable.

##### 9.3.1.3.2 Invocation and operation

Non-repudiation is a composed countermeasure in the model of clause 4. The exceptional invocation and operation procedures of the other countermeasures defined in the present document can apply in this clause. In clause 9.3.2 below the interaction with other security services is defined.

### 9.3.2 Interactions with other security services

In ISO/IEC 10181-4 [22] 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.

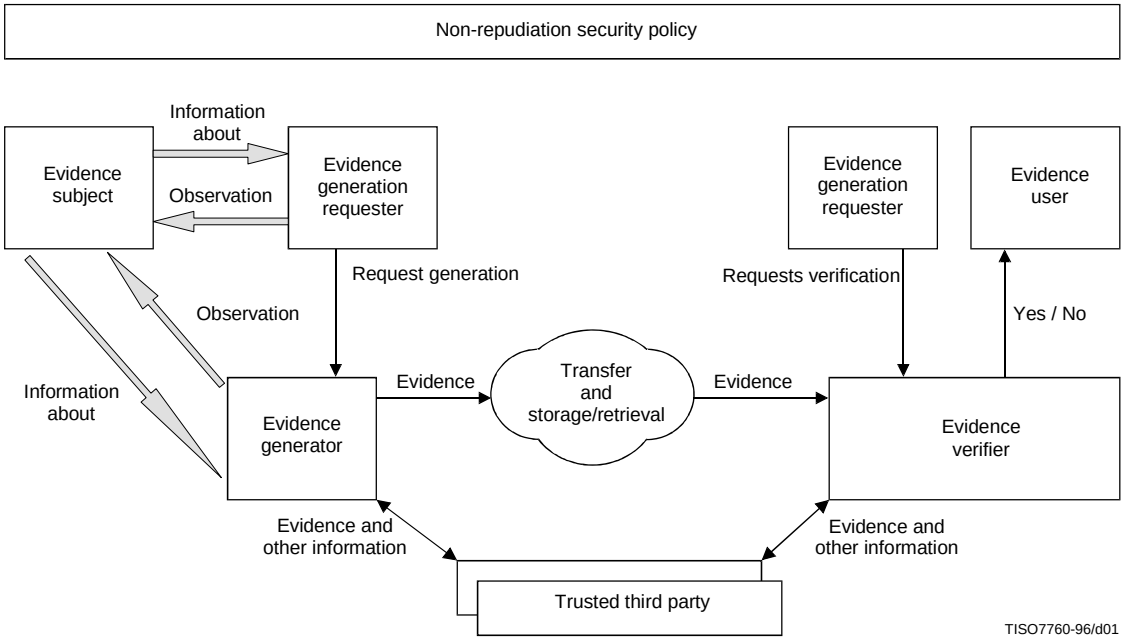
- Authentication
  - When entities interact with a TTP they may be required to prove their identity using an authentication service.
- Access control
  - An access control service may be used to ensure that information stored by a TTP, or service offered by a TTP, is made available only to authorized 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.

### 9.3.3 Interworking considerations

FFS.

## 9.4 Specific non-repudiation stage 2 models

The generic model for an non-repudiation system consists of 5 functional elements. Some of these elements are also defined in ISO/IEC 10181-4 [22].




NOTE: This figure is illustrative, not definitive.

**Figure 21: Entities involved in the generation, transfer, storage/retrieval and verification phases (from ISO/IEC 10181-4 clause 5.3)**

# 10 Subscription Services

FFS

# 11 Authorization services

FFS

# 12 Key management service

## 12.1 Overview

Where cryptographic methods are used to support security the primary element of achieving security is in the key. The general assumptions for any system relying on cryptology are:

- Knowledge of how algorithms work is in the public domain.
- Knowledge of protocols for authentication and key establishment are in the public domain.

The only means of assuring security remains in place, over and above the known limitations of the algorithm and protocol, is in the secrecy of the key. A secret is by definition not a secret when it is widely known and so a shared secret is not really secret. Symmetric key cryptography works only by control of the number of entities who know the secret and generally, for telecommunications, the intention is to limit this to two parties only. However in public communication where secrecy may be required of communication to a large number of unknown parties the normal definition of secrecy cannot apply. The challenge of this is met by a set of techniques based on non-secret cryptology, or asymmetric keying, whereby a key has two components one of which is private and the other is public. The success is built on the mathematics of the key construction and on the algorithms that make use of the key, but essentially it consists of a pair of one-way functions and the view that is computationally infeasible from knowledge of the public key to find the matching private key. A public key can then be distributed freely to either receive data encrypted by the private key, or to encrypt data to be sent to the holder of the private key.

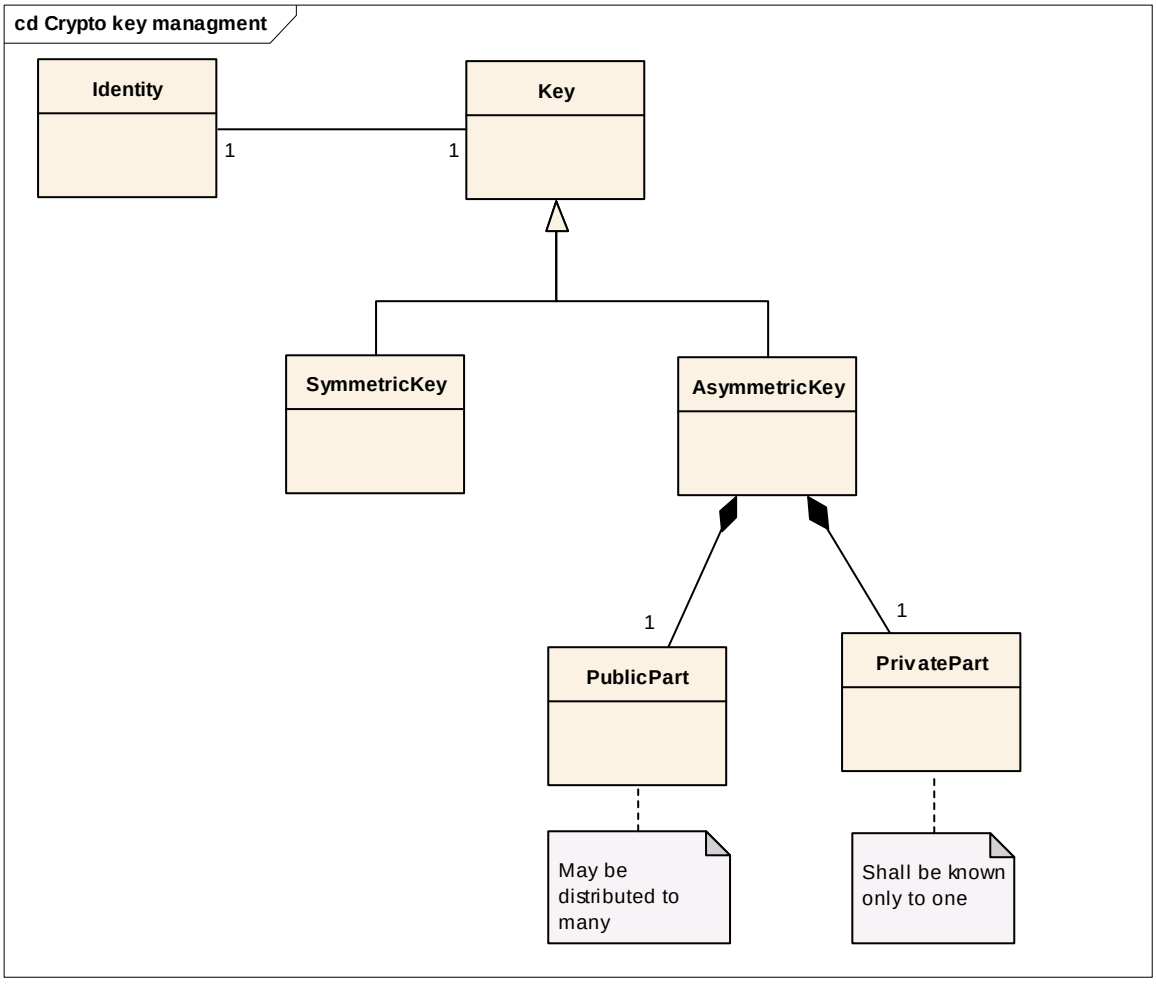



**Figure 22: Simplified model of key relationships**

## 12.2 Symmetric key management

In symmetric key cryptography there is one mandatory requirement:

- Only 2 parties have access to the key.

In order to maintain compliance with this requirement there are a number of approaches to key distribution that may be taken. In each case the key should be delivered in a manner that leaves an audit trail. In addition the key should be transmitted in a tamper proof format: tamper proofing may be achieved in either software or hardware. As defined in ISO/IEC 10181-4 [22], ITU-T Recommendation X.813 (see Bibliography), clause 8 as a framework.

## 12.3 Asymmetric key management

### 12.3.1 Overview

In asymmetric cryptography a public key can be distributed to either receive data encrypted by the private key, or to encrypt data to be sent to the holder of the private key. However there is a legitimate concern that whilst the mathematical relationship is understood to work there is often only a weak relationship between the two communicating parties hence trust that the data is visible to the correct party has to be assured. The counter to the trust problem is to distribute public keys through a trusted source within public key certificates according to clause 7 of ITU-T Recommendation X.509 [25].

NOTE: This document does not replace ITU-T Recommendation X.509 [25] but is intended to assist users of public key cryptosystems in its use.

### 12.3.2 Certificate generation

A certificate is a signed data object that contains the data elements outlined in table 4.

The content of a digital certificate can be summarized as follows:

- The identifier of the certification authority.
- The unique identifier of the user of the certificate.
- Some attributes of the user, like address, company, tax code, etc.
- Public key, generated with the private key, to be used to verify digital signature.
- Period of validity of the certificate, defined by a start date and an end date.
- Unique identity code of the certificate.
- Digital signature of the certification authority.
- Environment in which the certificate is valid.
- Non-mandatory attributes.

**Table 4: Contents of X.509 certificate**

| Information element | M/O | Notes |
|---|---|---|
| Version | M | Default value of v1 |
| Serial number | M | |
| Signature | M | |
| Issuer | M | |
| Validity | M | |
| Subject | M | |
| Subject public key information | M | |
| Issuer unique identifier | O | |
| Subject unique identifier | O | |
| Extension | O | |

### 12.3.3 Certificate extension

Certificate extensions can be used to provide service and service capabilities authorization as explained in clause 7.

As defined in ITU-T Recommendation X.509 [25], X.509v3 the extensions provide methods for associating additional attributes with users or public keys and for managing the hierarchy. It also allows communities to define private extensions. Extensions can be defined in a certificate as critical and no-critical. A system that uses a certificate must reject the certificate if it encounters a critical extension it does not recognize. Each extension includes an OID and an ASN.1 structure. Only one instance of a particular extension may appear in a particular certificate.

### 12.3.4 Certification authority

A Certification Authority (CA) is a trusted third party that issues certificates. In PKIs the CA verifies identity.

CAs (certification authorities) can issue different kinds of certificates:

- Identity.
- Authorization.
- Transaction.
- Time Stamp.

Repudiation services as defined in this document may use CA as TTP.

# Annex A (informative): Modelling techniques in countermeasure development

## A.1 Introduction

In the development of the security aspects of the NGN and in particular in the development of the Threat/vulnerability/risk analysis the use of simple modelling techniques to illustrate security relationships and to weigh risk was promoted. The modelling language of choice was the Unified Modelling Language (UML) as this fits to the entire development lifecycle. For the development of countermeasures UML is also used with the focus on behavioural relationships and ease of illustration of key concepts.

The following key concepts are reinforced:

- **Assets** of the system are at risk as they contain **weaknesses** that may be exploited for specific **threats** by specific **threat agents** giving rise to **unwanted incidents**.
- **Countermeasures** are deployed as special instances of **assets** to protect assets by limiting the ability of a **threat agent** to enact a **threat** thus removing (or significantly reducing) the possibility of an **unwanted incident** arising.
- The purpose of a **countermeasure** is to mitigate the **risk** to the **system** within the budget constraints of the system.

NOTE: Budget constrains cover performance, availability, complexity as well as cost.

## A.2 Use of UML patterns

In the design and development lifecycle the stage 1 and stage 2 phases of a design are intended to be applicable to many forms of implementation at stage 3. The use of patterns (frameworks) at stage 2 offers the same attribute as many detail implementations can be derived that comply to the same pattern or framework. The root for the security frameworks in the present document are those defined in the ISO/IEC 10181 [1] series of standards (mirrored in the ITU-T Recommendation X.800 series) updated for presentation and development using UML.

## A.3 Use of UML stereotypes

UML allows extension of its meta-model by means of stereotypes. Example of the use of stereotypes for UML in security design and analysis may be found in CORAS [CORAS] and in UMLsec [UMLsec]. The use of UML stereotypes used in this document are similar to those used in both CORAS and UMLsec with specific specialization for the standardization community.

# Annex B (informative): Use of IPsec to implement countermeasures

NOTE: This annex is a review of RFCs 4301 [11], 4303 [12], 4305 [14] and 4306 [13] when considered as applying to the countermeasures described in the core of this document.

## B.1 Overview

IPsec is a suite of services defined in the IETF to offer the following services:

- Source authentication (RFC 4303 [12] using ESP).
- Data integrity (RFC 4303 [12] using ESP).
- Data confidentiality (RFC 4303 [12] using ESP).
- Key distribution and management (RFC 4306 [13] using IKEv2).

Figure B.1 shows IPsec as a class of capabilities (of stereotype "protocol") composed of two sub-capabilities: Authentication using the Message Authentication Code approach (which also provides a proof of packet data integrity) and Packet Confidentiality.

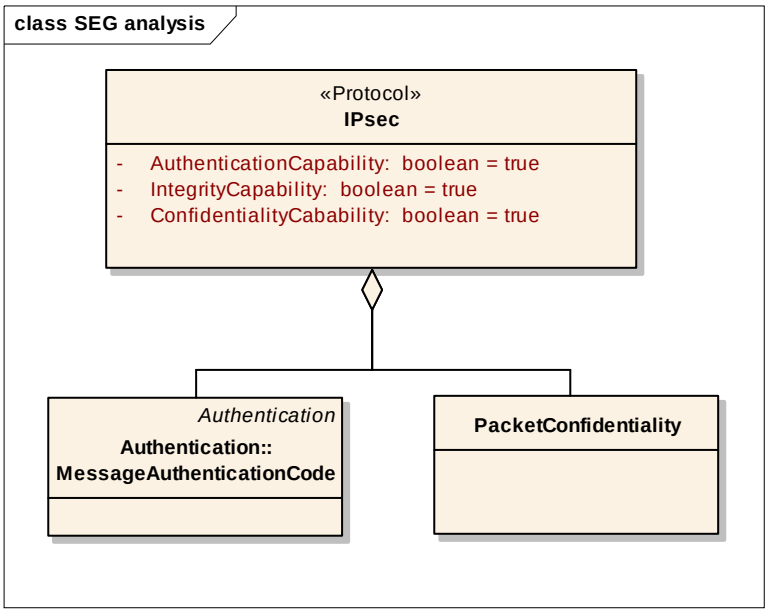



**Figure B.1: IPsec showing components**

IPsec is a key feature of IPv6 where its support is mandatory (i.e. all IPv6 deployments shall be able to support IPsec) with the key components also supported by IPv4. IPsec was originally published in 1996 but extensively revised and republished in 2005. In the IPsec Security Architecture RFC 4301 [11] the use of Encapsulating Security Payload (ESP) defined in RFC 4303 [12] is mandated where ESP provides two security services:

- Confidentiality
  - via encryption and limited traffic flow confidentiality.
- Connectionless integrity with data origin authentication and anti-replay.

**Table B.1: ESP contents (from RFC 4303)**

| Field name | Size (bits) | M/O/C | Function/comment |
|---|---|---|---|
| Security Parameters Index (SPI) | 32 | M | Used to uniquely identify the Security Association of the current datagram in combination with the destination IP address and the security protocol. |
| Sequence number field | 32 | M | Used for replay protection. |
| Payload data | Variable | M | |
| Padding field | 0 to 2040 | | Up to 255 bytes in length. |
| Pad length | 8 | M | |
| Next header | 8 | M | |
| Authentication data | N times 32 | O | Contains the Integrity Check Value (ICV) for this packet. |
| NOTE 1: The SPI and Sequence number fields constitute the header of ESP, the pad length and next header field constitute the tail of ESP.<br>NOTE 2: The payload data plus padding field plus Pad length plus Next header are encrypted. | | | |

### B.1.1 Identification of principals

In IPsec authentication the principal is the end point router with a known source address.

## B.2 IPsec architecture

The architecture of IPsec allows a number for a of implementations and two distinct modes of operation:

- Tunnel mode.
- Transport mode.

The selection of mode (tunnel versus transport) and the option of gateway versus host mode, and of the various "Bump in the Stack" versus "Bump in the wire" are all critical and shall be explicitly defined in this annex.

The use of IPsec ESP would normally apply at the following reference points identified in clause 4: TpoA; T2TpoA.

NOTE: A deployment at reference points TpoA and T2TpoA is equivalent to deployment at the $Z_A$ and $Z_B$ interfaces defined in TS 133 210 [18].

## B.3 Key management for IPsec

IPsec key management is described as using IKE although IKE is not mandated. The key management results in a known security association for each packet where the security association identifies the security features and the relevant algorithms and keys to be applied when processing each packet.

## B.4 IPsec implementation of authentication and integrity

### B.4.1 Authentication algorithm selection

The algorithms to be used in IPsec are defined in RFC 4305 [14].

EXAMPLE: AES-XBC-MAC-96 as defined in RFC 3566 [15].

#### B.4.1.1 Combined algorithm selection

The combined algorithm option is defined in clause 3.2.3 of RFC 4303 [12] with algorithm specified in RFC 4305 [14].

EXAMPLE: AES-CCM as defined in RFC 3686 [17].

# B.5 IPsec implementation of data confidentiality

## B.5.1 Confidentiality algorithm selection

The algorithms to be used in IPsec are defined in RFC 4305 [14].

EXAMPLE: AES-CBC with 128 bit keys as defined in RFC 3602 [16].

### B.5.1.1 Combined algorithm selection

The combined algorithm option is defined in clause 3.2.3 of RFC 4303 [12] with algorithms specified in RFC 4305 [14].

EXAMPLE: AES-CCM as defined in RFC 3686 [17].

## B.5.2 Requirements on the construction of the IV

The use of AES-CBC requires the use and transmission of an initialization vector for the algorithm (see RFC 3602 [16]).

NOTE: The requirements defined in this annex update those found in TS 133 210 [18] to take into account the restructuring of the IPsec RFCs.

- The IV field should be the same size as the block size of AES).
- The IV should be chosen at random with the following additional constraints:
  - The IV is not to be constructed from the encrypted data of the preceding encryption process.
  - The IV has to be unpredictable to any party other than the originator.

## B.5.3 Application of AES-CBC

The data to be encrypted has to be padded such that the length of the (Payload-Data || Padding || Pad length || Next header) combined field is a multiple of the block size (i.e. N*128 bits in length).

The IV field is not to be encrypted.

# Annex C (informative): Bibliography


- GSM 03.20: "European digital cellular telecommunications system (Phase 1); Security related network functions".
- GSM 02.09: "Digital cellular telecommunications system (Phase 2); Security aspects".
- GSM 12.03: "Digital cellular telecommunications system (Phase 2); Security management".
- ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security ".
- ETSI TS 101 303: "Telecommunications and Internet Protocol Harmonization Over Networks (TISPAN) Release 4; Service Independent Requirements Definition; Service and Network Management Framework; Overview and Introduction".
- ETSI TS 101 882-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TISPAN) Release 4; Protocol Framework Definition; Part 2: Registration and Service Attachment service meta-protocol definition".
- ITU-T Recommendation H.225.0 Version 2: "Call Signalling Protocols and Media Stream Packetization for Packet Based Multimedia Communications Systems".
- ITU-T Recommendation H.245 Version 3: "Control Protocol for Multimedia Communication".
- ITU-T Recommendation H.323 Version 3: "Packet Based Multimedia Communication Systems".
- ITU-T Recommendation H.323 Annex F: "Simple Endpoint Types".
- ITU-T Recommendation H.323 Annex J: "Security for H.323 Annex F".
- ITU-T Recommendation H.235 Version 2: "Security and Encryption for H Series (H.323 and other H.245 based) multimedia terminals".
- ITU-T Recommendation I.130: "Method for the characterization of telecommunication services supported by an ISDN and network capabilities of an ISDN".
- ISO/IEC 10181-2: "Information technology - Open Systems Interconnection - Security frameworks for open systems: Authentication framework".

NOTE: Equivalent to ITU-T Recommendation X.811.

- ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- ITU-T Recommendation X.813: "Information Technology - Open Systems Interconnection - Security Frameworks for Open Systems - Non-Repudiation".
- ITU-T Recommendation X.800 series.

# History

| Document history | | |
|---|---|---|
| V4.1.1 | February 2003 | Publication |
| V4.2.1 | February 2007 | Publication |
| | | |
| | | |
| | | |