

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Review of activity on security



Reference

DTR/TISPAN-07011-Tech

Keywords

management, report, security

ETSI

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

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

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

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2005.
All rights reserved.

DECTTM, **PLUGTESTS**TM and **UMTS**TM are Trade Marks of ETSI registered for the benefit of its Members.
TIPHONTM and the **TIPHON logo** are Trade Marks currently being registered by ETSI for the benefit of its Members.
3GPPTM is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

Contents

Intellectual Property Rights	5
Foreword.....	5
1 Scope	6
2 References	6
3 Definitions and abbreviations.....	8
3.1 Definitions	8
3.2 Abbreviations	8
4 Introduction	9
5 Review of other security domain specifications.....	9
5.1 ISO/IEC 17799	9
6 ENUM Case study.....	9
6.1 Purpose	9
6.2 Overview of ENUM	9
6.3 Security and common criteria in ENUM.....	11
6.3.1 Privacy concerns	11
6.3.2 Security concerns	11
6.3.2.1 DNS security mechanisms	12
6.3.3 Security critical ENUM operations.....	13
6.3.3.1 Registration of an E.164 number in the ENUM database	13
6.3.3.2 Processes for creation, modification and deletion of NAPTR Records in the Tier 2 database	14
6.3.3.3 Processes for removal of E.164 numbers from ENUM databases.....	15
6.3.3.4 Processes for changing Registrars.....	16
6.3.4 ENUM assets	16
6.3.4.1 NAPTR records.....	16
6.3.4.2 ENUM query.....	17
6.3.5 Composite security model	17
6.4 CORAS method application in ENUM analysis	18
6.4.1 Introduction.....	18
6.4.2 CORAS platform and UML profile	18
6.4.3 The risk management process.....	21
6.4.4 The risk documentation framework.....	23
7 UML modelling.....	24
7.1 Introduction	24
7.2 Core security model.....	24
7.3 Development of stereotypes	26
7.4 Application of stereotypes.....	29
Annex A: UML modelling of ISO/IEC 15408-2.....	30
A.1 Introduction	30
A.2 Structure of the UML model	33
A.3 UML model for ISO/IEC 15408-2	34
A.3.1 TSF Package Dependency.....	34
A.3.2 Package TSF_FAU.....	35
A.3.3 Package TSF_FCO.....	45
A.3.4 Package TSF_FCS.....	50
A.3.5 Package TSF_FIA	76
A.3.6 Package TSF_FMT.....	86
A.3.7 Package TSF_FPR.....	96
A.3.8 Package TSF_FPT.....	103
A.3.9 Package TSF_FRU.....	124

A.3.10	Package TSF_FTA	130
A.3.11	Package TSF_FTP	139
History	144

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 Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document gathers together and presents information regarding the progress of work in the development of guidelines on the use of the Common Criteria for the evaluation of IT security (ISO/IEC 15408 [22]).

The purpose of the present document is to be a repository for information which is of interest but which has no clear place in the core guidance documents, thus:

- notes on information studied in order to prepare the core guidance documents:
 - method for application of Common Criteria to ETSI deliverables, EG 202 387 [1];
 - method and proforma for defining Protection Profiles, ES 202 382 [2];
 - method and proforma for defining Security Targets, ES 202 383 [3].
- notes on use of tools and tool development; and
- notes on the assistance given to TISPAN-WG4 on the ENUM privacy analysis.

2 References

For the purposes of this Technical Report (TR), the following references apply:

- [1] 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".
- [2] 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".
- [3] 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".
- [4] IETF RFC 3761 (2004): "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)".
- [5] ETSI TS 102 051: "ENUM administration in Europe".
- [6] ETSI TS 102 172: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Minimum requirements for interoperability of ENUM implementations".
- [7] IETF RFC 2915: "The Naming Authority Pointer (NAPTR) DNS Resource Record".
- [8] IETF STD 013: "Domain Names - Concepts And Facilities".
- [9] IETF RFC 2535: "Domain Name System Security Extensions".
- [10] ETSI TS 102 165-1: "Telecommunications and Internet Protocol Harmonization over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 1: Threat Analysis".
- [11] IETF RFC 1034 (1987): "Domain names - concepts and facilities".
- [12] IETF RFC 1035 (1987): "Domain names - implementation and specification".
- [13] Draft-ietf-dnsext-dns-threats-07 (2004): "Threat Analysis of the Domain Name System".

- [14] Draft-ietf-dnsext-dnssec-protocol-06 (2004): "Protocol Modifications for the DNS Security Extensions".
- [15] Draft-ietf-dnsext-dnssec-records-08 (2004): "Resource Records for DNS Security Extensions".
- [16] ITU-T Recommendation E.164 (1997): "The international public telecommunication numbering plan".
- [17] Draft-ietf-dnsext-dnssec-intro-11 (2004): "DNS Security Introduction and Requirements".
- [18] "DNSSEC: The Protocol, Deployment, and a Bit of Development" - The Internet Protocol Journal, Volume 7, Issue 2, June 2004.
- [19] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".
- [20] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements".
- [21] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance requirements".
- [22] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".
- [23] ISO/IEC 17799 (2000): "Information technology - Code of practice for information security management".

NOTE: BS 7799-1 contains the same information as ISO/IEC 17799.

- [24] BS 7799-2 (2002): Information security management systems - Specification with guidance for use".
- [25] CORAS (2003): "UML profile for security assessment", Mass Soldal Lund, Ida Hogganvik, Fredrik Seehusen, Ketil Stølen. SINTEF Telecom and Informatics (<http://coras.sourceforge.com>).
- [26] ETSI SR 002 211 (2004): "List of standards and/or specifications for electronic communications networks, services and associated facilities and services; in accordance with Article 17 of Directive 2002/21/EC".
- [27] ISO 9000 family: "Quality management systems", 2000, consisting of:
ISO 9000 (2000): "Quality management systems - Fundamentals and vocabulary"; and
ISO 9001 (2000): "Quality management systems - Requirements".
- [28] ISO/IEC Guide 2: "Standardization and related activities - Vocabulary"; and ISO/IEC DIS 17000: "Vocabulary for conformity assessment".

NOTE: ISO/IEC DIS 17000 is currently in the draft International Standard stage of development; it will replace some of the terminology defined in Guide 2.

- [29] OMG: "UML Profile for Modeling Quality of Service and Fault Tolerance Characteristics & Mechanisms".
- [30] ETSI TS 102 165-2: "Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON) Release 4; Protocol Framework Definition; Methods and Protocols for Security; Part 2: Counter Measures".
- [31] 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).
- [32] 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).

- [33] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
- [34] ISO/IEC 10746 (ODP-RM): "Information technology - Open Distributed Processing".
- [35] ETSI EN 300 396-6: " Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in the ISO/IEC Guide 2 [28] and the following apply:

accreditation: formal recognition by a specialized body - an accreditation body - that a certification body is competent to carry out ISO 9000 [27] certification in specified business sectors

certification: issuing of written assurance (the certificate) by an independent, external body that has audited an organization's management system and verified that it conforms to the requirements specified in the standard

registration: recording by an auditing body of a particular certification in its client register

3.2 Abbreviations

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

DNS	Domain Name System
DNSSEC	DNS Security extensions
EAL	Evaluation Assurance Level
ENUM	Electronic NUMbering
MBRA	Model-Based Risk Assessment
NAPTR	Naming Authority PointeR
NNPA	National Number Plan Administrator
PP	Protection Profile
PSTN	Public Switched Telephone Network
RR	Resource Record
RRSIG	Resource Record SIGnature
SIP	Session Initiation Protocol
TLD	Top Level Domain
TOE	Target of Evaluation
TSF	TOE Security Function
TSP	Telecommunications Service Provider
UDP	User Datagram Protocol
UML	Unified Modelling Language

4 Introduction

The present document gathers and presents information relating to the preparation of a set of ETSI deliverables on the application of the Common Criteria [22] to standardization.

- Clause 5 presents a review of public specifications relating to the management of security developments and how these relate to ETSI and to Common Criteria specifications.
- Clause 6 presents the results of a case study looking at a security analysis of ENUM. This clause also introduces and describes the results of applying the CORAS method to risk analysis and security requirements capture.
- Clause 7 presents the results of using UML in a security modelling environment.

5 Review of other security domain specifications

5.1 ISO/IEC 17799

There are many standards that lead to consistency in the quality of output from an undertaking. The most well known of these is probably the ISO-9000 [27] series which comprises standards and guidelines relating to quality management systems with related supporting standards on terminology and specific tools such as auditing (the process of checking that the management system conforms to the standard). In the ISO 9000 [27] context, the standardized definition of quality refers to all those features of a product (or service) which are required by the customer.

ISO/IEC 17799 [23] deals with quality for security. It is a "best practise" type of document which specifies what an organization should do to ensure that its products or services satisfy the customer's security requirements and comply with any applicable regulations. Due to the voluntary nature of standardization, the standards development process is unlikely ever to comply with ISO/IEC 17799 [23] whose requirements for personnel security (clause 6) in particular are almost impossible to meet in such an environment.

6 ENUM Case study

6.1 Purpose

The purpose of including a case study in the work of the preparation of a set of ETSI deliverables on the application of the Common Criteria [22] to standardization was to test and validate the guidance as it evolved in a "live" environment. A number of case studies were used in the development of the guidance. ES 202 382 [2] uses the TETRA Direct Mode Operation security specification (EN 300 396-6 [35]) as an example in building a Protection Profile from existing standards. The TIPHON threat analysis (ES 202 165-1 [10]) and countermeasure (ES 202 165-2 [30]) documents were examined in the development of guidance to the Vulnerability assurance evaluation class in EG 202 387 [1]. The use of ENUM as a case study was to examine the security analysis aspects of Common Criteria and in particular to determine how the guidance to the assurance classes of EG 202 387 [1] apply to a standard in development. In addition to this one of the tasks in the preparation of a set of ETSI deliverables on the application of the Common Criteria [22] to standardization was to evaluate the CORAS method and UML profile in the vulnerability analysis phase of security design. To this end a trial of the CORAS approach combined with the common criteria guidance has been applied to the security and privacy of ENUM. A summary of the CORAS method as it has been applied is given in clause 6.4.

6.2 Overview of ENUM

ENUM is an application of the Domain Name System (DNS) used to store and retrieve E.164 numbers [16] and is defined in RFC 3761 [4]. In the wider (non-DNS) environment the term ENUM is applied to both the definition of records and to the business process. In analysing ENUM therefore both business and technical assets have to be considered (see figure 1).

NOTE: The ENUM protocol is not owned or developed within ETSI so one further aspect of the ENUM case study is to consider the application of the guidance from DEG-7005 to 3rd party developments that are used within the ETSI domain.

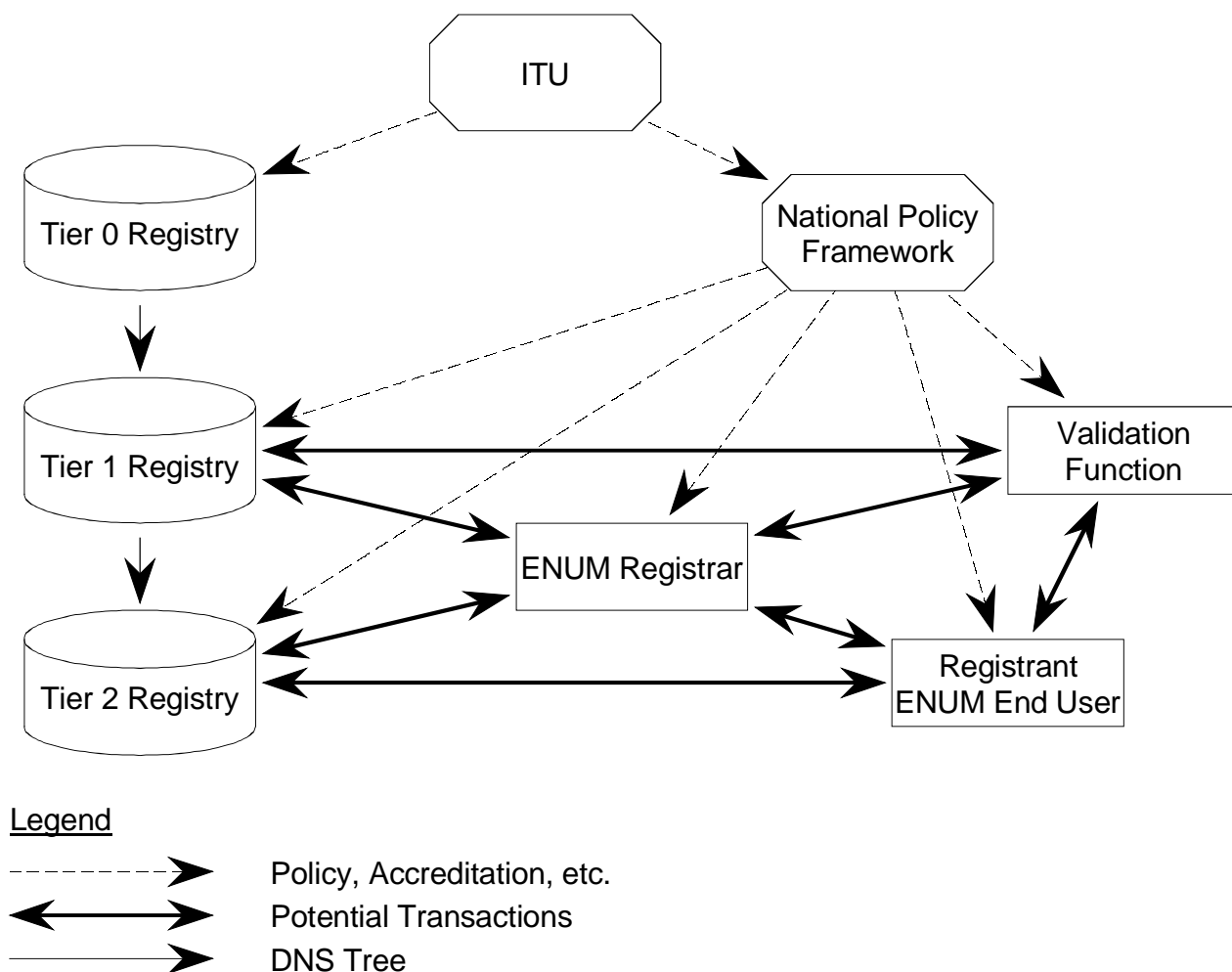


Figure 1: ENUM administration reference model

The ENUM information branches from the Top Level Domain (TLD) "arpa" (see figure 2) and the domain "e164.arpa" provides the infrastructure in DNS for storage of E.164 numbers.

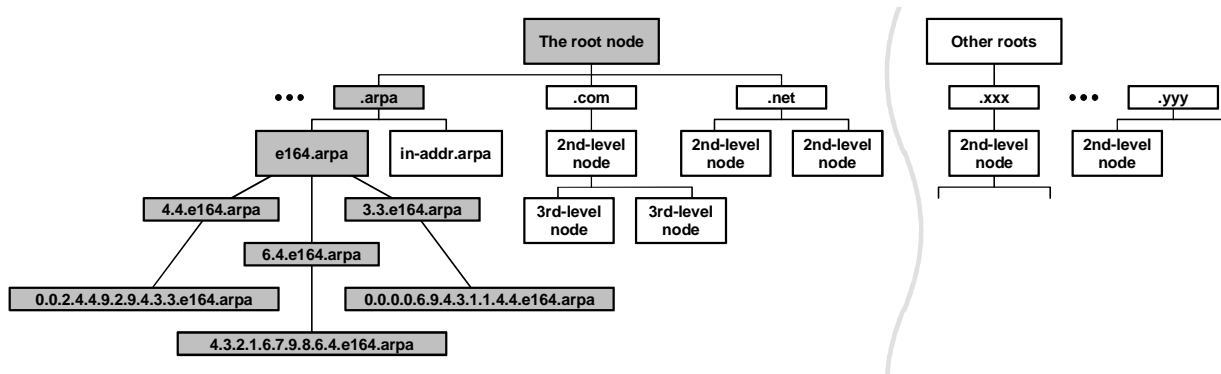


Figure 2: ENUM within the DNS structure

6.3 Security and common criteria in ENUM

6.3.1 Privacy concerns

ENUM as a service offers a number of modes of operation. One mode is to act as a directory service and there are constraints on the use of directory services identified by the European Union framework directive (2002/21/EC [31]) which contains the privacy directive (2002/58/EC [32]).

The Directive harmonizes the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

The Directive updates the previous Data Protection Directive (97/66/EC [33]) in the light of new technologies and ensures that the privacy rules that apply to phone and fax services also apply to e-mail and use of the Internet.

- *Subscriber directories - Subscribers will have a stronger right to decide whether they want to be listed in subscriber directories or not, and they must be given clear information about the directories in question, including any reverse search-type functions which allow directory users to identify names/addresses by searching against numbers rather than the other way round.*

All ENUM and DNS data are public and thus open for interrogation by appropriate protocols. As a result, it is impossible to make an absolute assurance of privacy although access to the data can be restricted and mechanisms to assure the integrity of data (i.e. that it has not been altered after submission) and the origin authentication (i.e. the assurance that the data stems from an authentic source) can be provided using DNSSEC and other similar protocols.

Organizations offering ENUM services have to comply with the constraints of the privacy directive.

Data maintained in DNS name servers, as part of the ENUM name space has to be protected from potential violations of the privacy directive. It has to be clear to the registrant what purpose the data is used for when entered into ENUM.

The name servers are open but the resolvers that access the name servers should be part of the trusted environment to ensure that data extracted from the name servers is used in a trusted manner.

6.3.2 Security concerns

Security measures are aimed at maintenance of each of confidentiality, integrity and availability of a system or service. The system security requirements may be classified in terms of each of confidentiality, integrity and availability, and the threats to the system may be classified as modifying one or more of the confidentiality, integrity and availability attributes.

- NOTE: Availability may be considered in terms of response time and therefore vary depending upon the application that is using ENUM. For example where ENUM is used to assist routing the ENUM service availability constraint may be set by the call establishment protocols. In contrast where ENUM is used as part of a user-directory service the availability constraints may be established by user interface metrics.

Table 1: Security concern classification from RFC 3761

CIA	Security concern	Attack form
Confidentiality	Packet interception	man-in-the-middle attacks eavesdropping on requests combined with spoofed responses
	ID guessing and query prediction	An attack based on ID guessing or query prediction relies on predicting the behaviour of a resolver. It is most likely to be successful when the victim is in a known state, whether because the victim rebooted recently, or because the victim's behaviour has been influenced by some other action by the attacker or because the victim is responding (in a predictable way) to a third party action known to the attacker.
	Masquerade	Masquerading is a type of attack in which one system entity poses illegitimately as another user or administrator.
	Eavesdropping	Reading and interpreting data flowing in either direction. An eavesdropper does not have to be able to spoof data.
Integrity	Spoofing	Modifying data flowing in either direction. Spoofing can lead to modified queries or to modified responses
	RR Presence denial	Removes complete resource records from a response.
	Cache Poisoning	feeding bad data into a victim's cache, thus potentially subverting subsequent decisions based on DNS names.
	Name Chaining	Modification of the RDATA portion of RRs that contain DNS names thus diverting the victim's queries to a fraudulent part of the DNS tree.
	DNS server perversion	This attack feeds illegitimate data into the DNS thus perverting (part of) the DNS. The DNS may then be configured to give back answers that are not in the best interest of the user.
	Loss of data integrity	This attack feeds any illegitimate data into the DNS.
	Name-based attacks	use of the actual DNS caching behaviour to insert bad data into a victim's cache.
	Betrayal By A Trusted Server	The placing of a malicious entry into the database to point to an unexpected URI.
	Authenticated denial of Domain Names	The placing of a malicious entry into the database to ensure that calls cannot be completed for the user.
Integrity and Availability	Administrator Action Repudiation	Removal of audit trails for administrator actions.
Availability	Denial of service	Use of DNS servers as denial of service amplifiers.
	Data Mining	A data mining attack attempts to derive as much data as possible from a database.
	Denial and Degradation of Service	This attack prevents or delays the authorized access to a system resource which should be accessible and usable upon demand by an authorized system entity, according to performance specifications for the system.

The public nature of the DNS service, and of ENUM as a profile of that service, suggest as shown in the above table that the most damaging attacks against ENUM (DNS) are those that attack the integrity of the data and the availability of the service. The attacks against confidentiality are less motivated as the data is already public.

6.3.2.1 DNS security mechanisms

The security mechanisms offered to DNS provide data origin authentication and data integrity by use of public key cryptography mechanisms.

When applying DNSSEC [14], [17], [15] to ENUM the smallest protected unit is a RRSet. Each resource record is digitally signed and a name server query returns both the RRSet and the signature for the set (this is contained in a RRSIG record). Checking of the RRSIG indicates both the integrity of the data contained in the RRSet and the source of the data; the origin authentication is based on a trusted root and a chain of trust by following pointers with proven integrity.

6.3.3 Security critical ENUM operations

There are a large number of ENUM operations identified that either provide protection or which require protection. These are summarized in the operation scenarios below.

6.3.3.1 Registration of an E.164 number in the ENUM database

This clause describes the process for registration of a new ENUM domain name in the ENUM Tier 2 Nameserver Provider and the delegation of the related zone in the Tier 1 Registry. The process is based on the assumption that the request of registration is initiated by the end user to which the E.164 number has been assigned or by a third party (agent) operating on behalf of the end user after its authorization. In the following the entity initiating the registration process (end user or agent) is referred to as the ENUM Registrant.

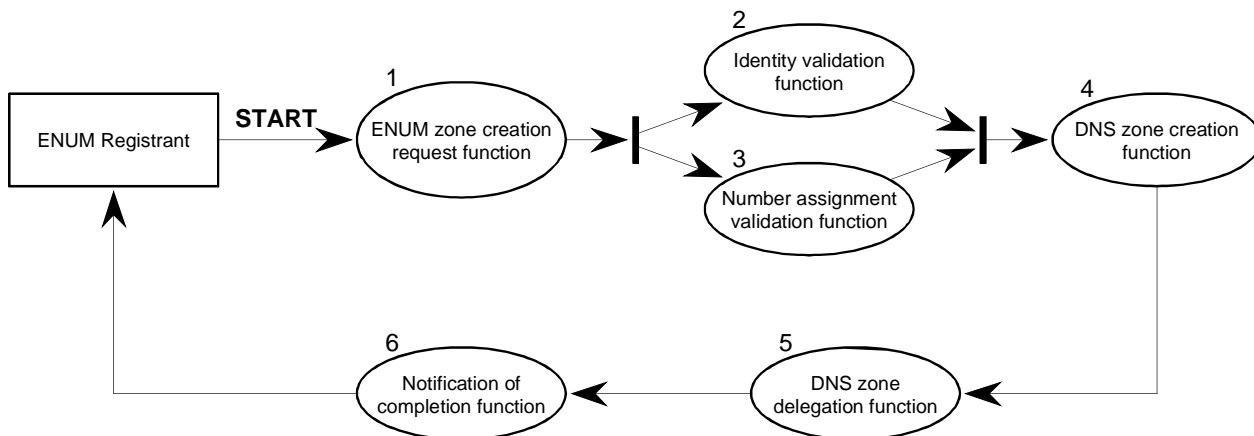


Figure 3: Functional model for Registration

Figure 3 represents a functional model and should not be considered as a business model as variants may exist.

As shown in figure 6, the following process takes place for the registration and provision of NAPTR records:

- 1) The **ENUM zone creation request** step involves receiving requests from an ENUM Registrant to create a DNS zone for his E.164 number.
- 2) The **identity validation** step involves confirming the identity of the ENUM Registrant and their authority to act on behalf of an end user.
- 3) The **number assignment validation** step involves confirming the assignment of the E.164 number to the ENUM end user.
- 4) **The DNS zone creation** step involves creation of a zone in the ENUM Tier 2 Nameserver Provider.
- 5) The **DNS zone delegation** step involves delegating DNS authority to the new zone by inserting the appropriate pointers in the Tier 1 Registry to the ENUM Tier 2 Nameserver Provider selected by the end user.
- 6) The **notification of completion** step involves informing the ENUM Registrant that the registration process has been successfully completed.

In the context of the Common Criteria the following functional components should therefore be introduced at step 2:

- FIA_UID.2: The user, in this case the ENUM registrant, is not allowed to perform any action prior to successful identification.

In addition it may be required to also introduce an authentication component as follows:

- FIA_UAU.2: The user, in this case the ENUM registrant, is not allowed to perform any action prior to successful authentication.
- FIA_UAU.3: The authentication procedure should ensure that forged or copied authentication data cannot be used.

6.3.3.2 Processes for creation, modification and deletion of NAPTR Records in the Tier 2 database

This clause describes the process for amendment of NAPTR Resource Records in the Tier 2 database. This could take the form of the creation, modification or deletion of a NAPTR or group of NAPTR records related to a specific E.164 number. A request for amendment is initiated by the ENUM end user or an agent acting on behalf of the ENUM end user (both referred to as the ENUM Registrant).

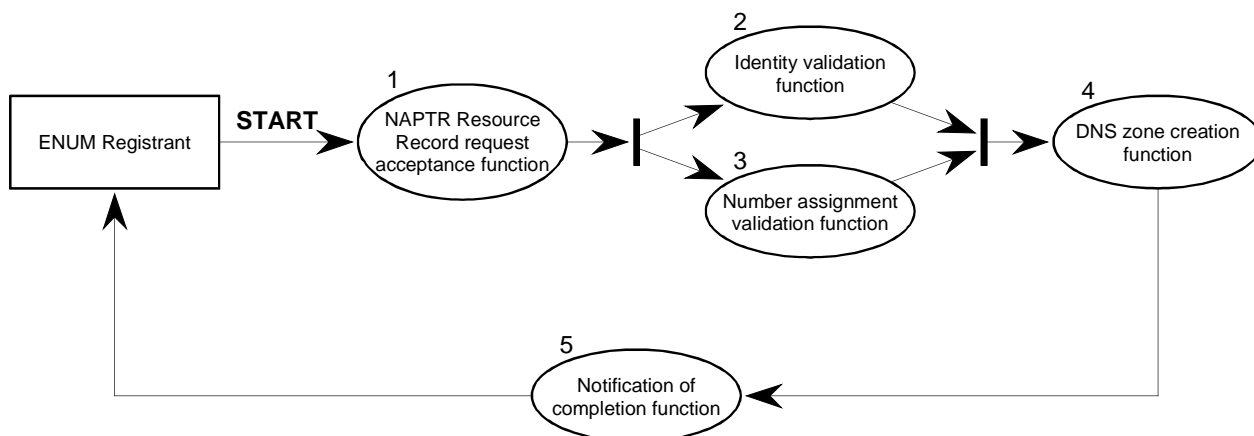


Figure 4: Functional model for amendment of NAPTR Resource Records in Tier 2 database

Figure 4 represents a functional model and should not be considered as a business model as variants may exist.

The following process takes place for the amendment of NAPTR Resource Records in the Tier 2 database:

- 1) The **NAPTR Resource Record request acceptance** step involves receiving requests from an ENUM Registrant to create, modify or delete a NAPTR Resource Record corresponding to the ENUM end user's E.164 number.
- 2) The **identity validation** step involves confirming:
 - the identity of an ENUM Registrant who is the ENUM end user; or
 - the identity of an ENUM Registrant who is not the ENUM end user and its authority to make a request on behalf of the ENUM end user.
- 3) The **number assignment validation** step involves confirming the assignment of the E.164 number to the ENUM end user.
- 4) The **DNS zone update** step involves updating ENUM service details corresponding to the ENUM end user's E.164 number in the DNS in the required format.
- 5) The **completion notification** step involves informing the ENUM Registrant that the amendment process has been successfully completed.

In the context of the Common Criteria the following functional components should therefore be introduced at step 2:

- FIA_UID.2: The user, in this case the ENUM registrant, is not allowed to perform any action prior to successful identification.

In addition it may be required to also introduce an authentication component as follows:

- FIA_UAU.2: The user, in this case the ENUM registrant, is not allowed to perform any action prior to successful authentication.
- FIA_UAU.3: The authentication procedure should ensure that forged or copied authentication data cannot be used.

6.3.3.3 Processes for removal of E.164 numbers from ENUM databases

This clause describes the process for removal of E.164 numbers and NAPTR Resource Records from ENUM databases. The process is based on the assumption that an ENUM end user should have information corresponding to its E.164 number in ENUM databases until:

- it no longer requires the services that are reliant on ENUM;
- it otherwise relinquishes the number or the number is withdrawn.

In the event of relinquishment or withdrawal of the number, it is important for NAPTR Resource Records corresponding to the number to be removed before any conflict is generated by use of the number by a new end user. In the case that the ENUM end user requires the removal of information relating to its E.164 number from ENUM databases, the ENUM end user or an agent acting on behalf of the ENUM end user (both referred to as the ENUM Registrant) initiates the removal request. In the case that the ENUM end user relinquishes the number or the number is withdrawn, it may be appropriate to allow the Assignment Entity to initiate the request to remove information relating to the E.164 number from ENUM databases, or to periodically verify that ENUM data corresponding to an end user's E.164 number should continue to be maintained.

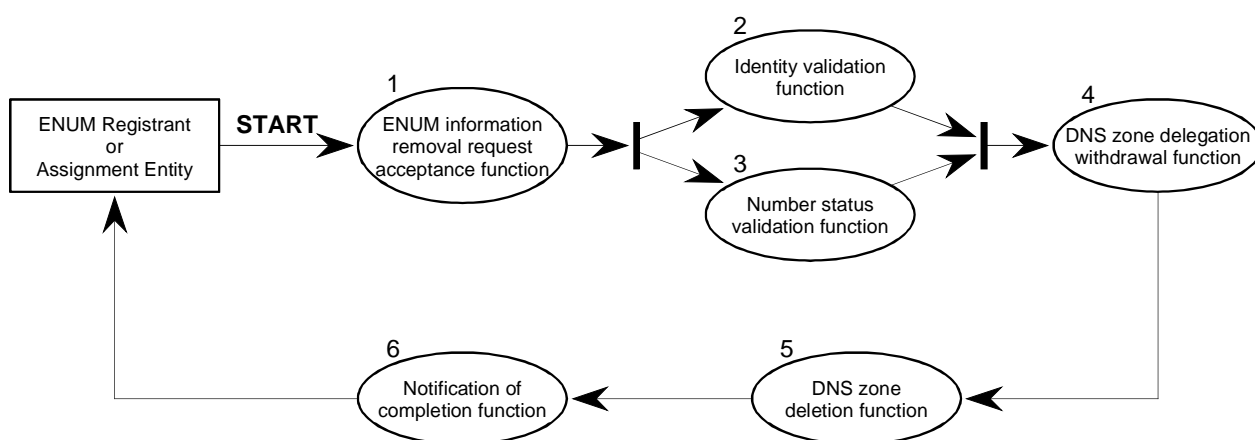


Figure 5: Functional model for removal of E.164 numbers from ENUM databases

Figure 5 represents a functional model and should not be considered as a business model as variants may exist.

The following process takes place for the removal of E.164 numbers and NAPTR Resource Records from ENUM databases:

- 1) The **ENUM information removal request acceptance** step involves accepting requests from an ENUM Registrant (either an end user or an agent acting on behalf of an end user) or an Assignment Entity to remove information relating to an E.164 number from ENUM databases.
- 2) The **identity validation** step involves confirming:
 - the identity of an ENUM Registrant who is the ENUM end user; or
 - the identity of an ENUM Registrant who is not the ENUM end user and its authority to make a request on behalf of the ENUM end user; or
 - the identity of an Assignment Entity and its authority to make a request in relation to a particular E.164 number.
- 3) The **number status validation** step involves confirming that the E.164 number is assigned to the ENUM end user or, prior to its relinquishment or withdrawal, was assigned to the ENUM end user.
- 4) The **DNS zone delegation withdrawal** step involves withdrawing the delegation of DNS authority to the zone corresponding to an E.164 number by removing the pointers to the URI corresponding to the number.
- 5) The **DNS zone deletion** step involves deleting ENUM information relating to an E.164 number from the DNS.

- 6) The **notification of completion** step involves informing the originator of the removal request that the removal process has been successfully completed.

In the context of the Common Criteria the following functional components should therefore be introduced at step 2:

- FIA_UID.2: The user, in this case the ENUM registrant, is not allowed to perform any action prior to successful identification.

In addition it may be required to also introduce an authentication component as follows:

- FIA_UAU.2: The user, in this case the ENUM registrant, is not allowed to perform any action prior to successful authentication.
- FIA_UAU.3: The authentication procedure should ensure that forged or copied authentication data cannot be used.

6.3.3.4 Processes for changing Registrars

Requirements and procedures should exist to enable an ENUM Registrant to change the Registrar responsible for registration of the domain and creation of the NAPTR records corresponding to an E.164 number. These requirements and procedures should support change of Registrar in such a way that no interruption in an ENUM end user's use of the domain name and NAPTR records.

Where requirements and procedures for change of Registrar exist in a country in respect of normal Internet domain name registrations, these requirements and procedures should be checked to establish whether they meet the additional requirements that apply when an ENUM Registrar changes. Where no such requirements and procedures exist in a country the following points should be considered:

- an ENUM end user should be able to change Registrar at any time;
- an ENUM end user with domain name registrations and NAPTR records for more than one E.164 number should be able to change Registrar in respect of all or some of the numbers;
- a request to change Registrar should be made by an ENUM Registrant to its selected new Registrar;
- the new Registrar should validate the identity of the ENUM Registrant and, if the latter is not the ENUM end user, verifies its authority to act on behalf of the ENUM end user;
- the new Registrar should verify that the E.164 number is assigned to the ENUM end user;
- the new Registrar should notify the Tier 1 Registry and ENUM Tier 2 Nameserver Provider and the old Registrar of the intention of the ENUM Registrant to change Registrar;
- within a specified time, the Tier 1 Registry and ENUM Tier 2 Nameserver Provider should amend their Registrant information to identify the new Registrar as the Registrar of record for the particular ENUM Registrant, and notify the old and new Registrars of the amendments. It is the prime responsibility of the Tier 1 Registry to supervise the proper completion of the process; and
- in the case that an unauthorized change of Registrar occurs, the ENUM Tier 2 Nameserver Provider should reverse the amendment of its Registrant information within a specified time.

6.3.4 ENUM assets

6.3.4.1 NAPTR records

As described in RFC 2915 [7] in the text of example 3 in clause 7.3 the ENUM application uses a NAPTR record to map an e.164 telephone number to a URI.

EXAMPLE 1: The E.164 phone number "+1-770-555-1212" when converted to a domain-name would be "2.1.2.1.5.5.0.7.7.1.e164.arpa."

When an ENUM (DNS) query is executed against this number the following records may be returned:

```
EXAMPLE 2: $ORIGIN 2.1.2.1.5.5.0.7.7.1.e164.arpa.
IN NAPTR 100 10 "u" "sip+E2U" "!^.*$!sip:information@tele2.se!"
IN NAPTR 102 10 "u" "mailto+E2U" "!^.*$!mailto:information@tele2.se!"
```

The returned resource record set contains the information needed to contact that telephone service. The example above states that the available protocols used to access that telephone's service are either the Session Initiation Protocol or SMTP mail.

The NAPTR record is an asset of the ENUM system. The principal attack against ENUM is to the integrity of the NAPTR records. In the context of the Common Criteria the following functional components should therefore be introduced:

- FDP_SDI.1: The stored data is continually monitored to detect errors in its integrity.
- FDP_SDI.2: This extends FDP_SDI.1 by allowing predefined actions to be taken in the event of errors being found.

The provisions in DNSSEC offer some support to each of these capabilities.

6.3.4.2 ENUM query

The purpose of an ENUM query is to return the NAPTR records held against the E164 number. In the context of the Common Criteria the following functional components should therefore be introduced:

- FDP_UIT.1: The data that is transferred is monitored to detect errors in its integrity.
- FDP_UIT.2: This extends FDP_UIT.1 by allowing predefined actions to be taken in the event of errors being found using assistance from the source (i.e. the error is reported to the source and both source and destination take part in the corrective action).
- FDP_UIT.3: This extends FDP_UIT.2 by allowing predefined actions to be taken in the event of errors being found without using assistance from the source (i.e. the corrective action takes place only at the receiver).

The provisions in DNSSEC offer some support to each of these capabilities.

6.3.5 Composite security model

A picture of the ENUM security model can be drawn using UML as in figure 6.

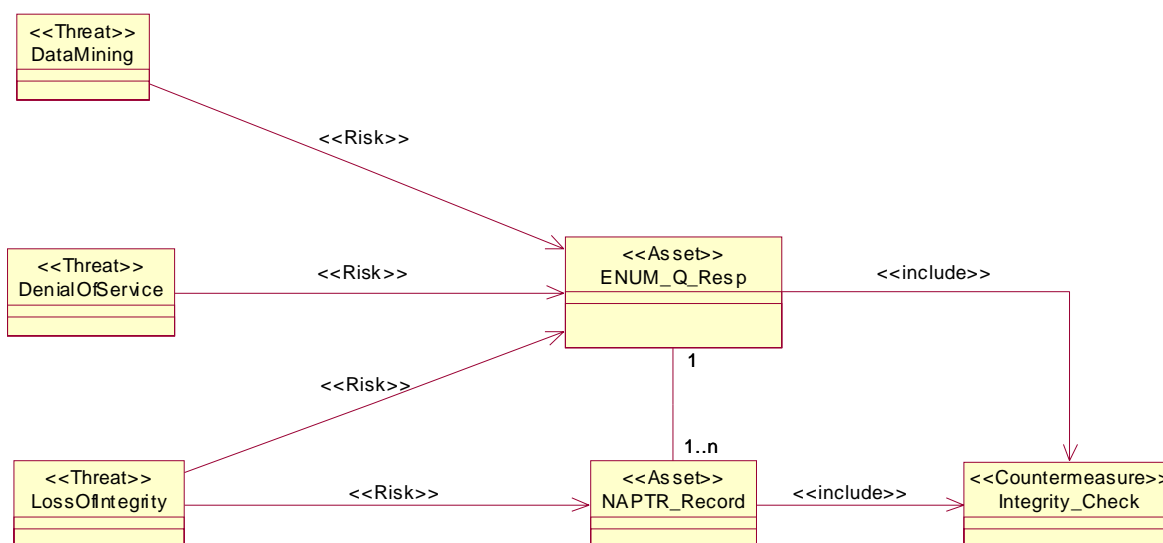


Figure 6: ENUM model showing threats, risks and assets

6.4 CORAS method application in ENUM analysis

6.4.1 Introduction

The EU-funded CORAS project (IST-2000-25031) has produced a framework for Model-Based Risk Assessment (MBRA) of security-critical systems. This framework is characterized by:

- 1) A careful integration of techniques and features from partly complementary risk assessment methods.
- 2) Patterns and methodology for UML oriented modelling targeting the different risk assessment methods.
- 3) A risk management process.
- 4) A risk documentation framework.
- 5) An integrated risk management and system development process.
- 6) A platform for tool-inclusion.

For the case study the risk management process and the risk documentation framework have been selected to test their applicability in the development of ETSI standards. Item 1 in the list has no relevance to ETSI (it describes the rationale for CORAS), item 2 in the list is addressed by ETSI in a different manner, items 5 and 6 have not been addressed by ETSI in this case study.

6.4.2 CORAS platform and UML profile

In the context of MBRA the CORAS project has developed a modelling platform that builds a database of the analysis results that may be supplemented by UML diagrams for illustration. The CORAS platform has not been used by ETSI in the analysis phase although the UML stereotypes have been modelled into a single CORAS-Analysis package for potential future use. Figure 7 identifies the structure of the UML profile developed in the CORAS project and published by the Object Management Group [29].

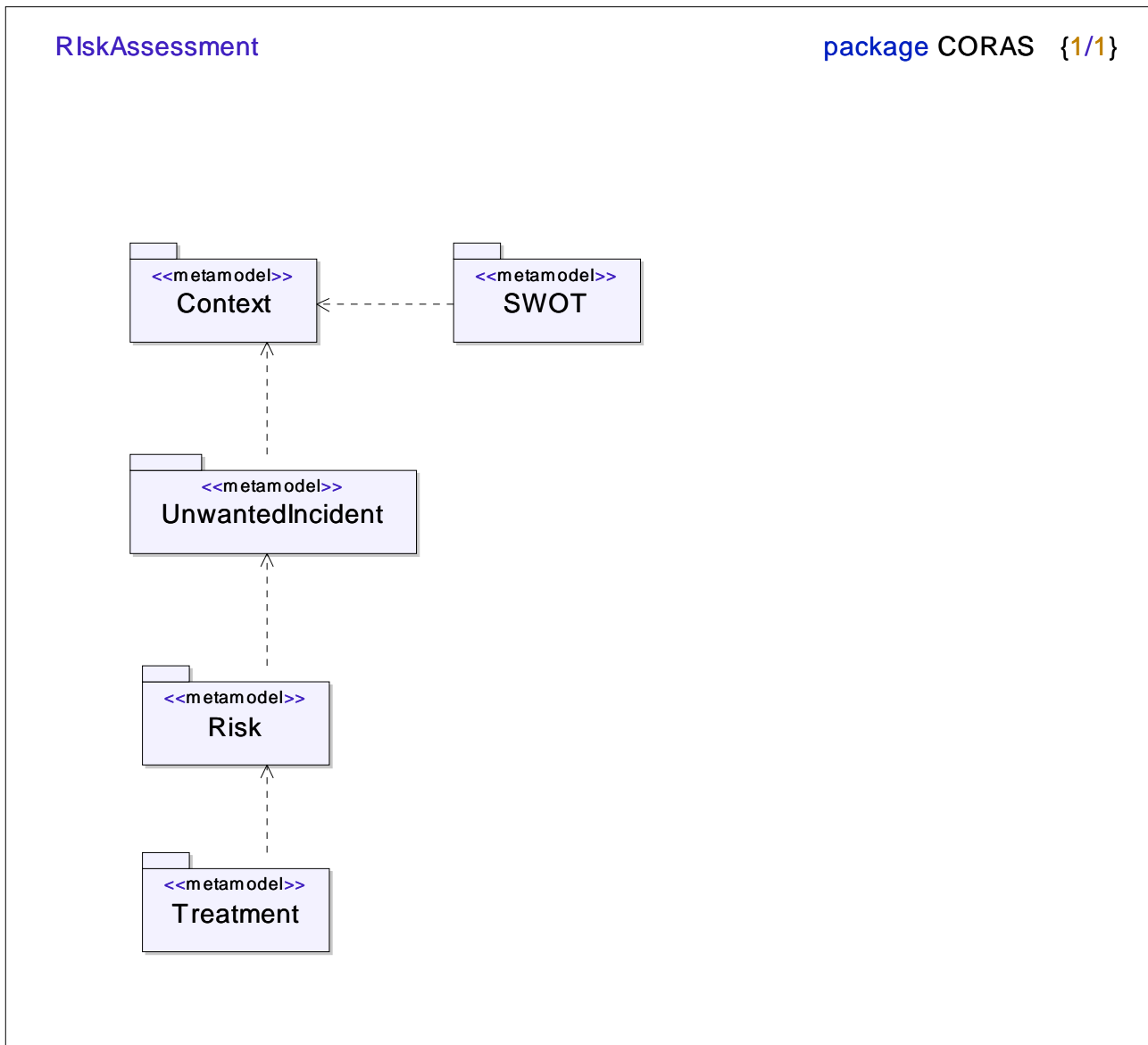


Figure 7: The CORAS risk assessment model

The CORAS UML packages show clear dependencies between each other and suggest a "waterfall" development model although that may not be the intention. The stereotypes developed in [29] and shown (for the use case extensions) in figure 8 have graphical constructs (see table 2).

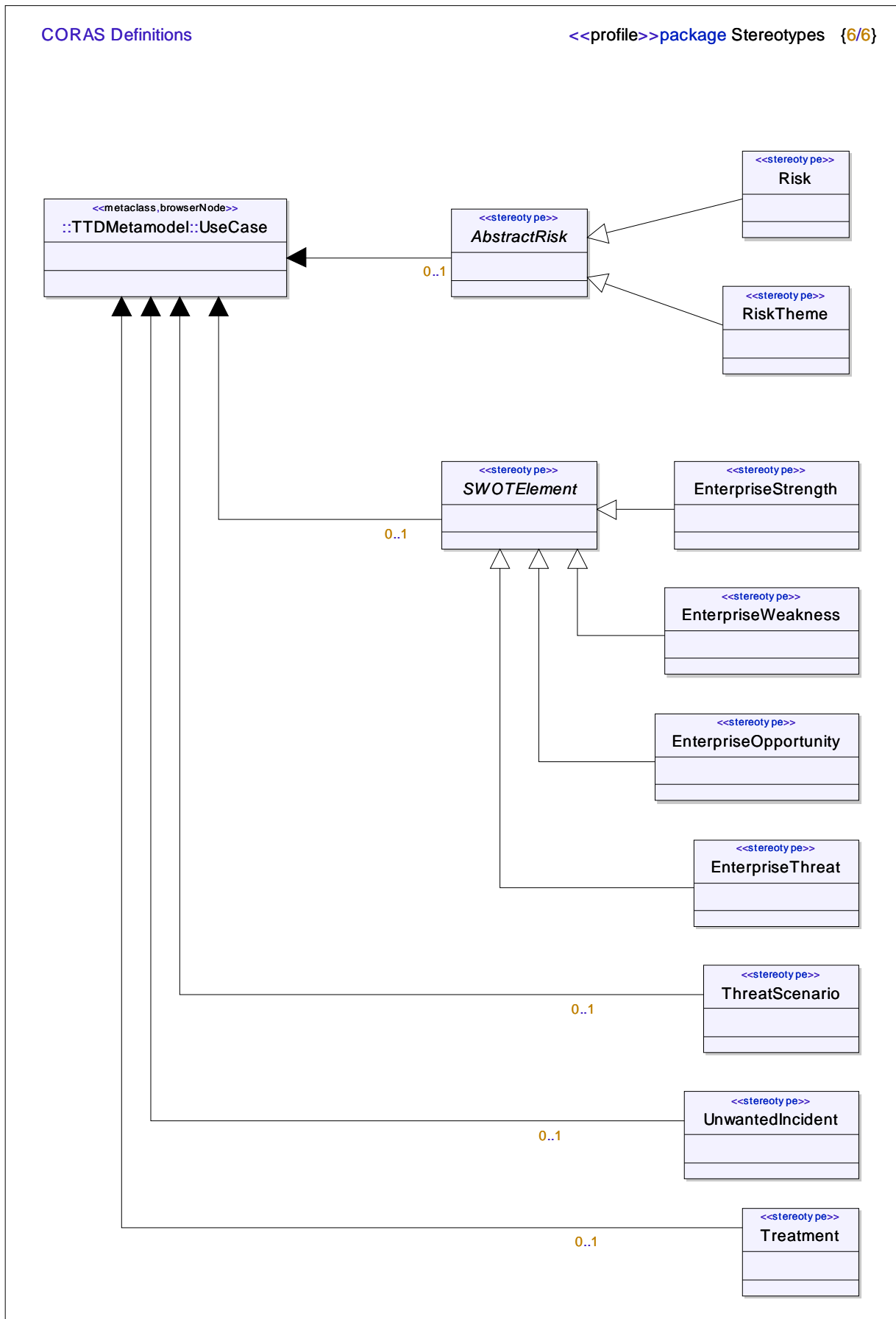
















Figure 8: Use case based stereotypes from CORAS

Table 2: CORAS stereotype graphical form

<<Asset>>		<<Stakeholder>>	
<<EnterpriseAsset>>		<<EnterpriseStrength>>	
<<EnterpriseWeakness>>		<<EnterpriseOpportunity>>	
<<EnterpriseThreat>>		<<ThreatAgent>>	
<<ThreatScenario>>		<<UnwantedIncident>>	
<<Risk>>		<<RiskTheme>>	
<<Treatment>>		<<TreatmentEffect>>	

NOTE: The CORAS project proposed an additional set of graphical stereotypes for different forms of threat agent (zombie, Trojan horse, logic bomb and so forth) which have not been incorporated to the published UML profile.

6.4.3 The risk management process

The CORAS risk management offers a decomposition of a risk management process and is shown graphically in figure 9.

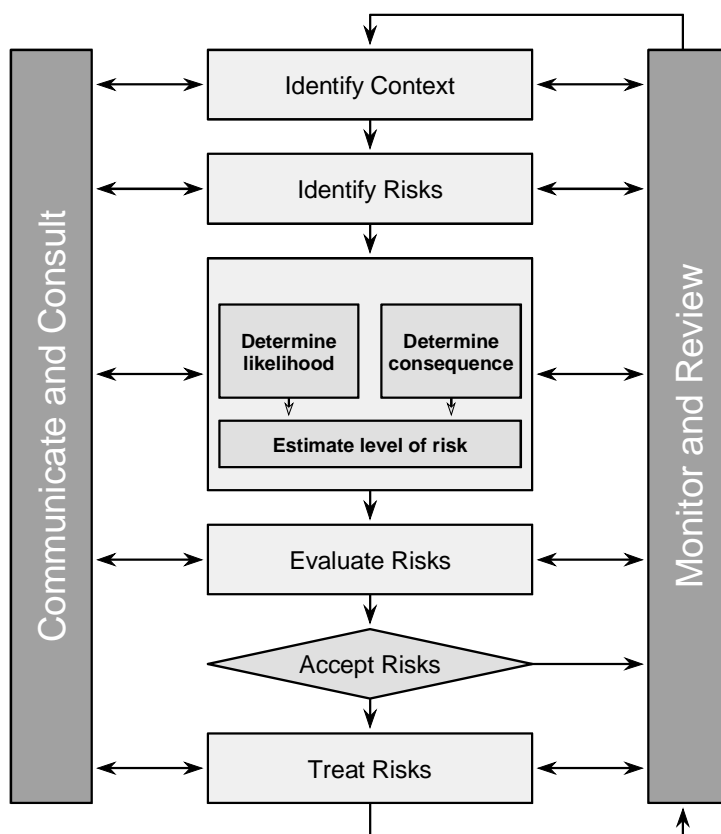


Figure 9: CORAS risk management process

The main notions in CORAS risk management process are as follows:

- Risk management: The culture, processes and structures that are directed towards effective management of potential opportunities and adverse effects.
- Risk management process: The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.
- Risk identification: The process of determining what can happen, why and how.
- Risk assessment: The overall process of risk analysis and risk evaluation.
- Risk analysis: A systematic use of available information to determine how often specified events may occur and the magnitude of their consequences.
- Risk evaluation: The process used to determine risk management priorities by comparing the level of risk against predetermined standards, target risk levels or other criteria.
- Risk treatment: Selection and implementation of appropriate options for dealing with risk.

Many of the features of the CORAS risk management process are aligned with the requirements tested in the Common Criteria evaluation class "Vulnerability assessment" and the guidance given in clause 6.8 of EG 202 387 [1].

6.4.4 The risk documentation framework

The CORAS risk documentation framework is a specialization of the Reference Model for Open Distributed Processing ISO/IEC 10746 (ODP-RM) [34]. ODP-RM is an ISO standardized reference model for distributed systems architecture, based on object-oriented techniques. ODP-RM divides the system documentation into five viewpoints as described below and illustrated in figure 10.

The five viewpoints are:

- the enterprise viewpoint: a viewpoint on the system and its environment that focuses on the purpose, scope and policies for the system;
- the information viewpoint: a viewpoint on the system and its environment that focuses on the semantics of the information and information processing performed;
- the computational viewpoint: a viewpoint on the system and its environment that enables distribution through functional decomposition of the system into objects which interact at interfaces;
- the engineering viewpoint: a viewpoint on the system and its environment that focuses on the mechanisms and functions required to support distributed interaction between objects in the system; and
- the technology viewpoint: a viewpoint on the system and its environment that focuses on the choice of technology in that system.

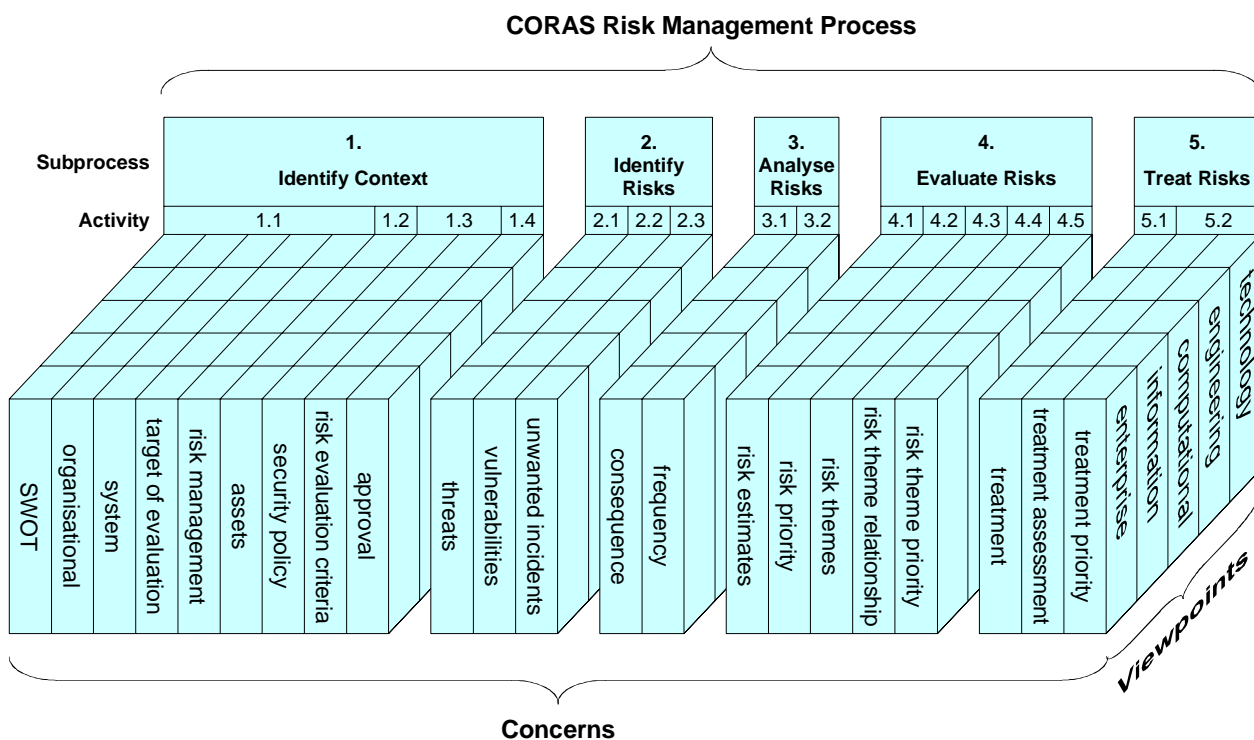


Figure 10: The CORAS risk documentation framework

7 UML modelling

7.1 Introduction

Modelling in support of illustration and development of standards is well established, and has been applied to communications standards development for a number of years. It has been less well applied to topics such as vulnerability analysis and security design. The CORAS project started to look into the use of UML for the purpose of model based risk analysis (see clause 6) by defining some UML stereotypes for use in visual modelling. This clause looks at some options for modelling using UML by defining stereotypes for the key elements in a vulnerability analysis and the relationships between them.

To get hands-on experience with Telelogic's tool TAU G2 - a state-of-the-art UML 2.0-based tool (that has been used to draw the diagrams in this clause) - and to get familiar with the classes and their families specified in the Common Criteria ISO/IEC 15408-2 [20], a formal model was developed. This model is shown in annex A.

7.2 Core security model

The core system and security model can be represented in UML as in figure 11. This shows that a system, represented by the class `SystemDesign`, is composed of a set of assets, represented by the class `SystemComponent`. The model also shows that the system is dependent upon the system objectives which are themselves a composition of both the security objectives and the evaluation objectives. Each system asset may have an associated vulnerability with a weighted risk dependency between the vulnerability and the asset. A vulnerability is modelled as existing only if both a weakness and a threat exist.

The model also shows a treatment of requirements where the System Requirements are a composition of Security requirements and assurance requirements which are all dependent on the respective objectives.

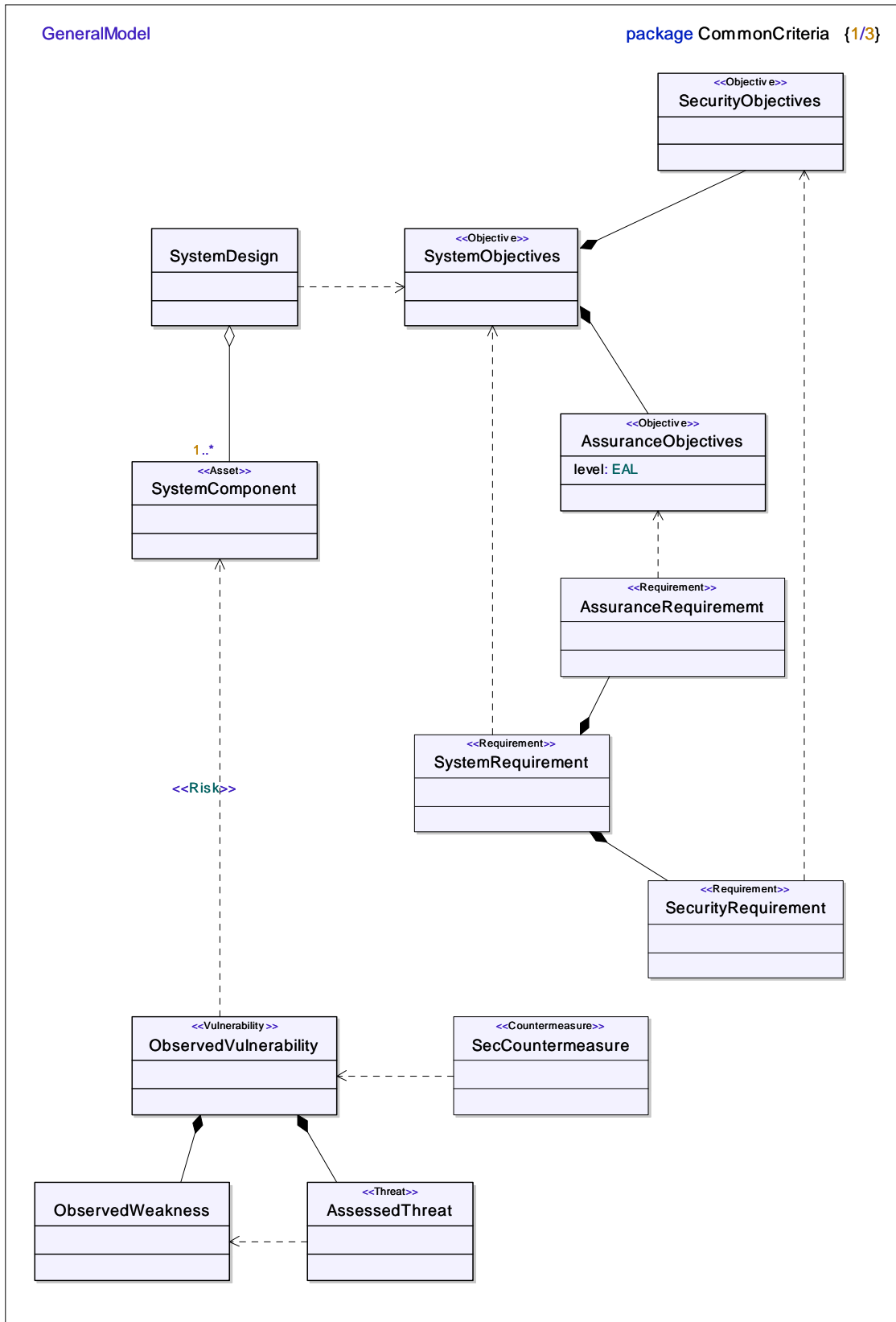


Figure 11: UML model of generic system security design

7.3 Development of stereotypes

The model presented in figure 11 contains a number of UML Stereotypes. The purpose of the stereotypes is to group objects of similar type together with constraints and attributes that have to exist for all elements of the class type.

The following stereotypes have been defined and used in the generic model of figure 11 and in the ENUM analysis work (see table 3).

Table 3: Stereotype definitions

Stereotype name	Base class	Required attributes	Constraints
Threat	Class	Threat type	
Asset	Class		
Weakness	Class		
Vulnerability	Class		
Countermeasure	Class		
Requirement	Class		
Objective	Class		
Risk	Dependency	Impact Likelihood	$RiskProduct = Impact * Likelihood$

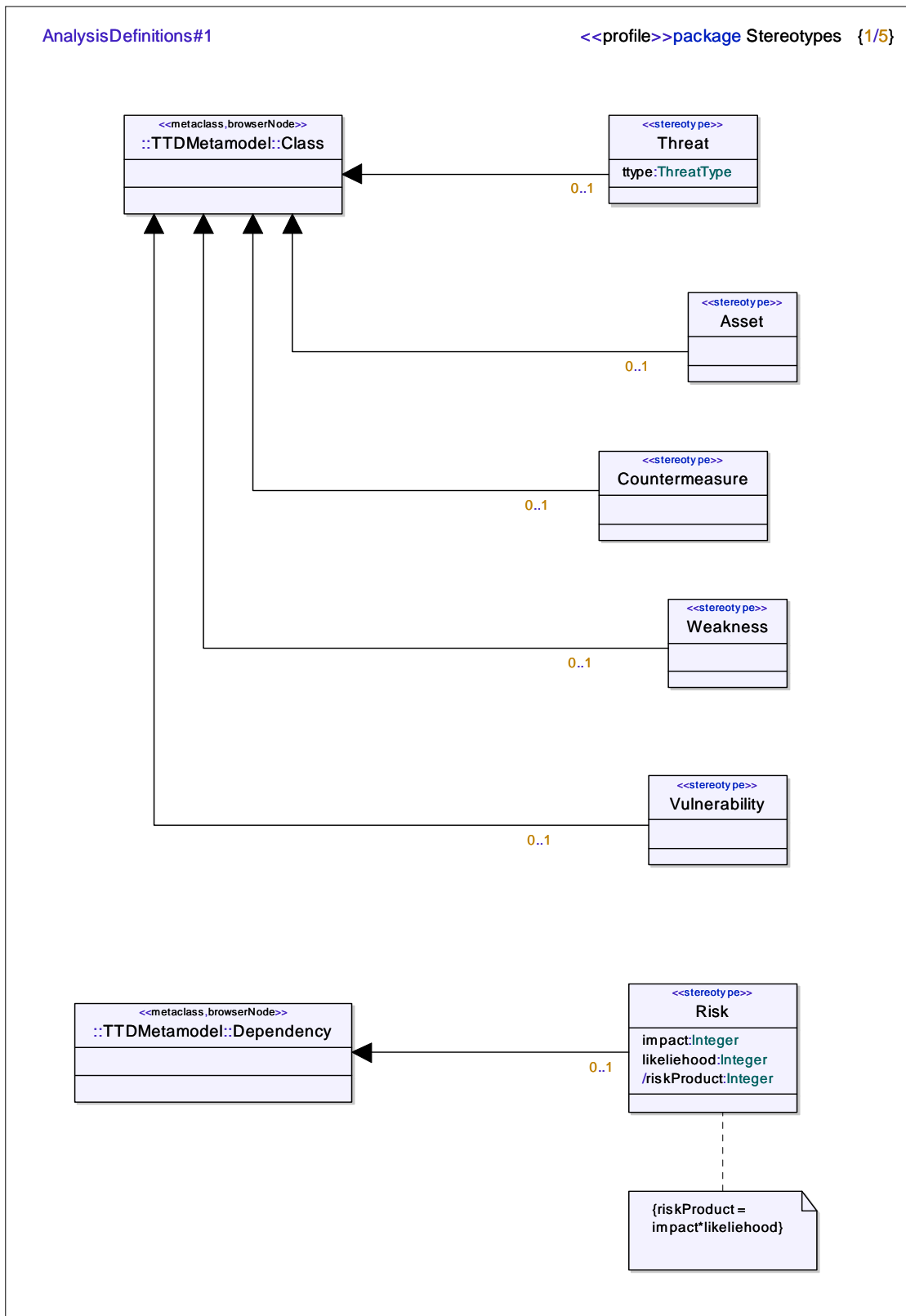


Figure 12: Stereotypes defined for security analysis and development (sheet 1 of 2)

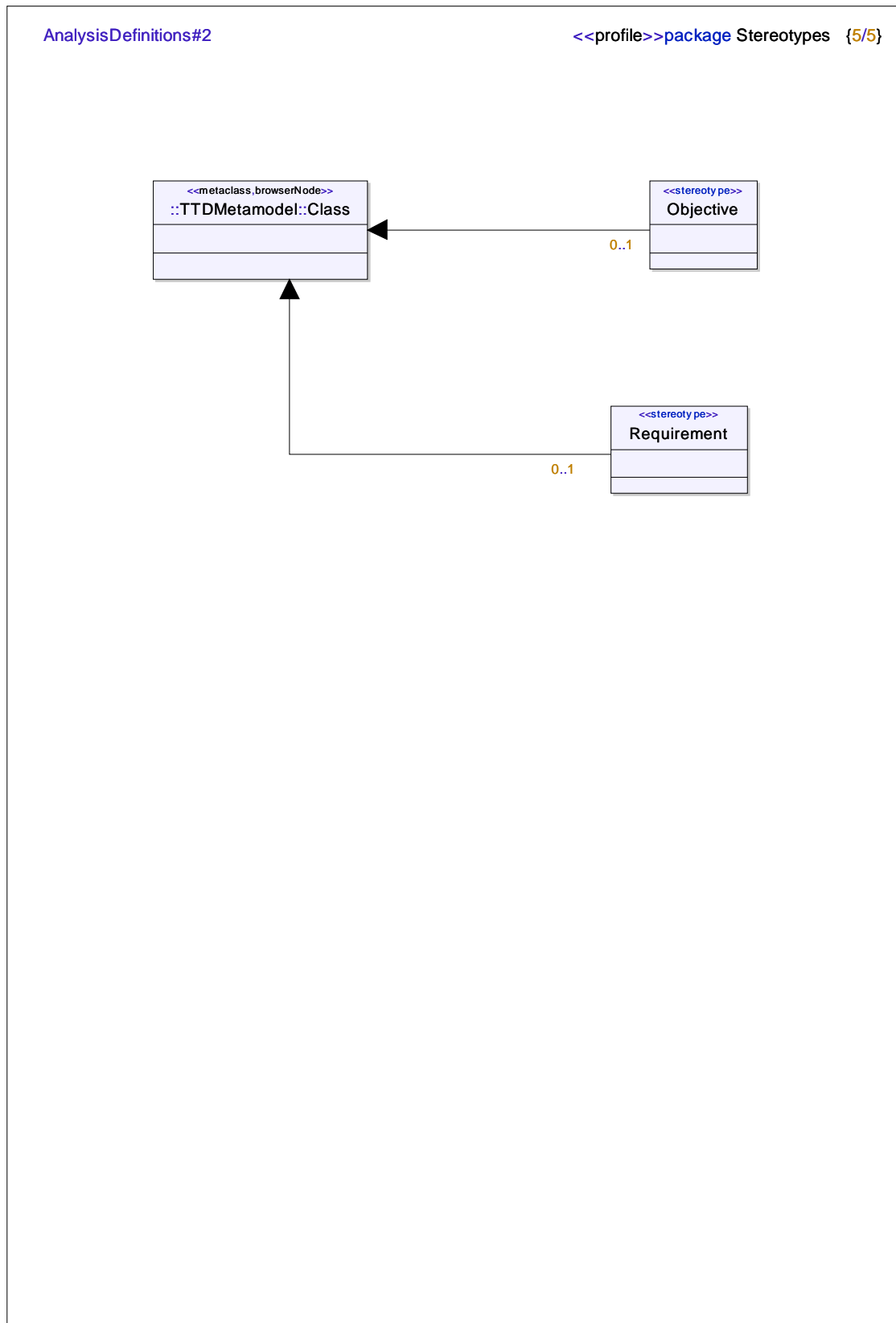


Figure 13: Stereotypes defined for security analysis and development (sheet 2 of 2)

7.4 Application of stereotypes

The stereotypes identified above can be applied to real systems (ENUM) as below:

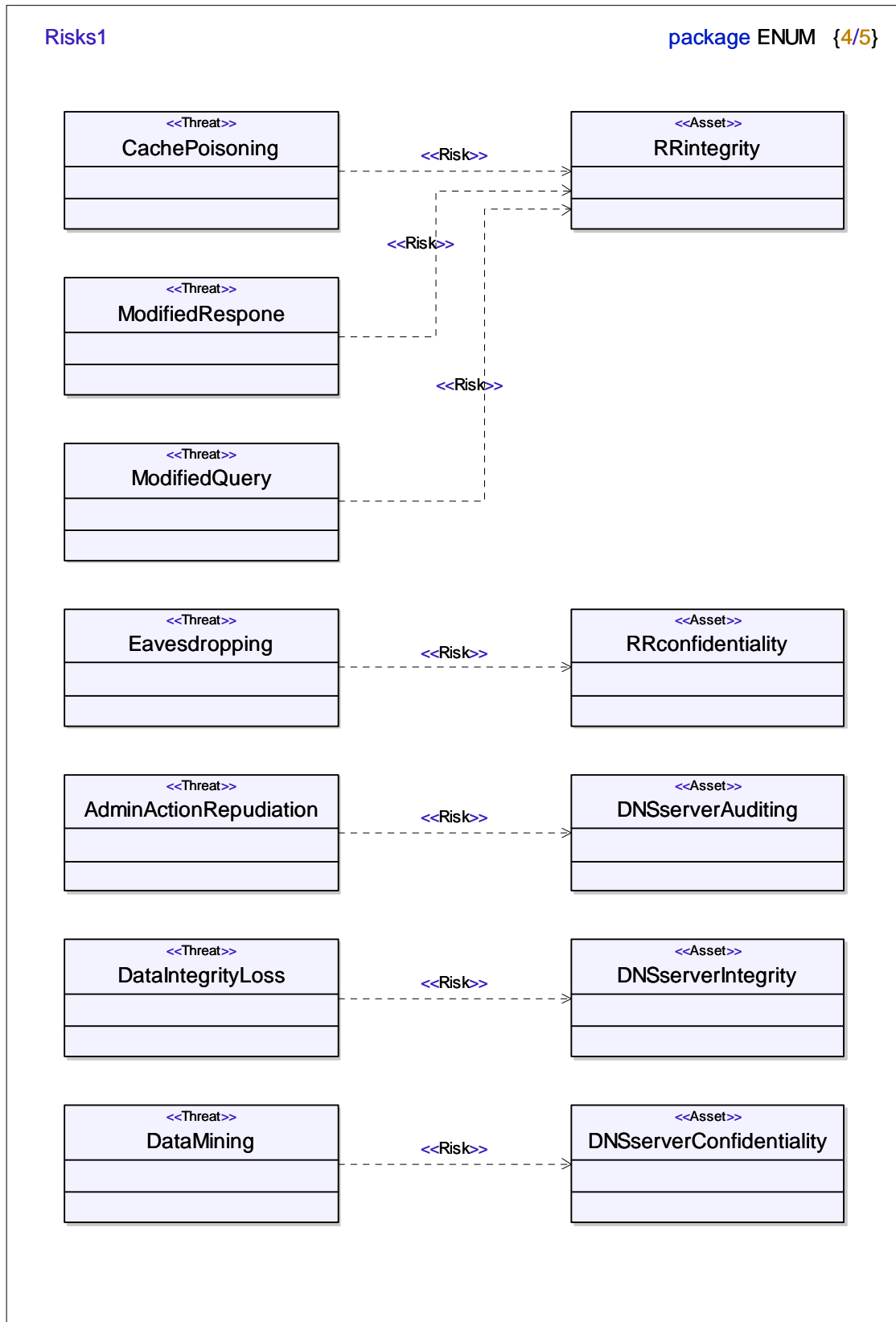


Figure 14: Application of stereotypes in ENUM analysis

Annex A: UML modelling of ISO/IEC 15408-2

A.1 Introduction

To gain experience in the development of formal security modelling and to become familiar with the classes and their families specified in ISO/IEC 15408-2 [20], a UML model of the classes, families and their components was developed using Teleogic's Tau G2 software tool.

The model shows the composition of the classes consisting of all families and the composition of the families consisting of the components, the audit functions, and the management functions. Extensive use has been made of the "stereotype" mechanism of the language.

NOTE: For obvious reasons "Class" is a reserved name in UML, hence, the stereotype "TSF" (Target Security Function) has been used for the classes of ISO/IEC 15408-2 [20].

Table A.1 summarizes the classes (TSFs) and their families.

Table A.1: ISO/IEC 15408-2 classes and families

Class	Class members
FAU Security audit	FAU_ARP Security audit automatic response FAU_GEN Security audit data generation FAU_SAA Security audit analysis FAU_SAR Security audit review FAU_SEL Security audit event selection FAU_STG Security audit event storage
FCO Communication	FCO_NRO Non-repudiation of origin FCO_NRR Non-repudiation of receipt
FCS Cryptographic support	FCS_CKM Cryptographic key management FCS_COP Cryptographic operation
FDP User Data Protection	FDP_ACC Access control policy FDP_ACF Access control functions FDP_DAU Data authentication FDP_ETC Export to outside TSF control FDP_IFC Information flow control policy FDP_IFF Information flow control functions FDP_ITC Import from outside TSF control FDP_ITT Internal TOE transfer FDP_RIP Residual information protection FDP_ROL Rollback FDP_SDI Stored data integrity FDP_UCT Inter-TSF user data confidentiality transfer protection FDP_UIT Inter-TSF user data integrity transfer protection
FIA Identification and authentication	FIA_AFL Authentication failures FIA_ATD User attribute definition FIA_SOS Specification of secrets FIA_UAU User authentication FIA_UID User identification FIA_USB User-subject binding
FMT Security management	FMT_MOF Management of functions in TSF FMT_MSA Management of security attributes FMT_MTD Management of TSF data FMT_REV Revocation FMT_SAE Security attribute expiration FMT_SMR Security management roles
FPR Privacy	FPR_ANO Anonymity FPR_PSE Pseudonymity FPR_UNL Unlinkability FPR_UNO Unobservability
FPT Protection of the TSF	FPT_AMT Underlying abstract machine test FPT_FLS Fail secure FPT_ITA Availability of exported TSF data FPT_ITC Confidentiality of exported TSF data FPT_ITI Integrity of exported TSF data FPT_ITT Internal TOE TSF data transfer FPT_PHP TSF physical protection FPT_RCV Trusted recovery Protection of the TSF FPT_RPL Replay detection FPT_RVM Reference mediation FPT_SEP Domain separation FPT_SSP State synchrony protocol FPT_STM Time stamps FPT_TDC Inter-TSF TSF data consistency FPT_TRC Internal TOE TSF data replication consistency FPT_TST TSF self test
FRU Resource Utilization	FRU_FLT Fault tolerance FRU_PRS Priority of service FRU_RSA Resource allocation

Class	Class members	
FTA TOE Access	FTA_LSA	Limitation on scope of selectable attributes
	FTA_MCS	Limitation on multiple concurrent sessions
	FTA_SSL	Session locking
	FTA_TAB	TOE access banners
	FTA_TAH	TOE access history
	FTA_TSE	TOE session establishment
FTP Trusted path/channels	FTP_ITC	Inter-TSF trusted channel
	FTP_TRP	Trusted path

Many of the classes are dependent upon each other. A summary of the dependencies is illustrated in figure A.1. The grey arrows show implicit dependencies, as all classes need some management and audit capabilities; the black arrows indicate explicit dependencies.

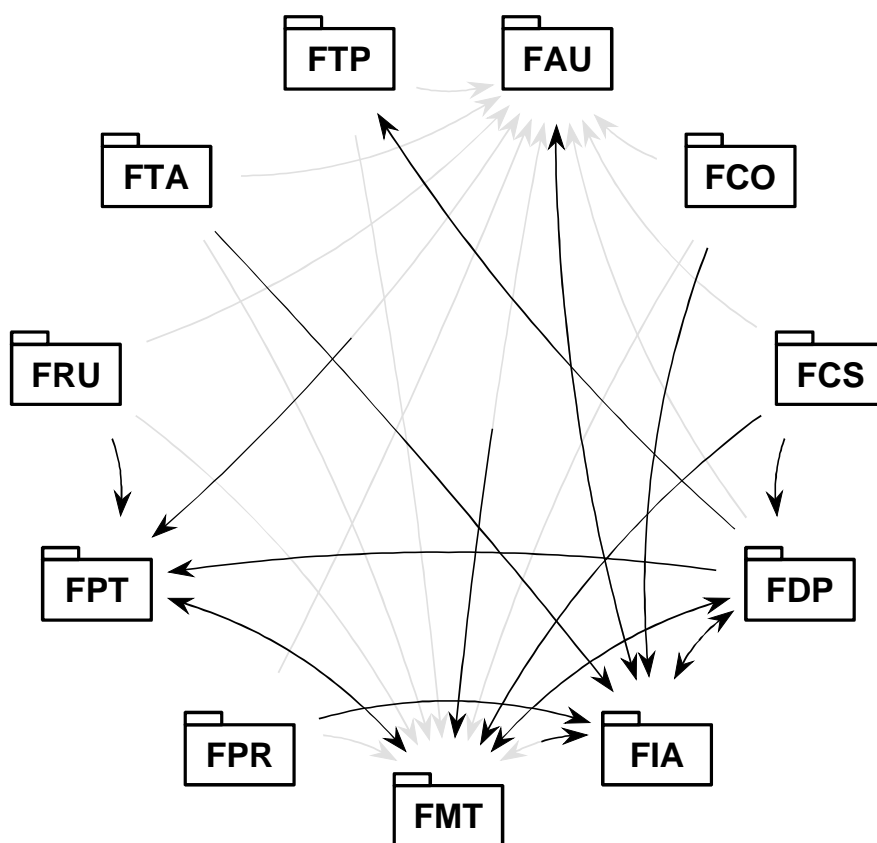


Figure A.1: Dependency for the classes in ISO/IEC 15408-2

A.2 Structure of the UML model

Figure A.2 shows the structure of the UML model for the security functional requirement classes of the Common Criteria described in ISO/IEC 15408-2 [20].

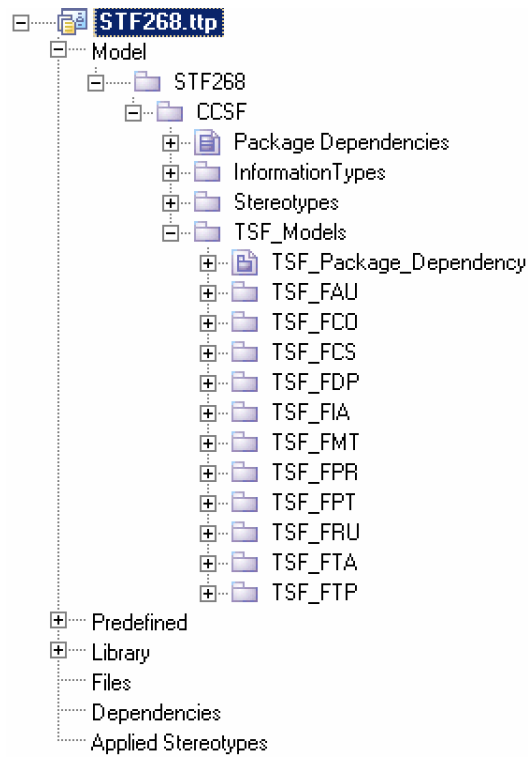


Figure A.2: The UML model

The Package Dependencies are shown in figure A.3. It indicates that the TSF Packages depend on both the stereotypes and the information types; the stereotypes itself depend on the information types.

NOTE: Neither the stereotype definition nor the definition of the information types are shown in the present document.

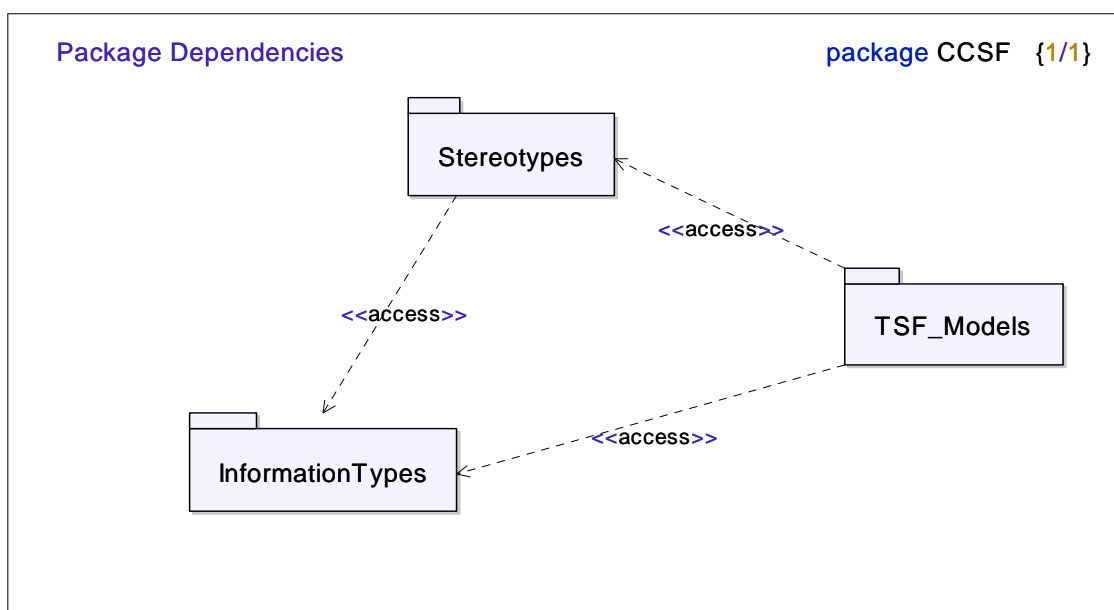
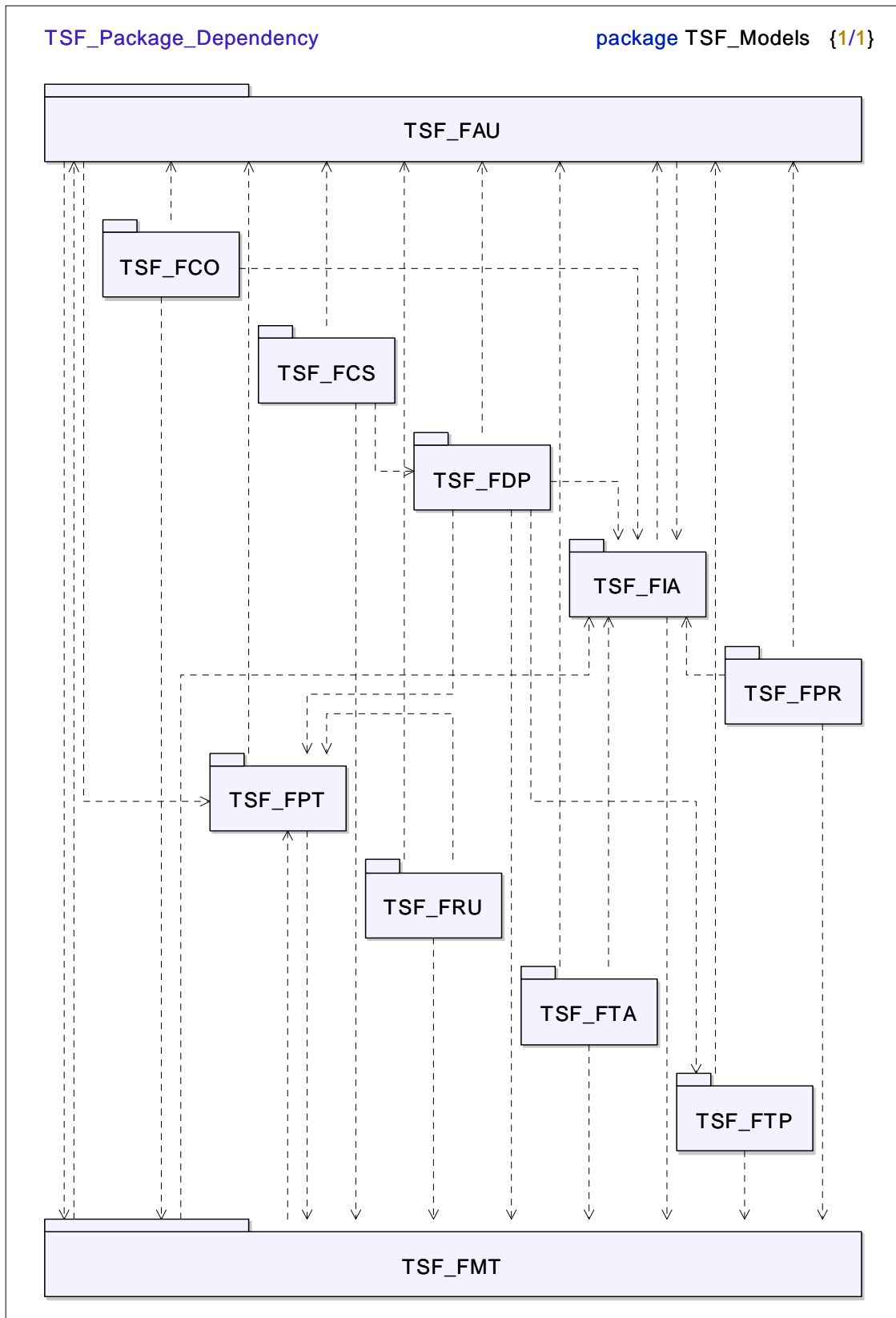


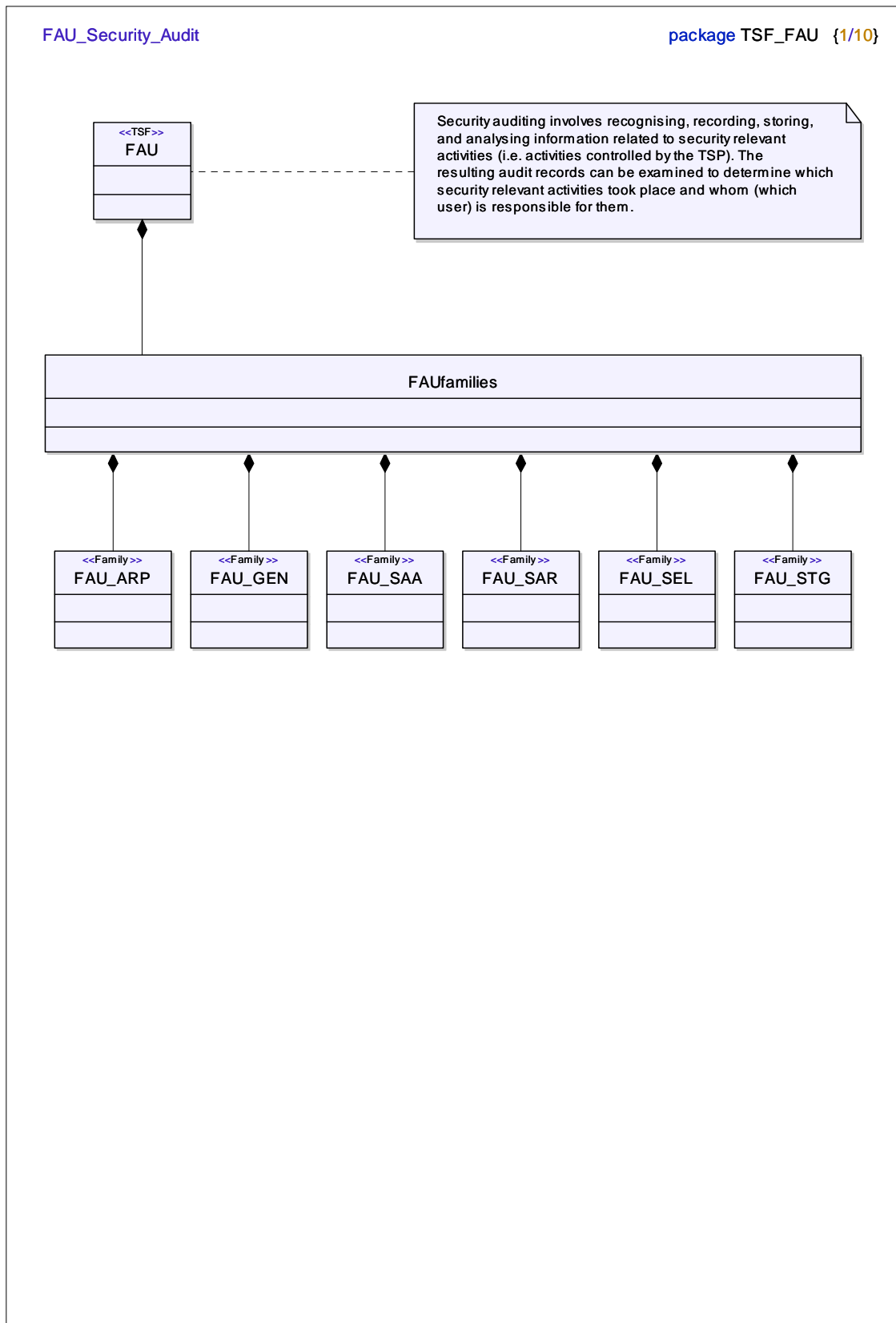
Figure A.3: The package dependencies

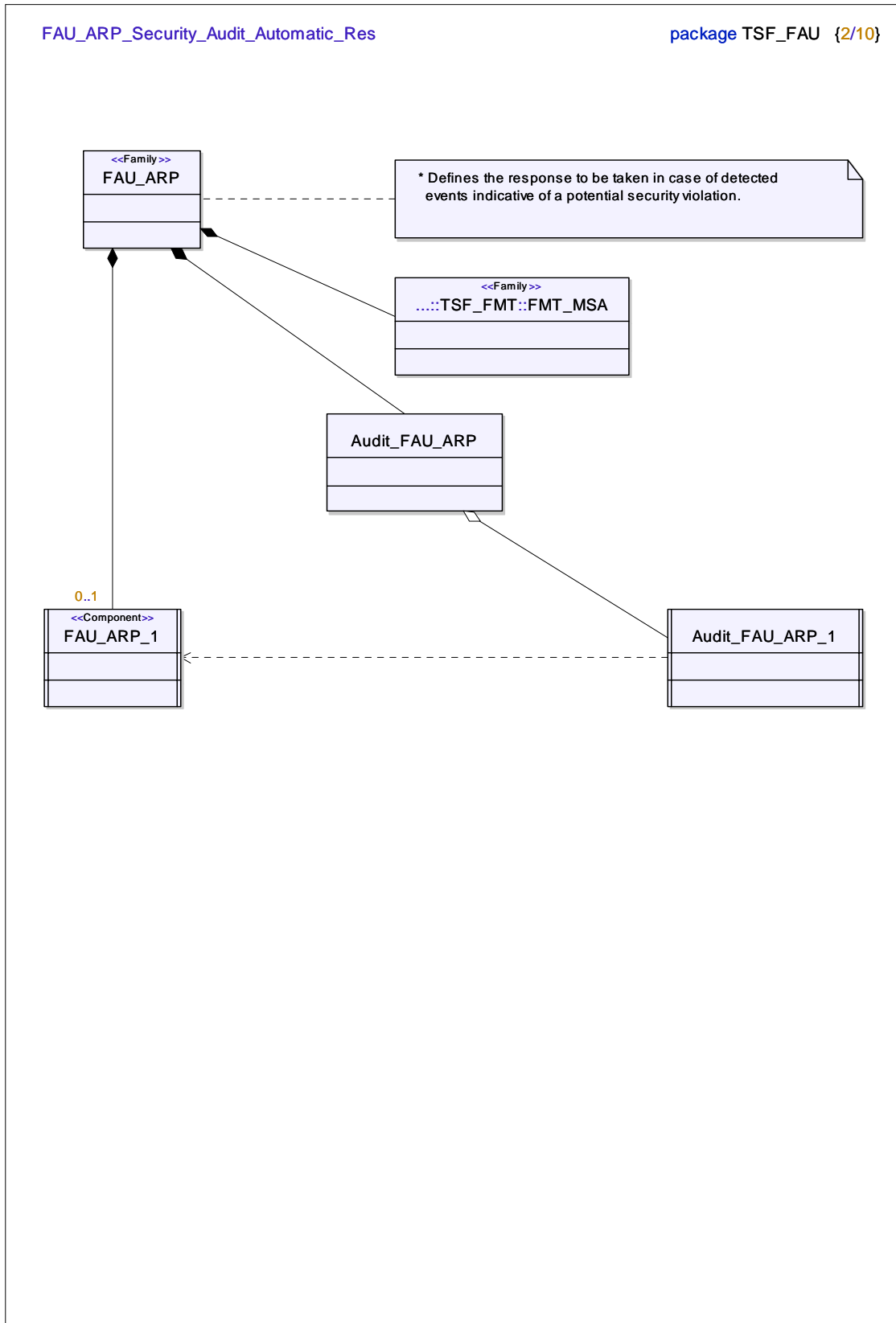
A.3 UML model for ISO/IEC 15408-2

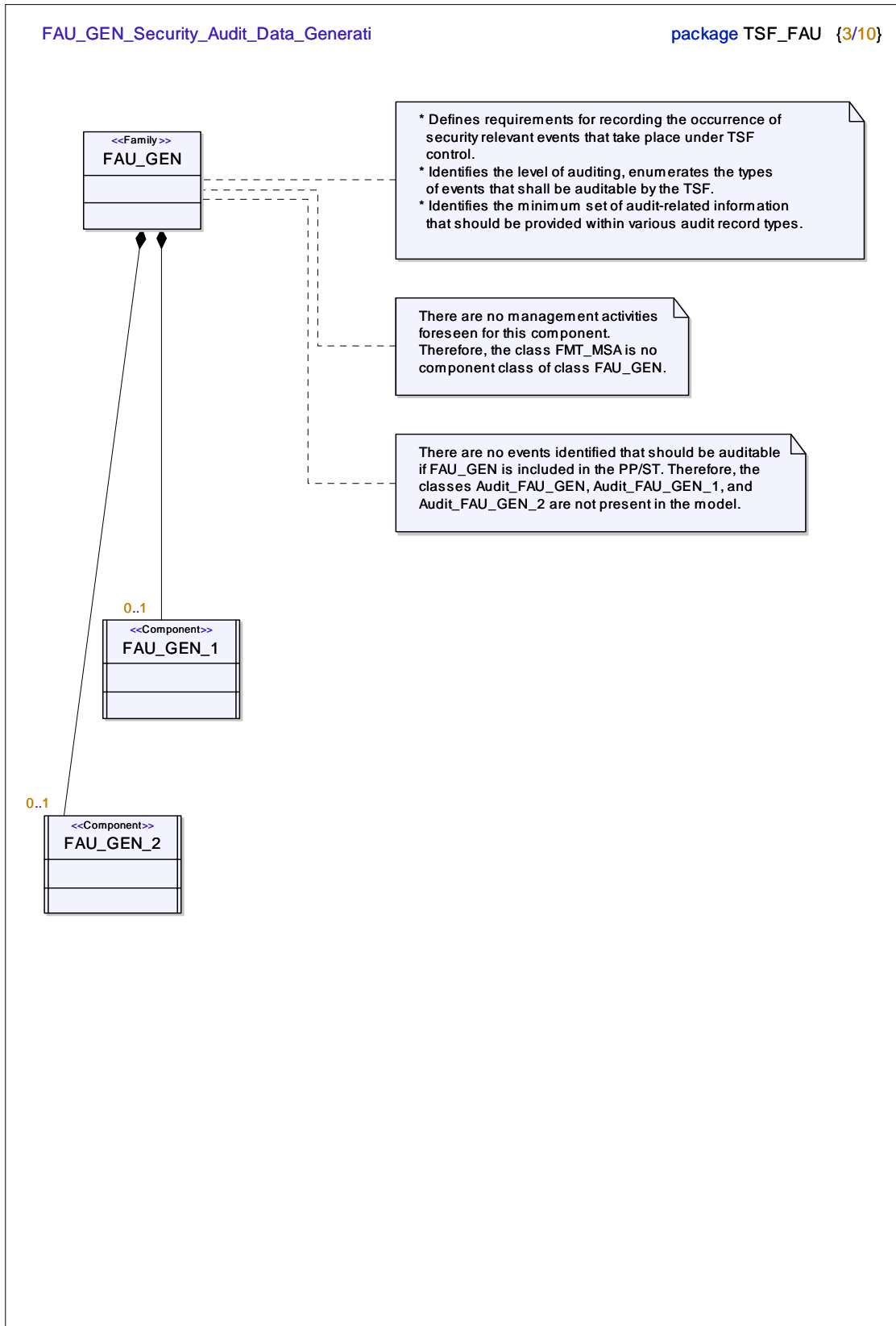
A.3.1 TSF Package Dependency

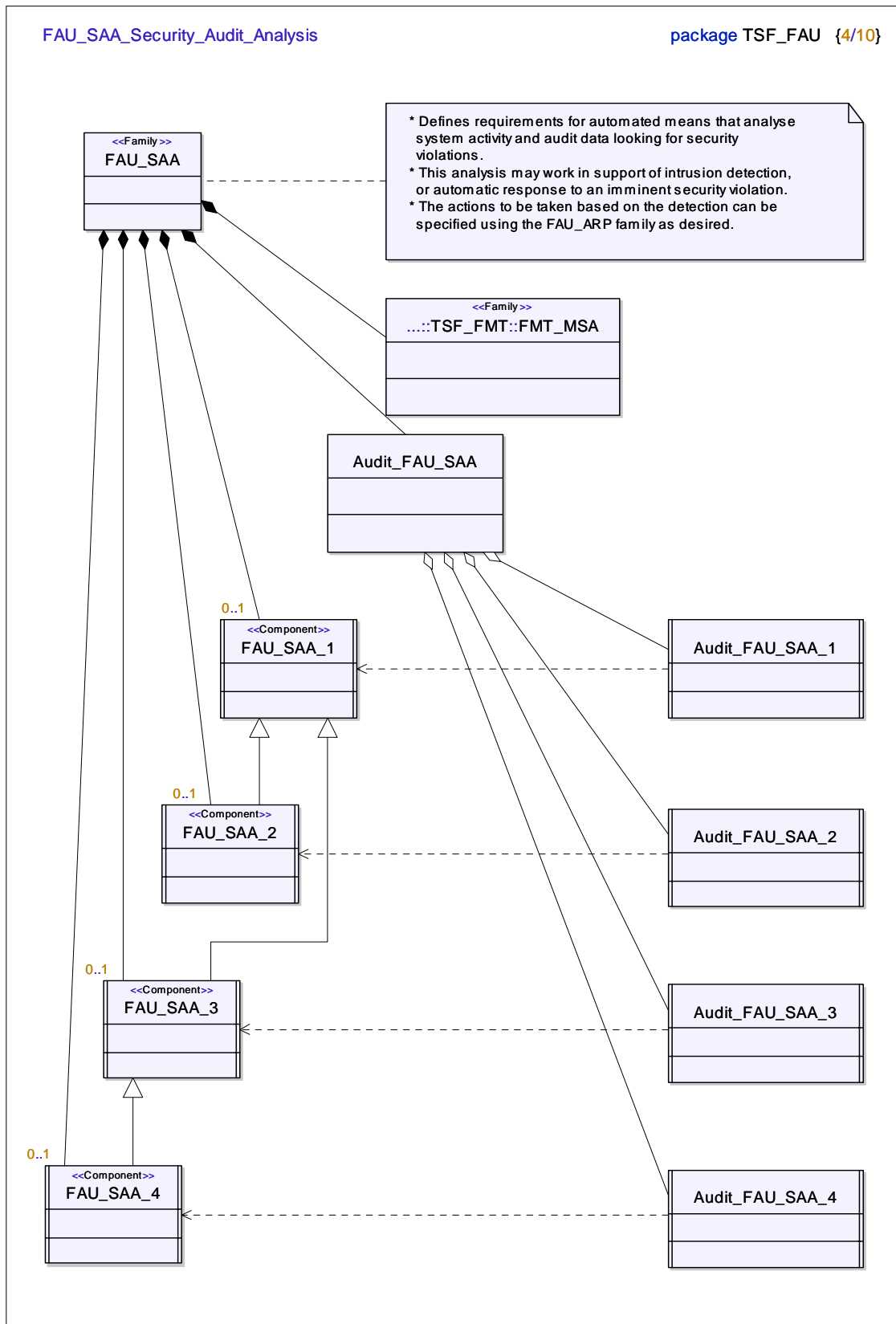


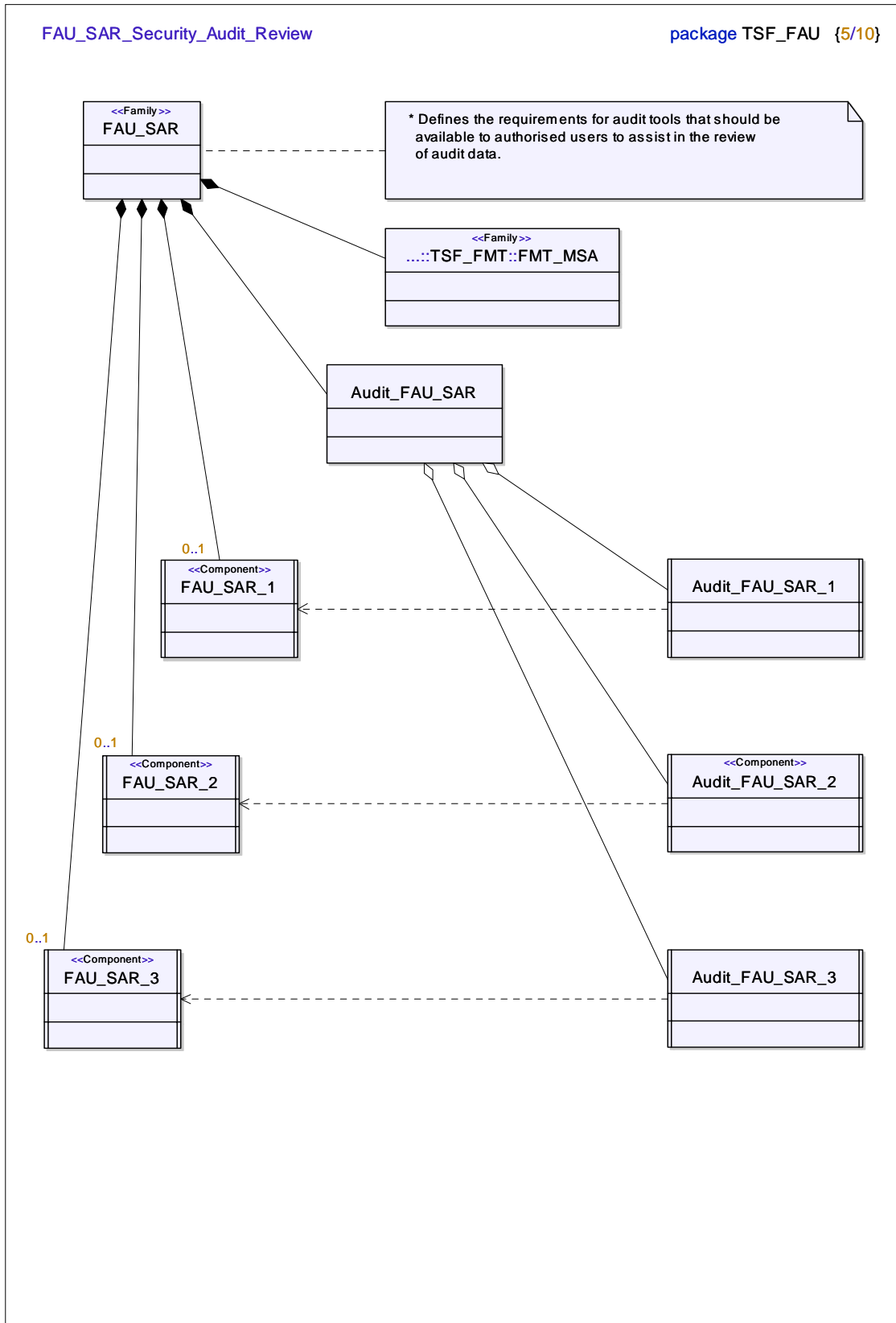
A.3.2 Package TSF_FAU

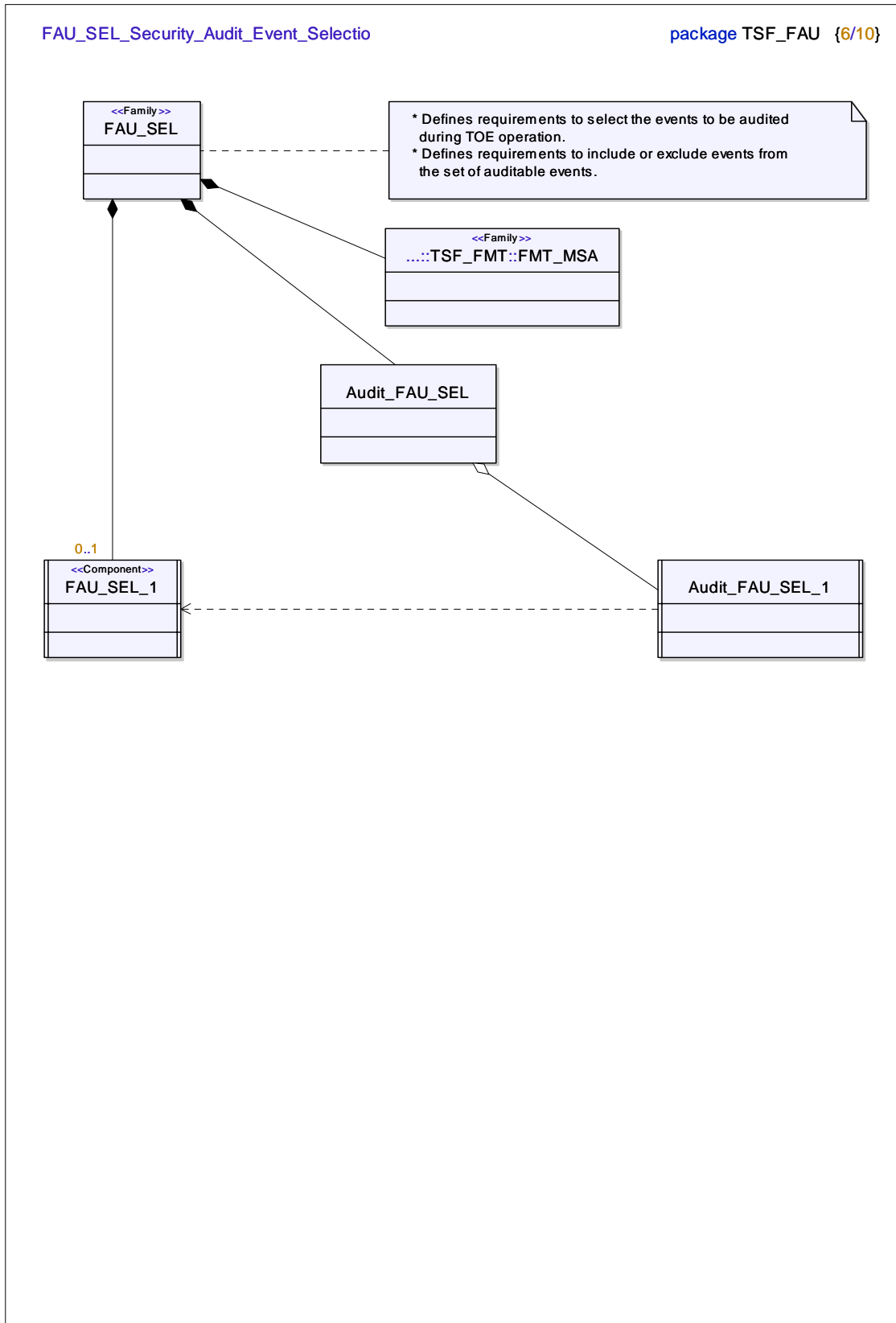


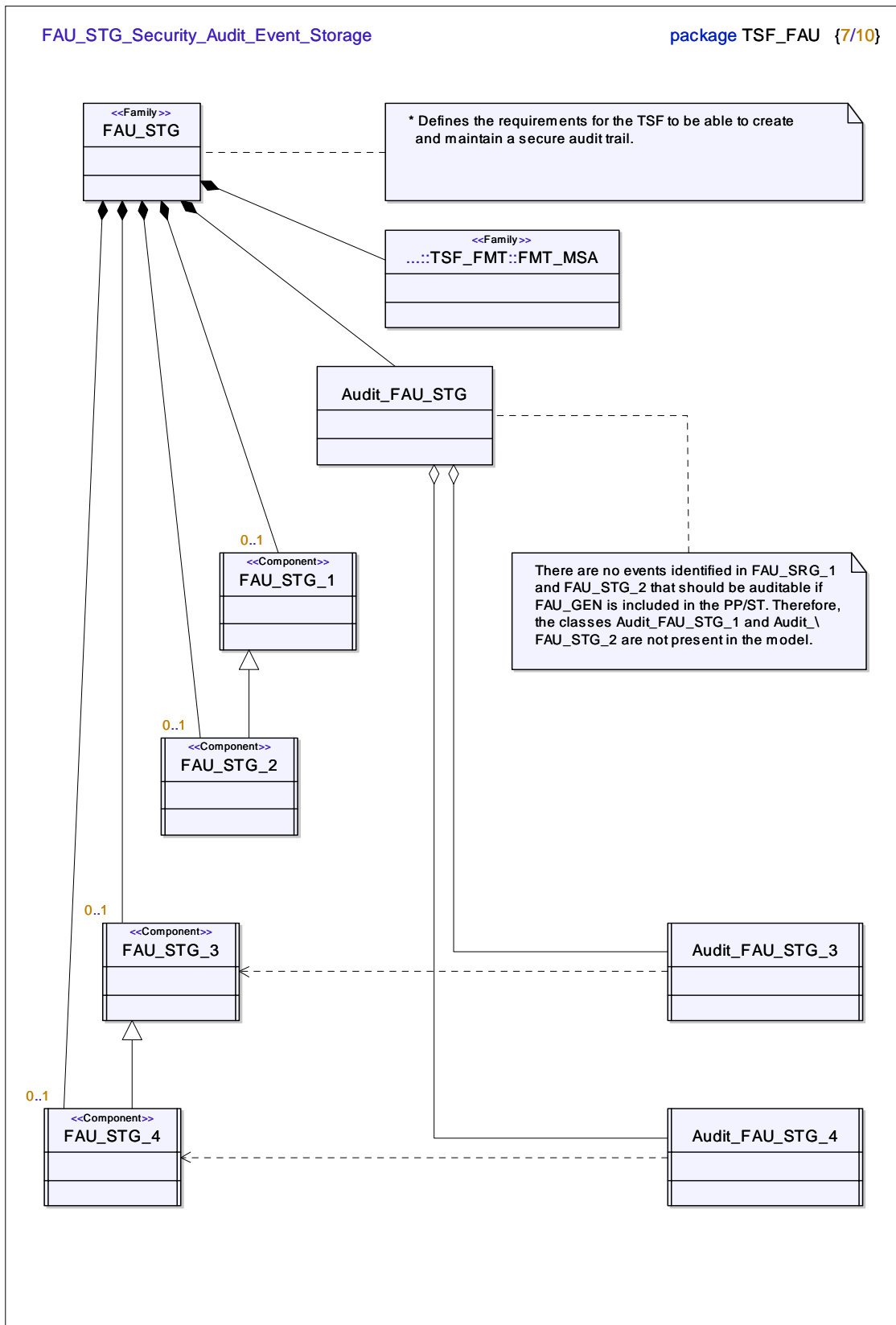


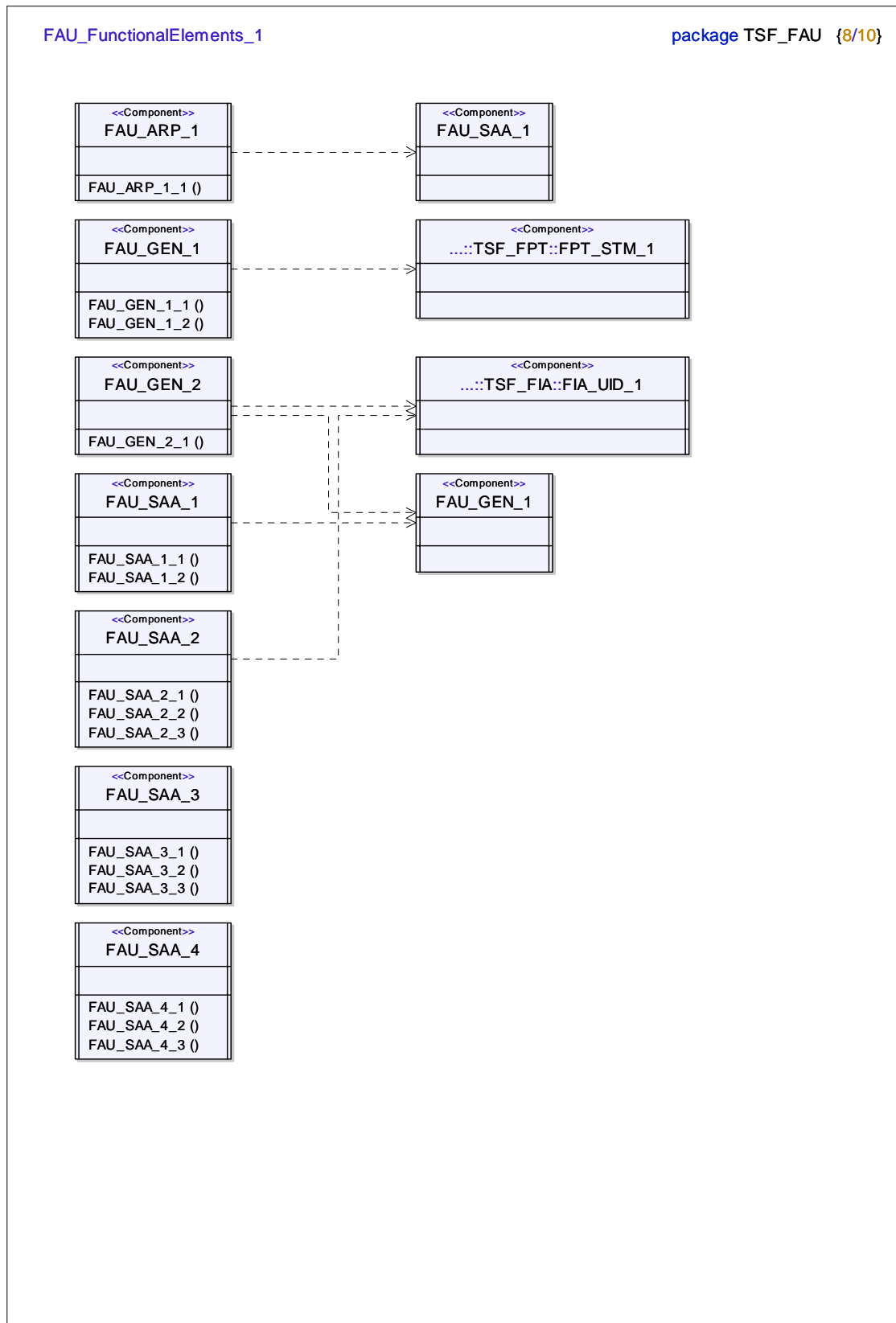


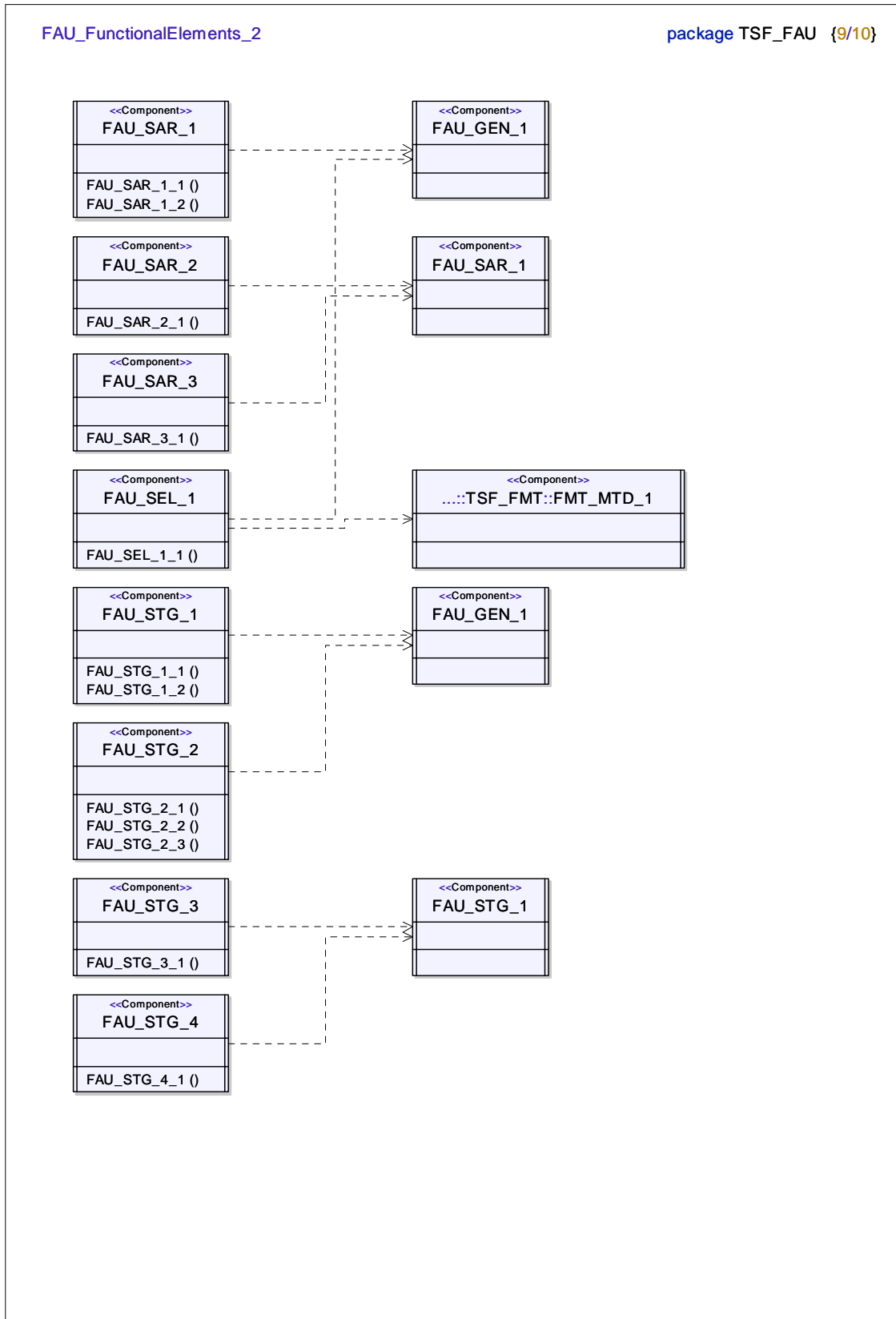












FAU_AuditEvents

package TSF_FAU {10/10}

Audit_FAU_ARP_1
auActnImminSecVioltn ()

Audit_FAU_SAA_1
auSecAnalysEnabDisab ()
auAutoRespons ()

Audit_FAU_SAA_2
auSecAnalysEnabDisab ()
auAutoRespons ()

Audit_FAU_SAA_3
auSecAnalysEnabDisab ()
auAutoRespons ()

Audit_FAU_SAA_4
auSecAnalysEnabDisab ()
auAutoRespons ()

Audit_FAU_SAR_1
auReadInfo ()

<<Component>>
Audit_FAU_SAR_2
auUnsuccesReadAtmpt ()

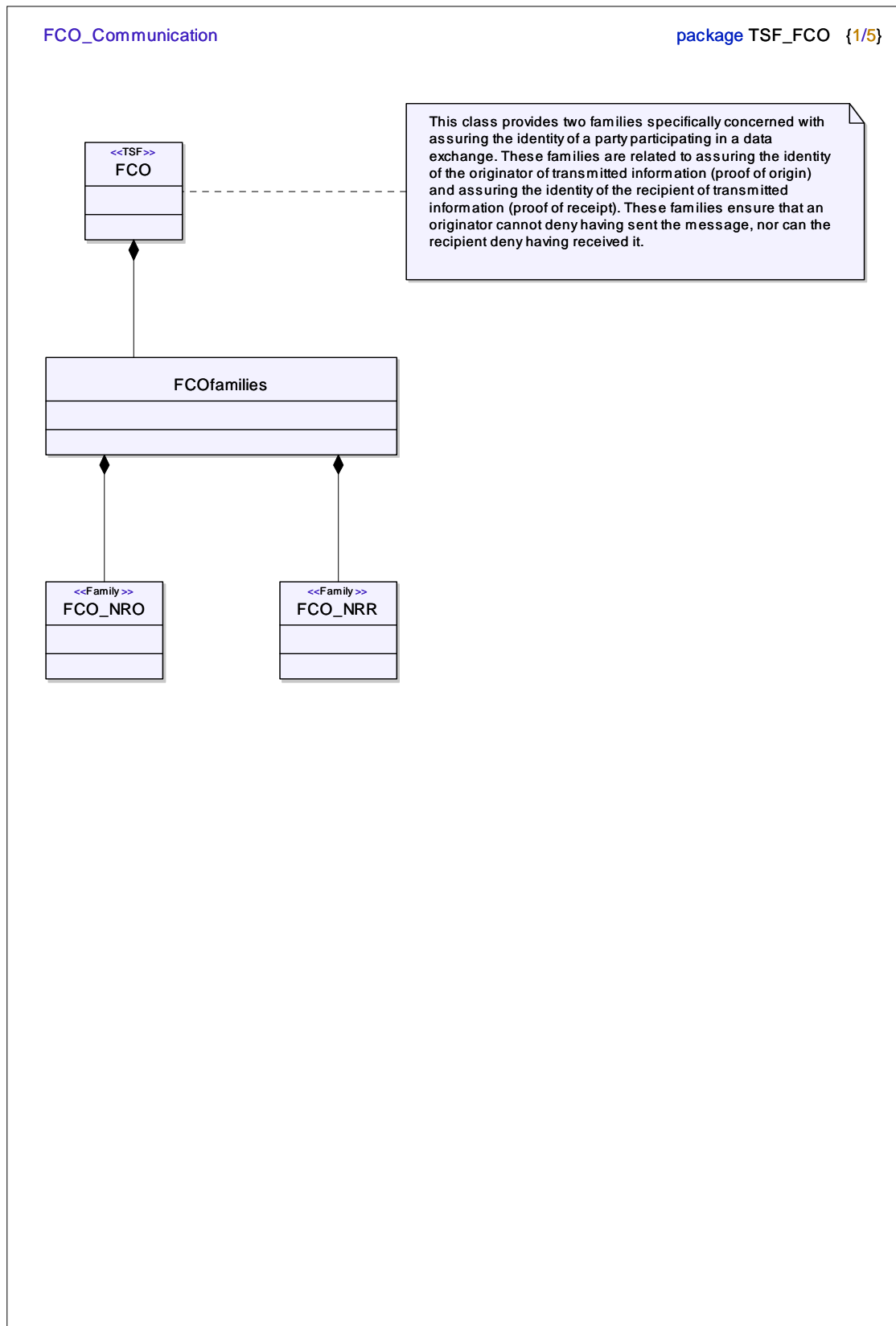
Audit_FAU_SAR_3
auViewingParam ()

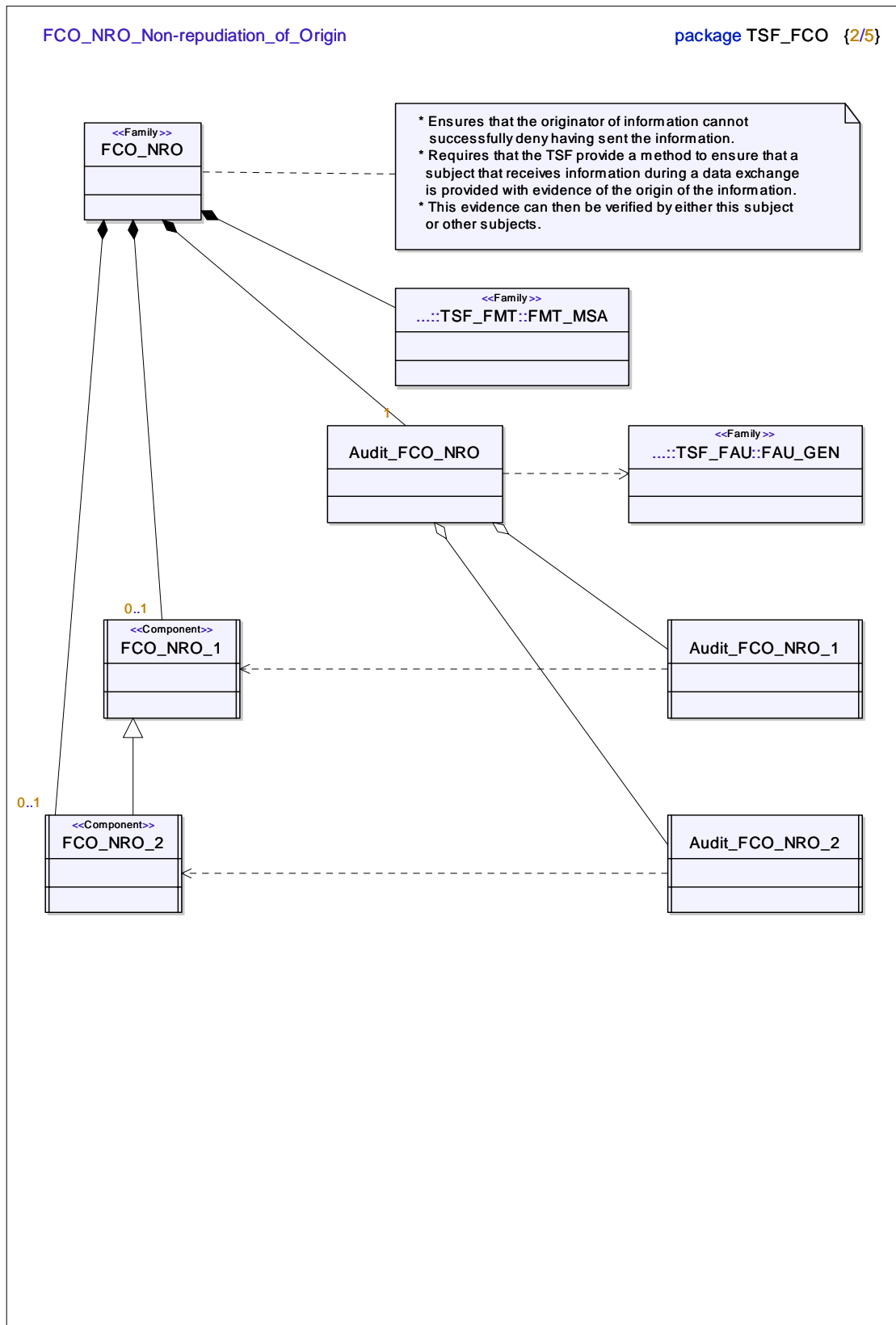
Audit_FAU_SEL_1
auAuditConfigModInOp ()

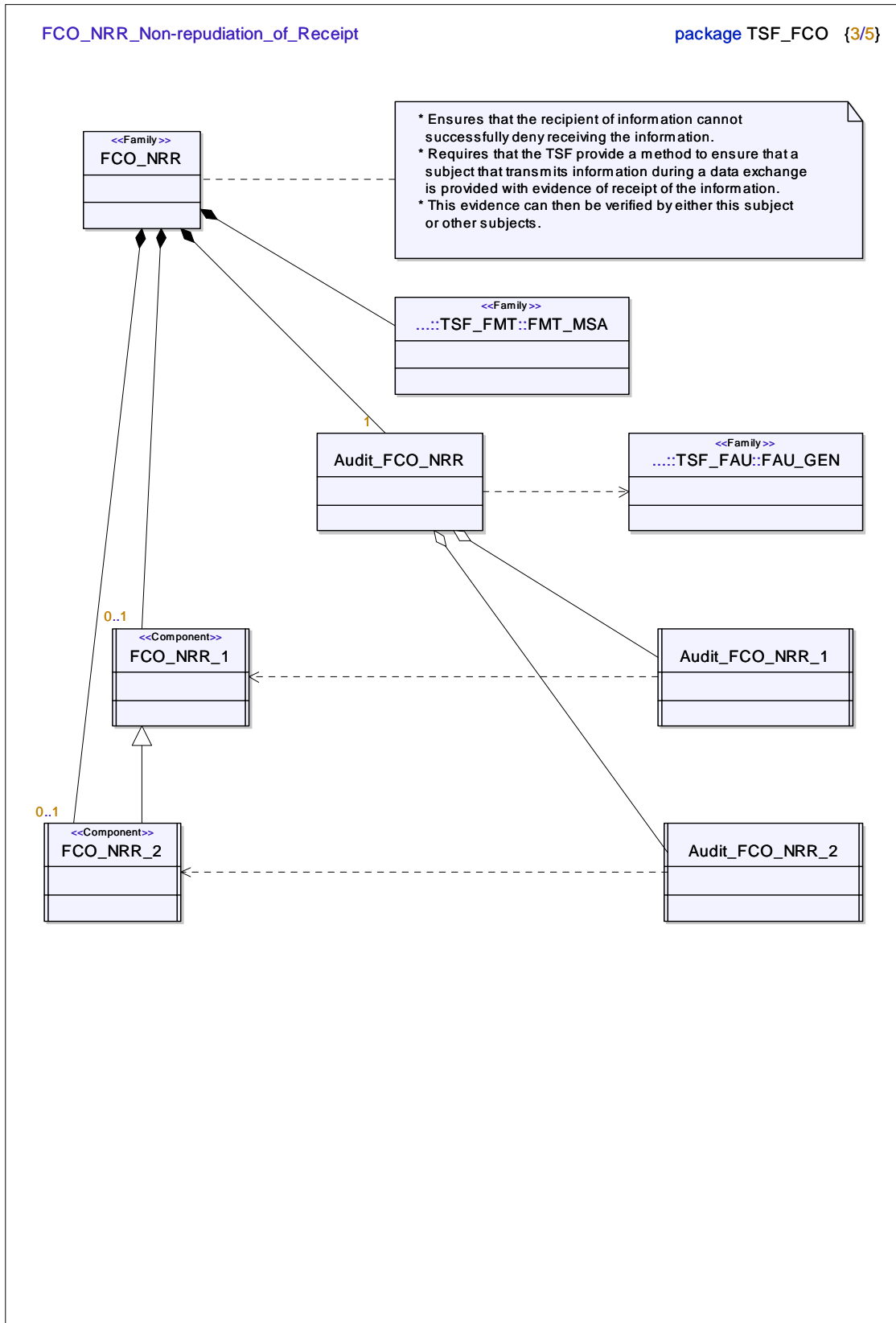
Audit_FAU_STG_3
auActnExceedThresh ()

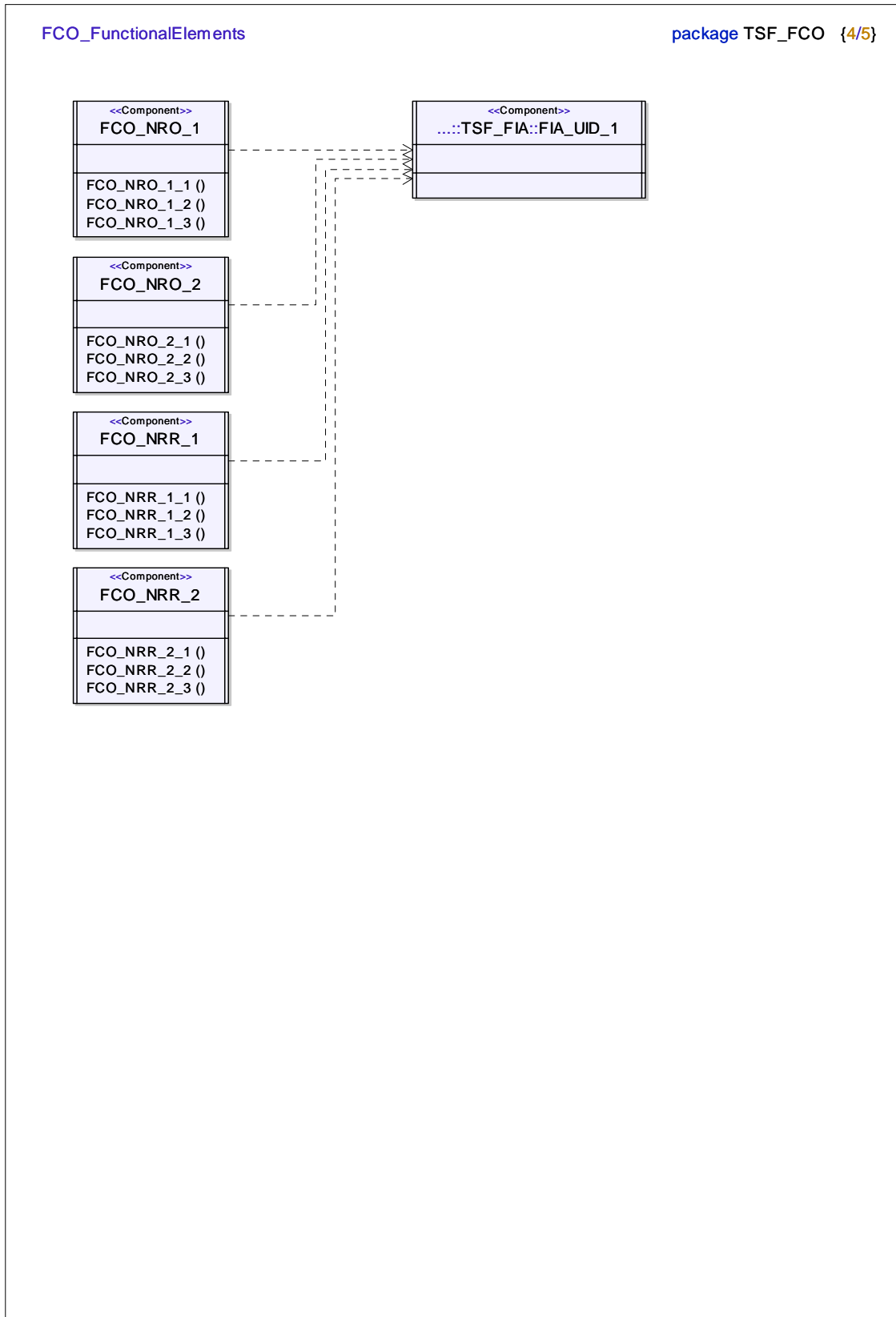
Audit_FAU_STG_4
auActnAuditStorageFail ()

A.3.3 Package TSF_FCO









FCO_AuditEvents

package TSF_FCO {5/5}

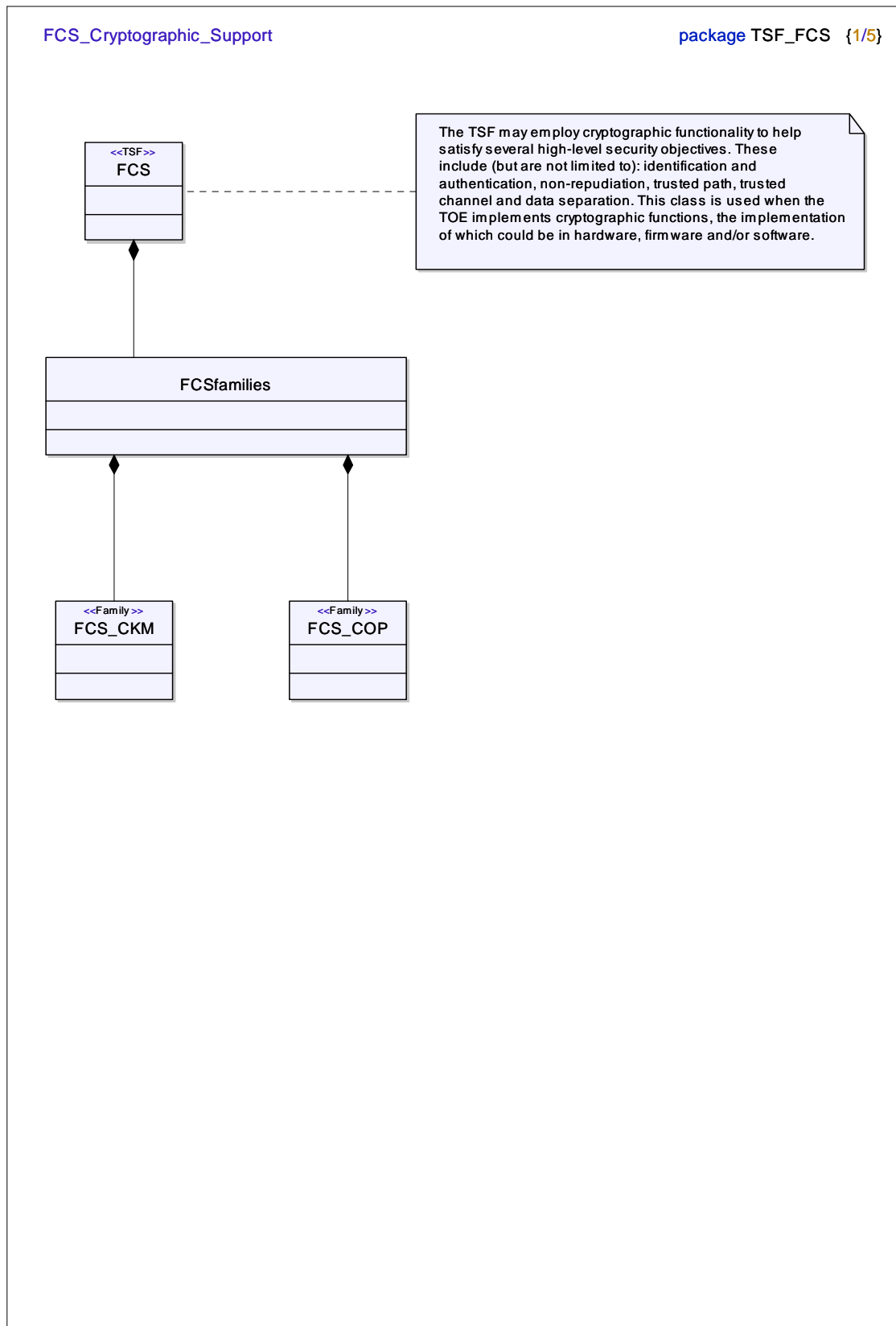
Audit_FCO_NRO_1
auDuserReqEvid () auInvokeNonRepudServ () auDinfoDestEvid () auDuserReqVerif ()

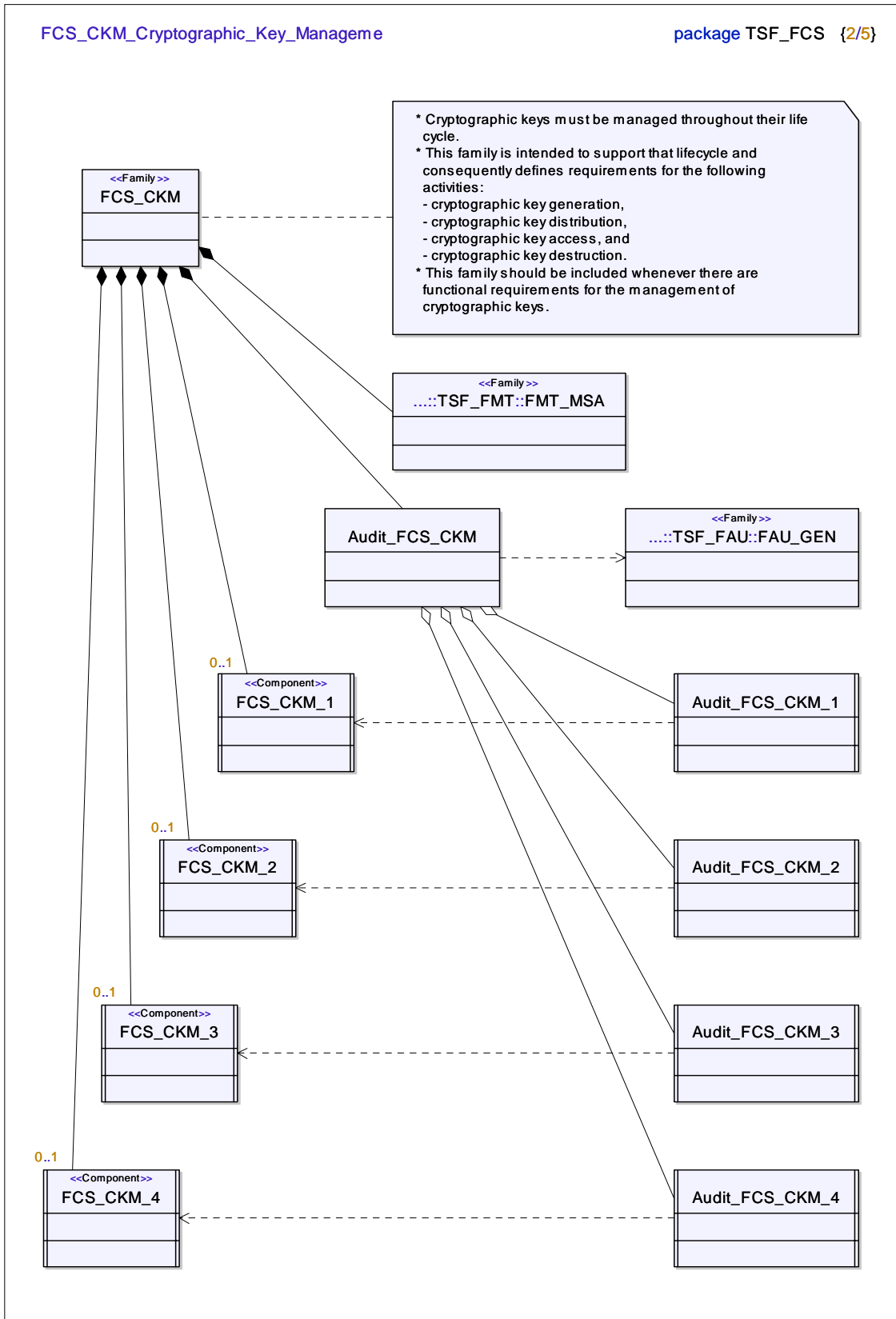
Audit_FCO_NRR_1
auDuserReqEvid () auInvokeNonRepudServ () auDinfoDestEvid () auDuserReqVerif ()

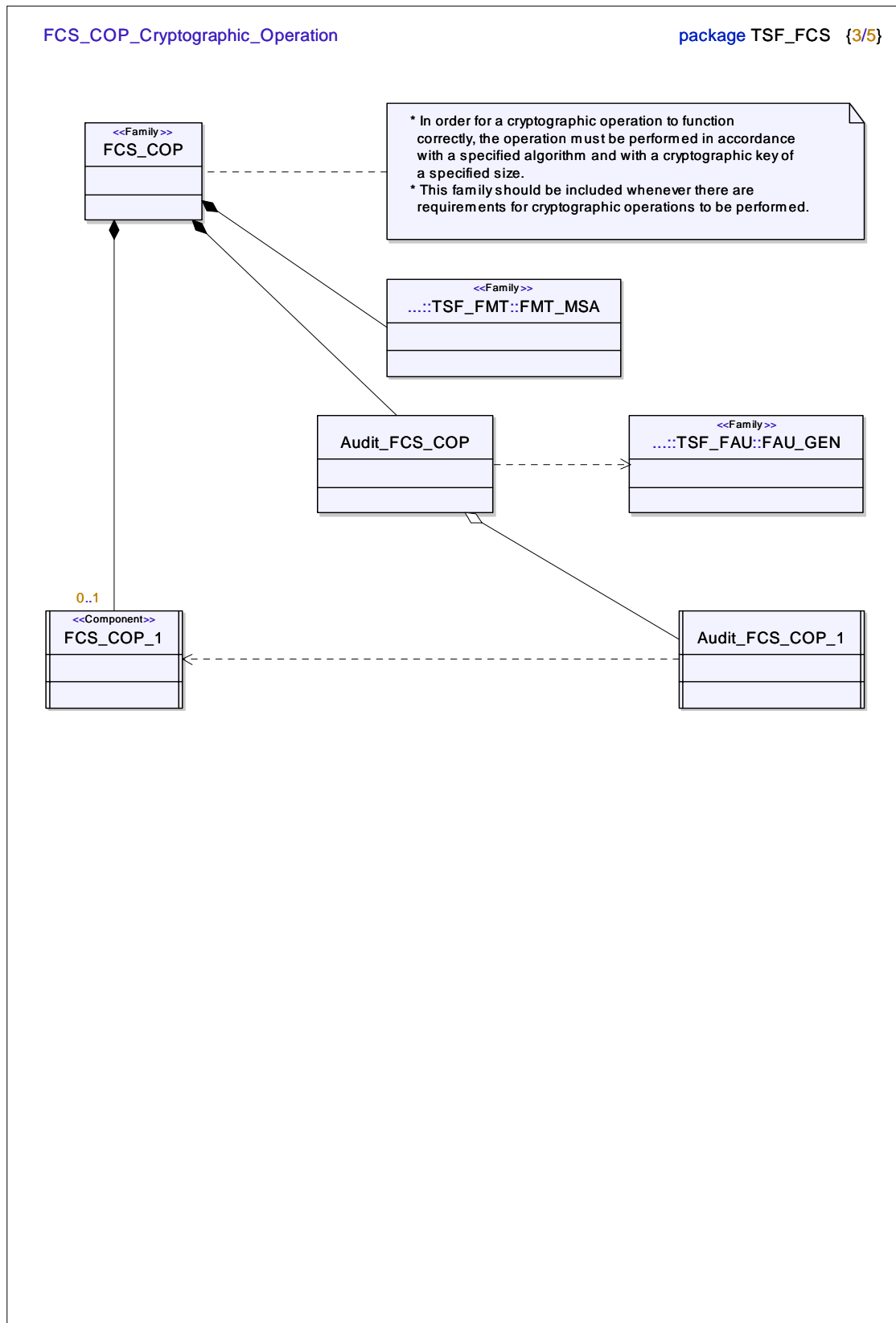
Audit_FCO_NRO_2
auInvokeNonRepudServ () auDinfoDestEvid () auDuserReqVerif ()

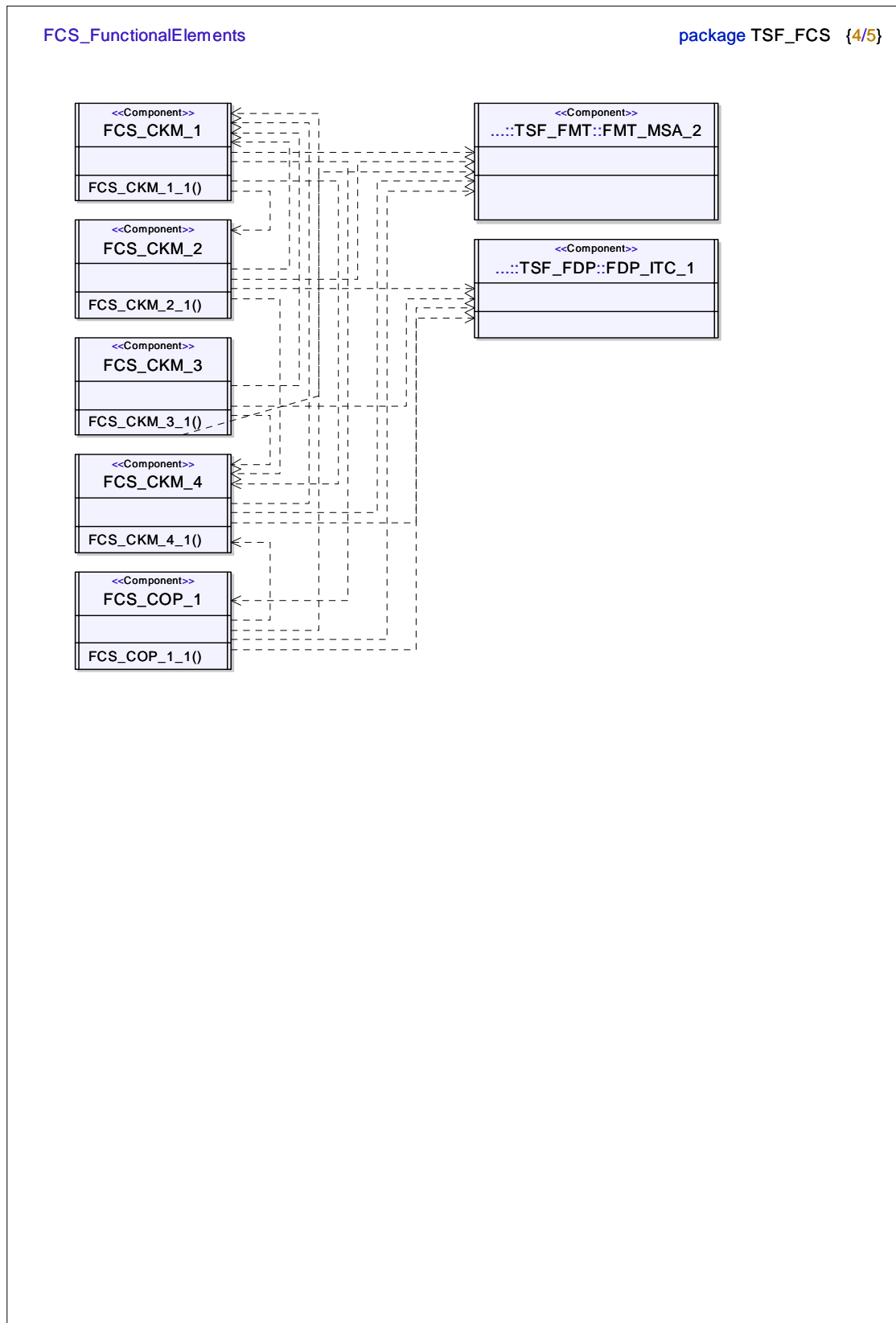
Audit_FCO_NRR_2
auInvokeNonRepudServ () auDinfoDestEvid () auDuserReqVerif ()

A.3.4 Package TSF_FCS









FCS_AuditEvents

package TSF_FCS {5/5}

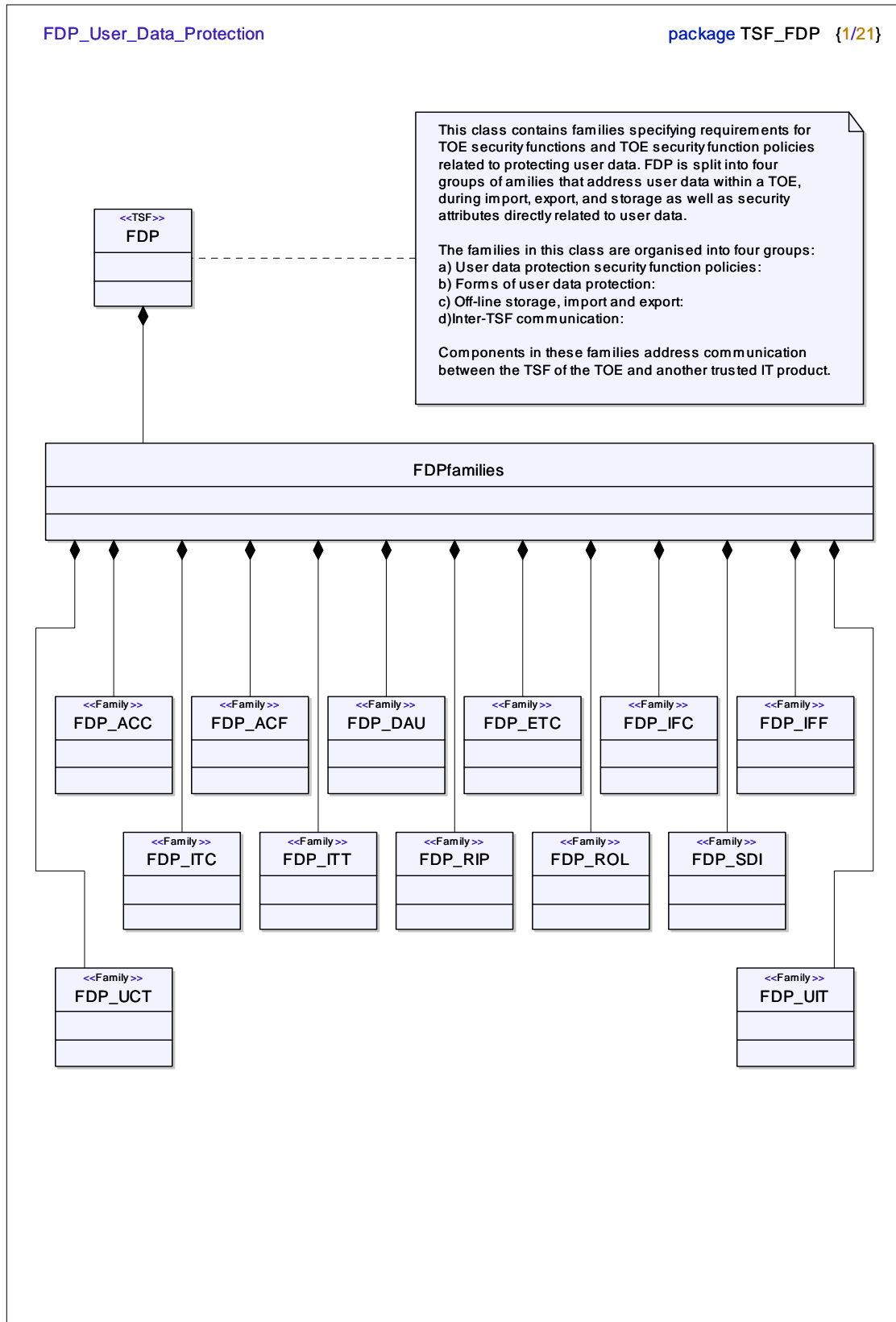
Audit_FCS_CKM_1
auSuccess () auObjectAttrib () auObjectValue ()

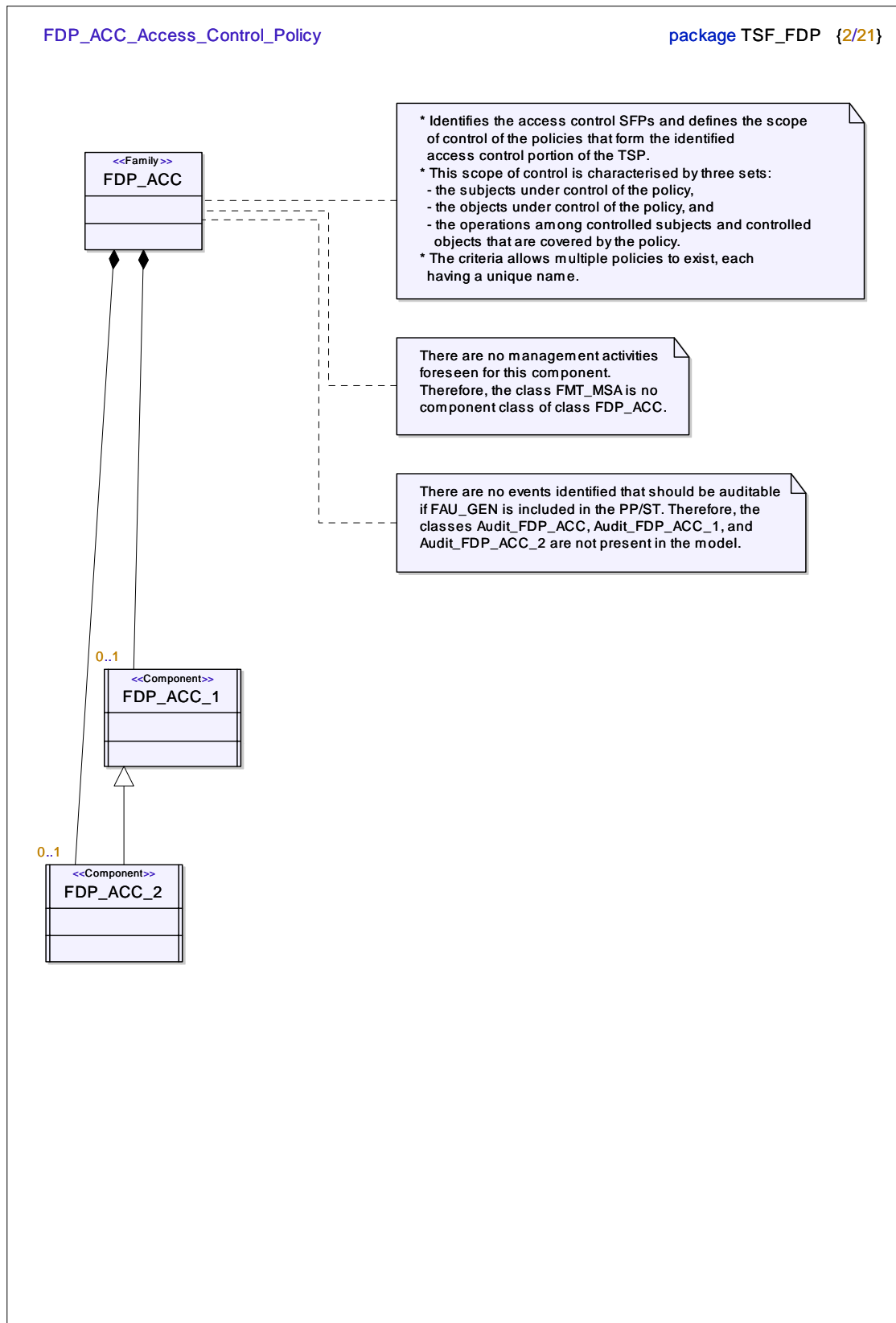
Audit_FCS_COP_1
auSuccess () auModeOperation () auObjectAttrib () auSubjectAttrib ()

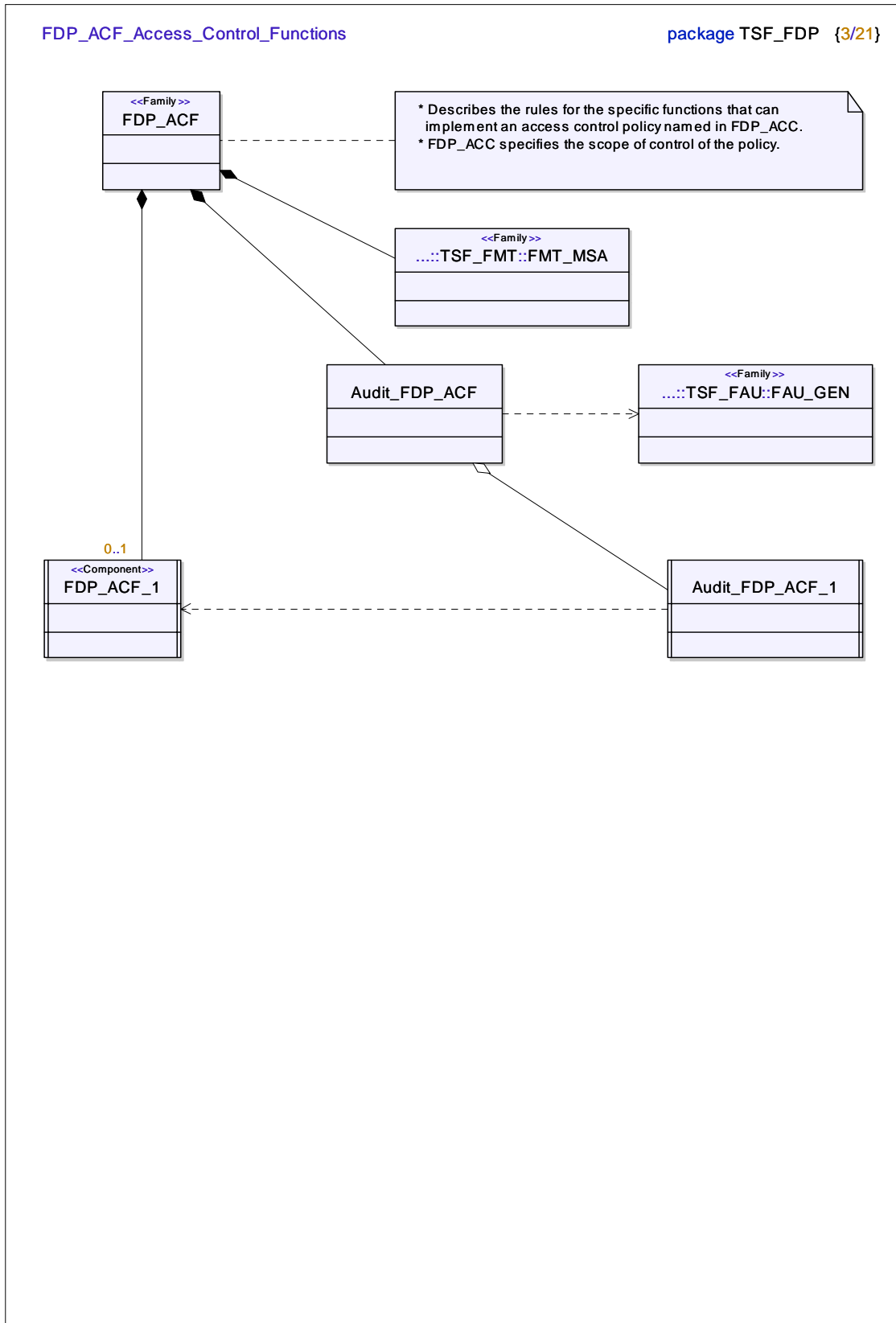
Audit_FCS_CKM_2
auSuccess () auObjectAttrib () auObjectValue ()

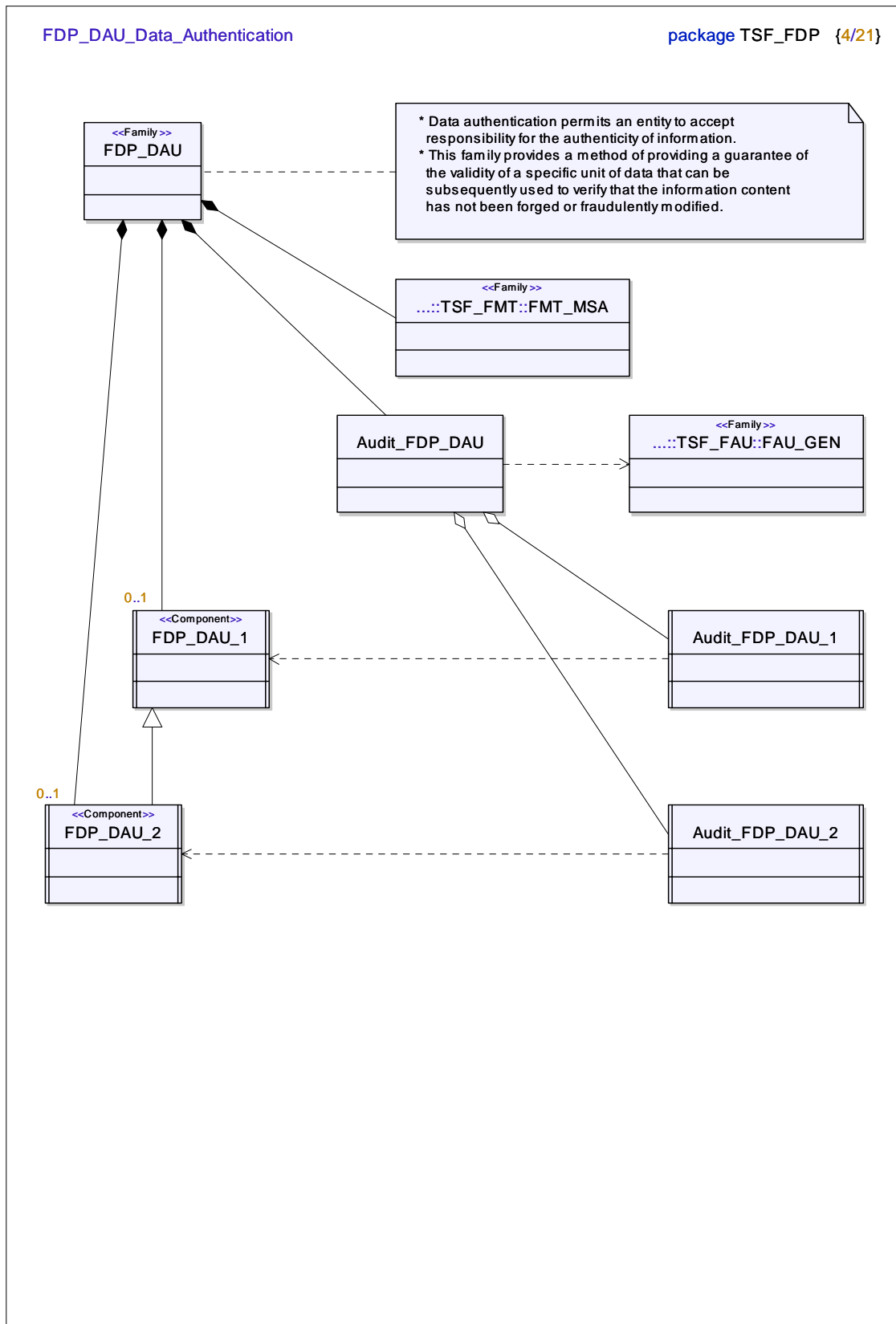
Audit_FCS_CKM_3
auSuccess () auObjectAttrib () auObjectValue ()

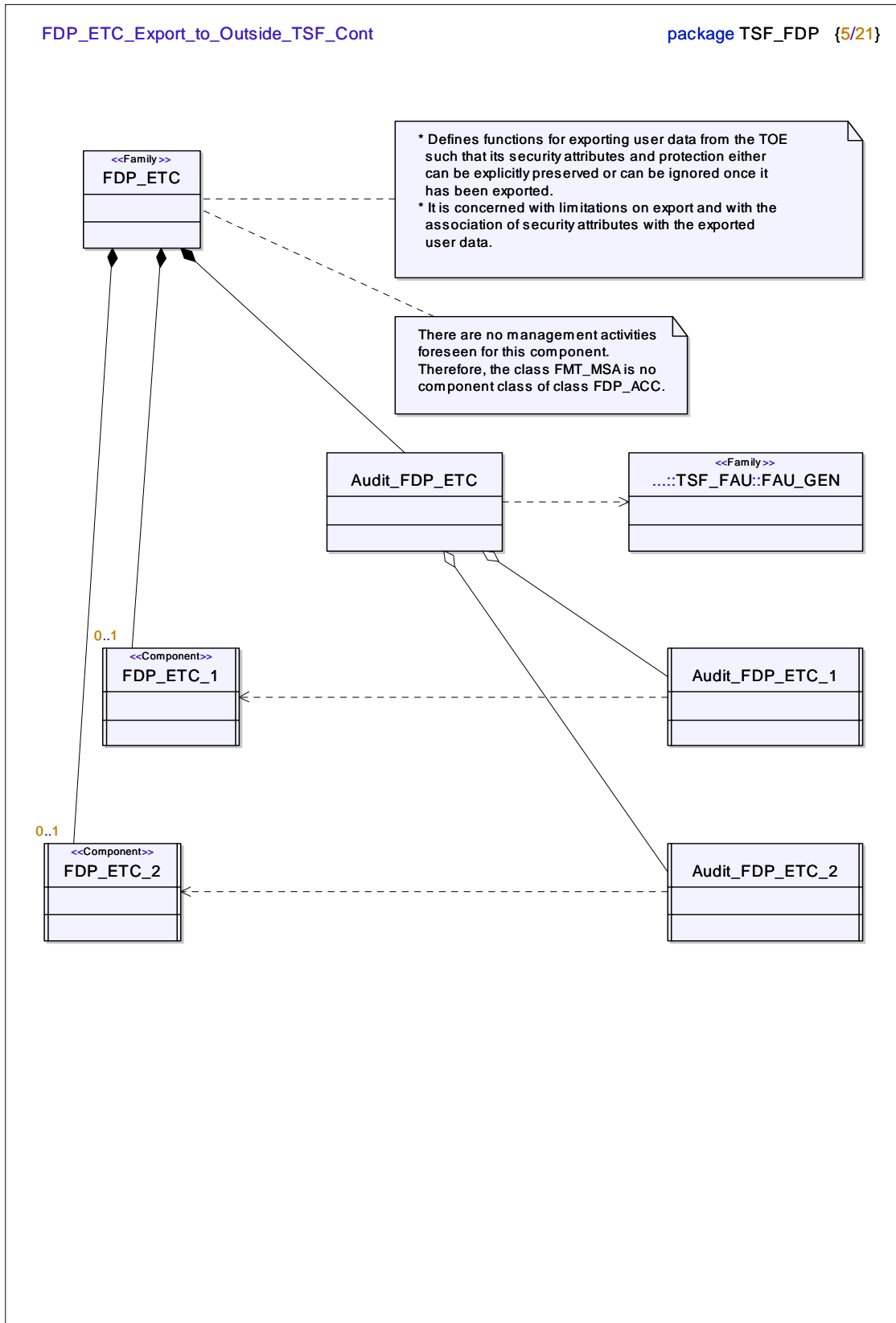
Audit_FCS_CKM_4
auSuccess () auObjectAttrib () auObjectValue ()

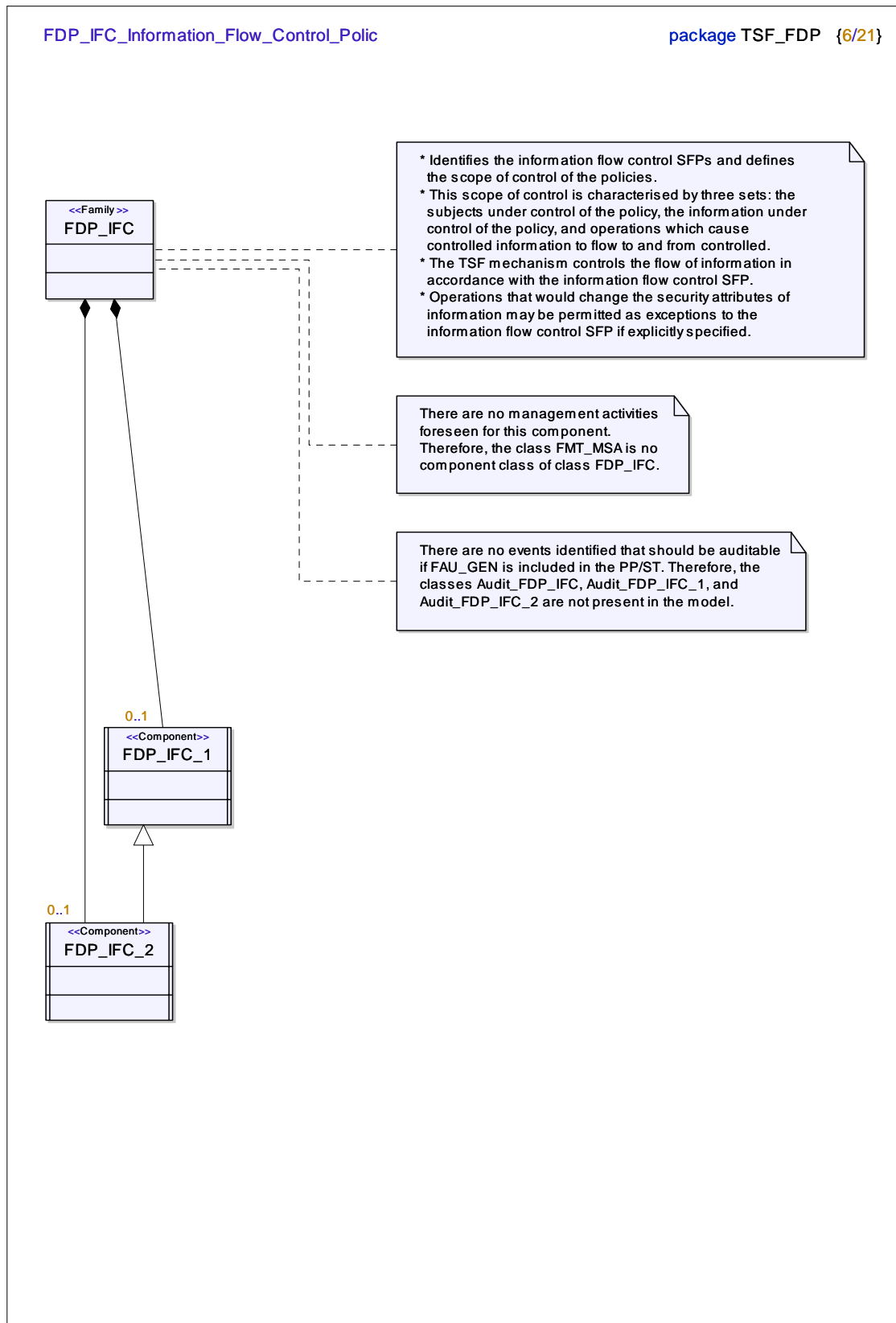


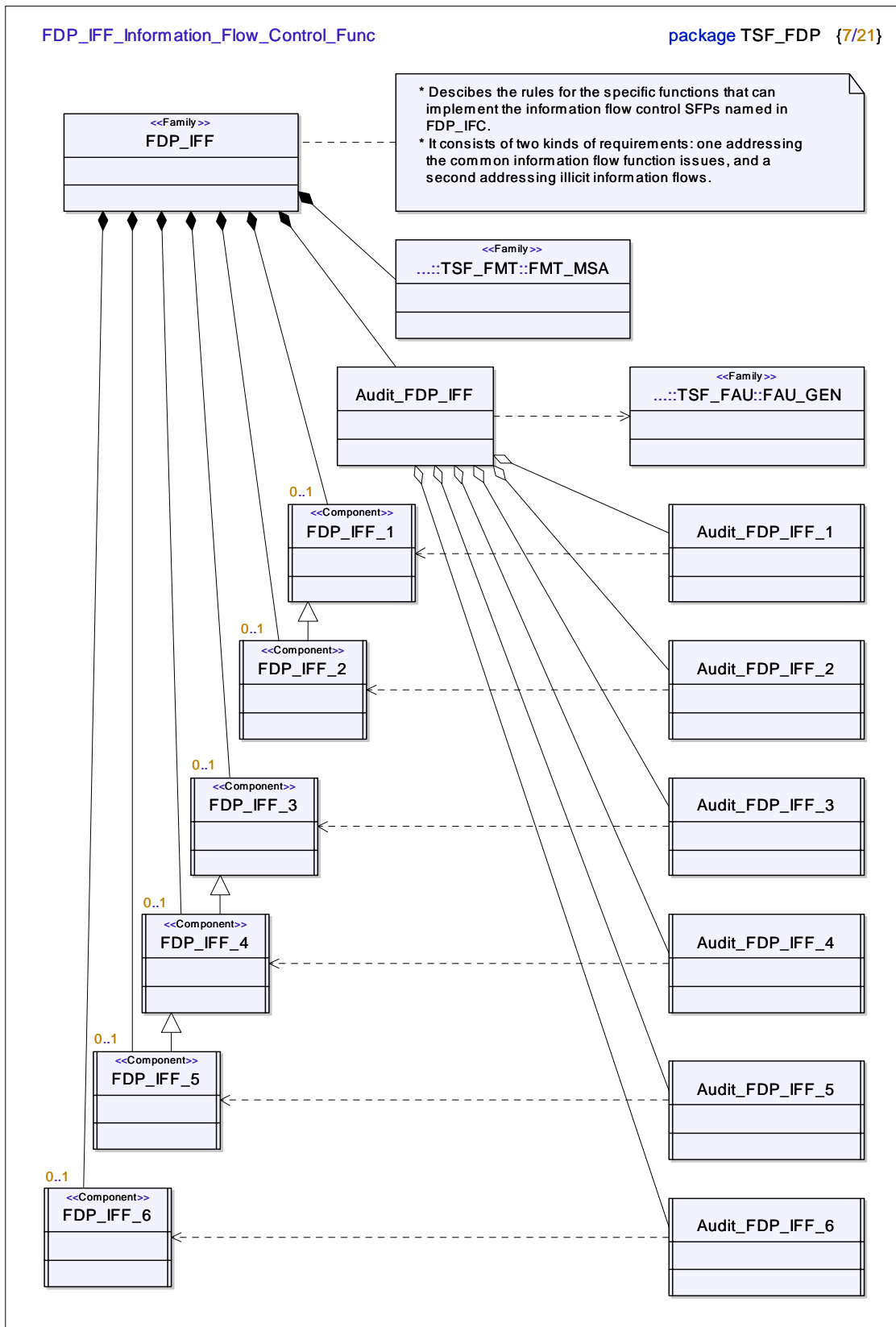


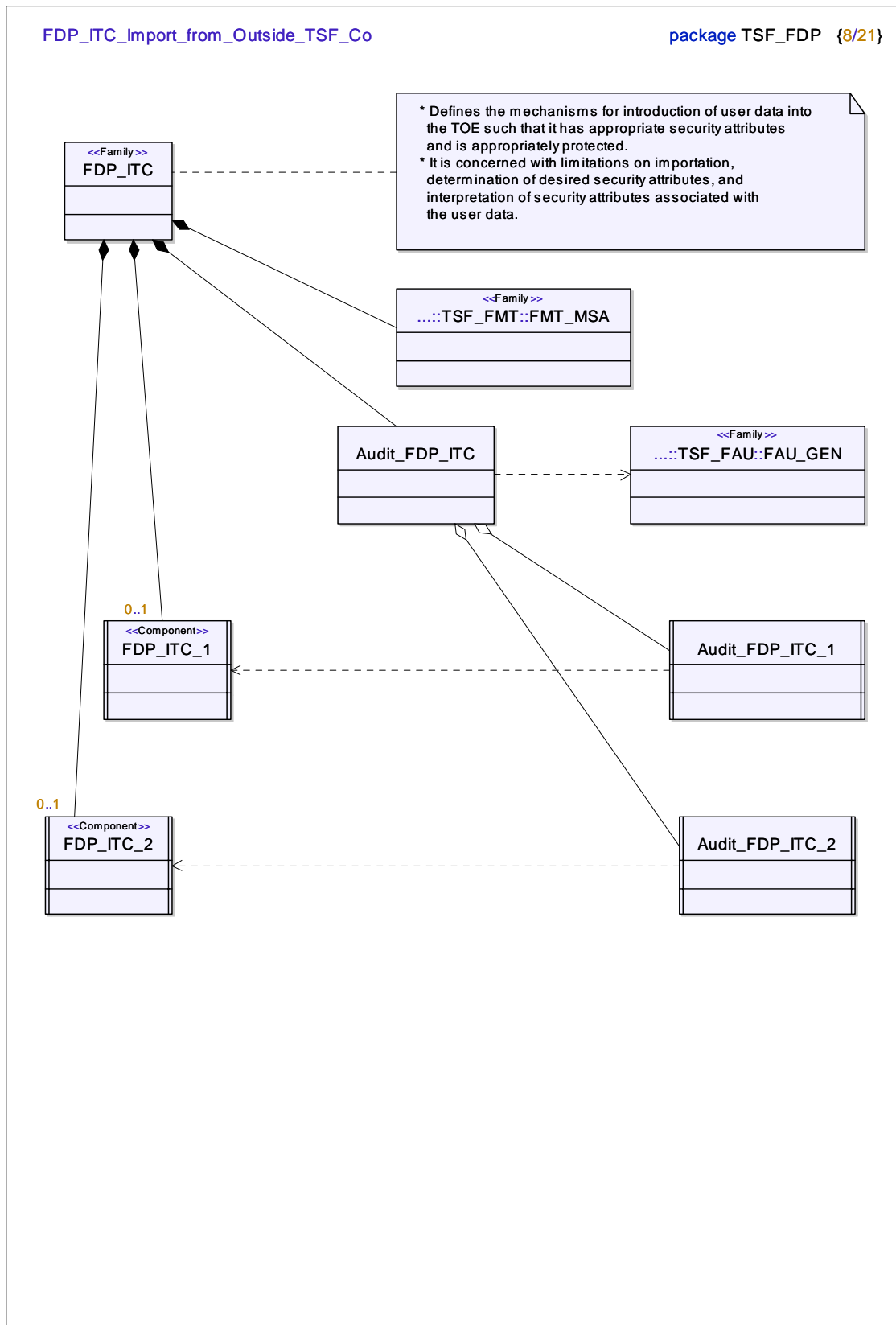


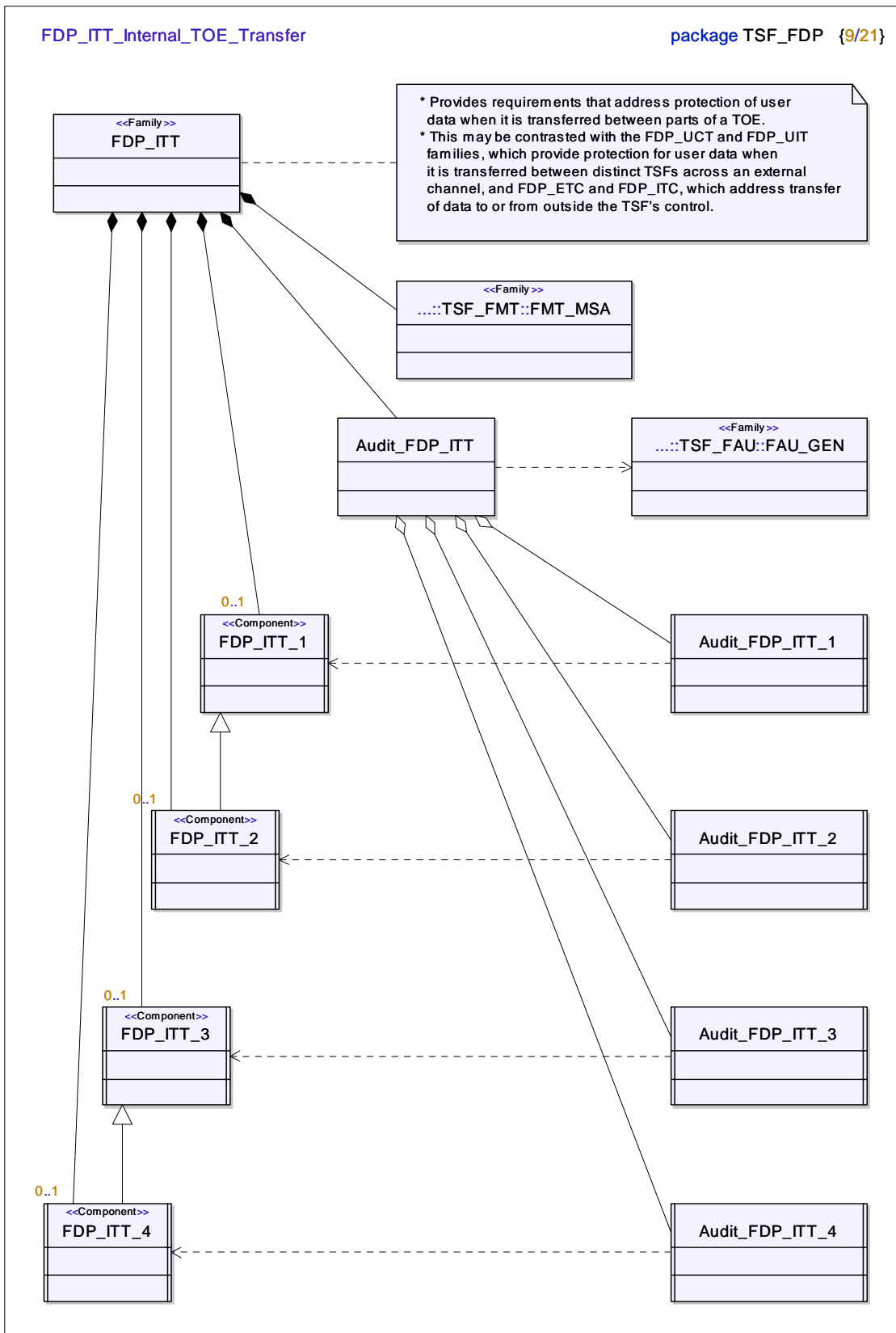


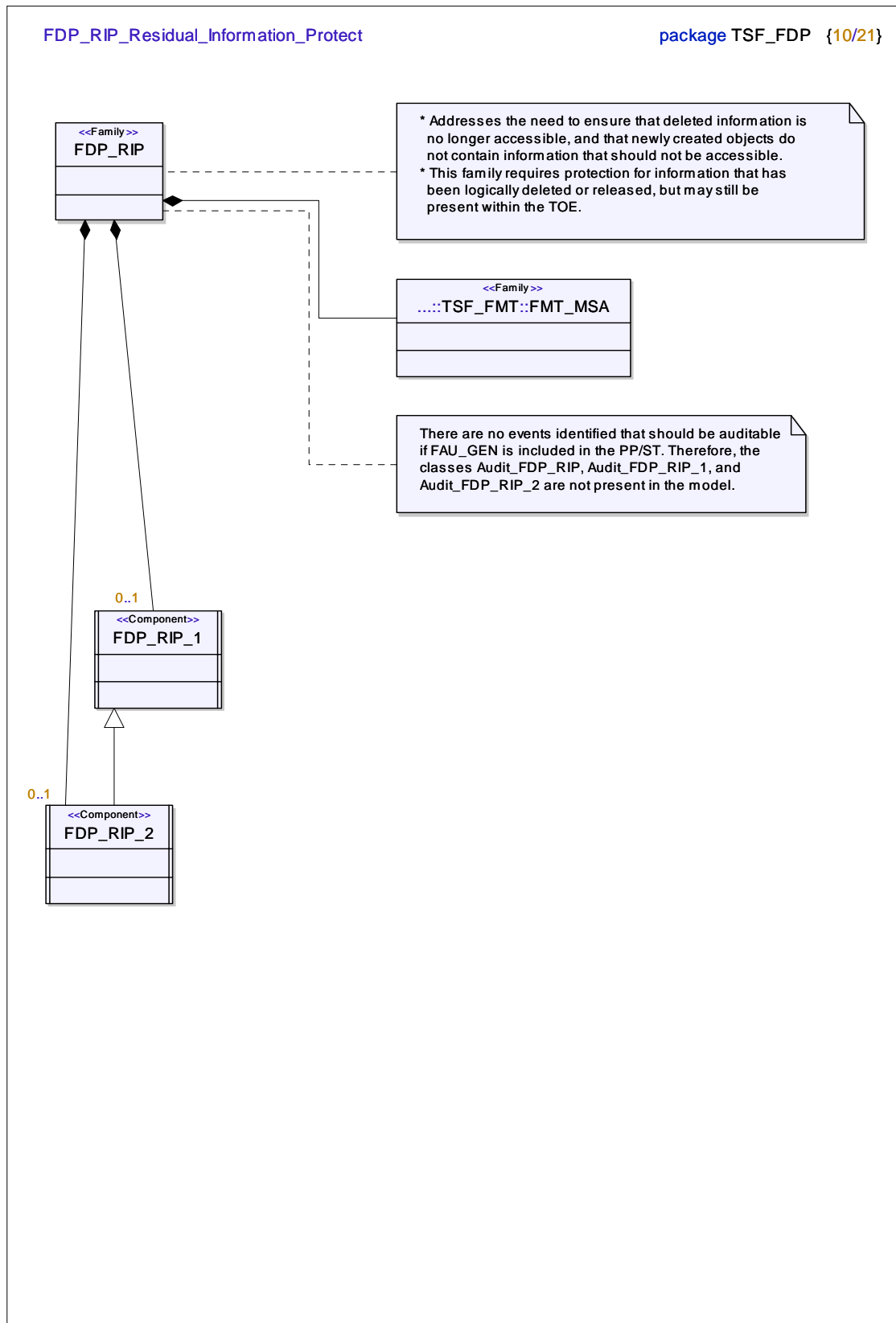


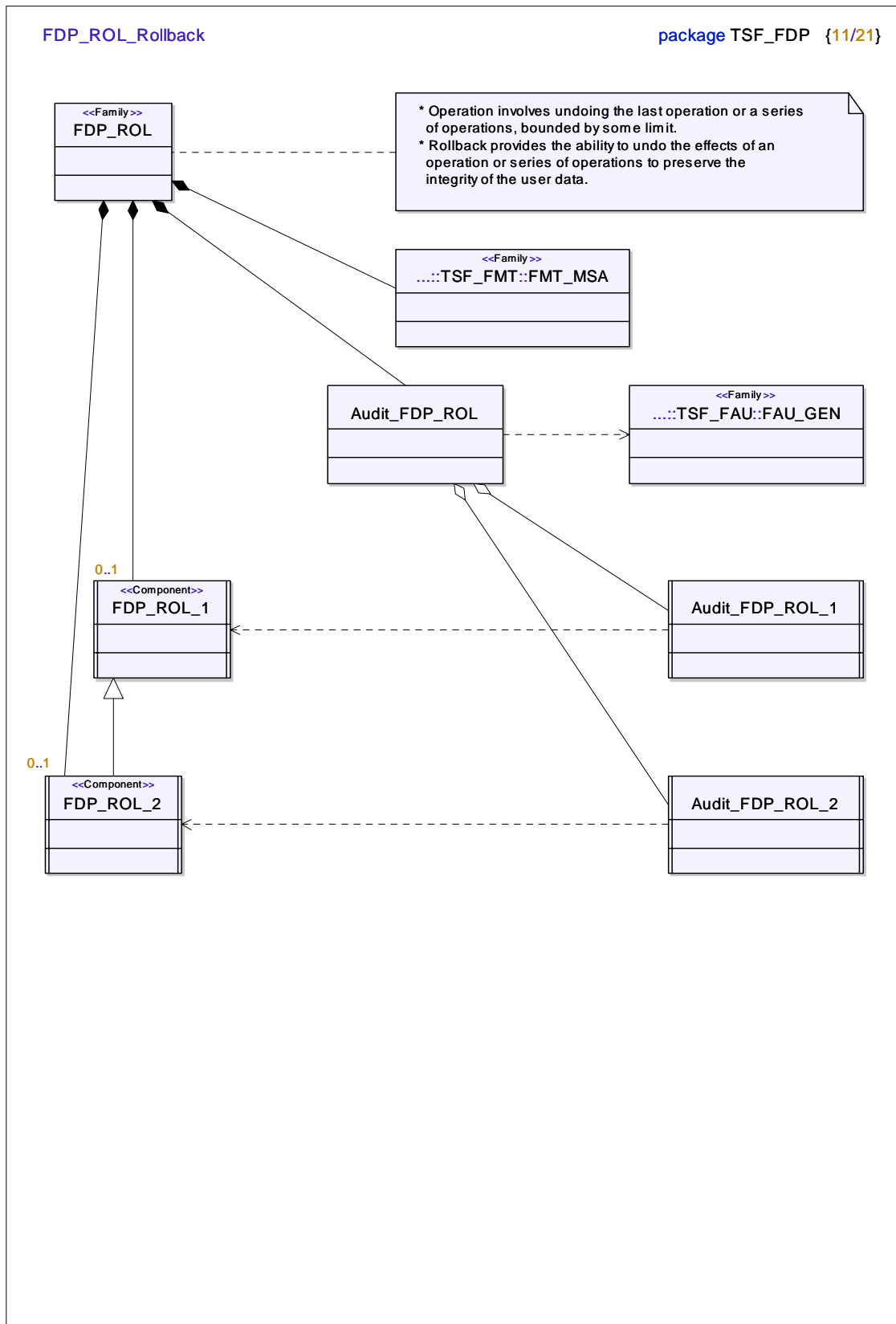


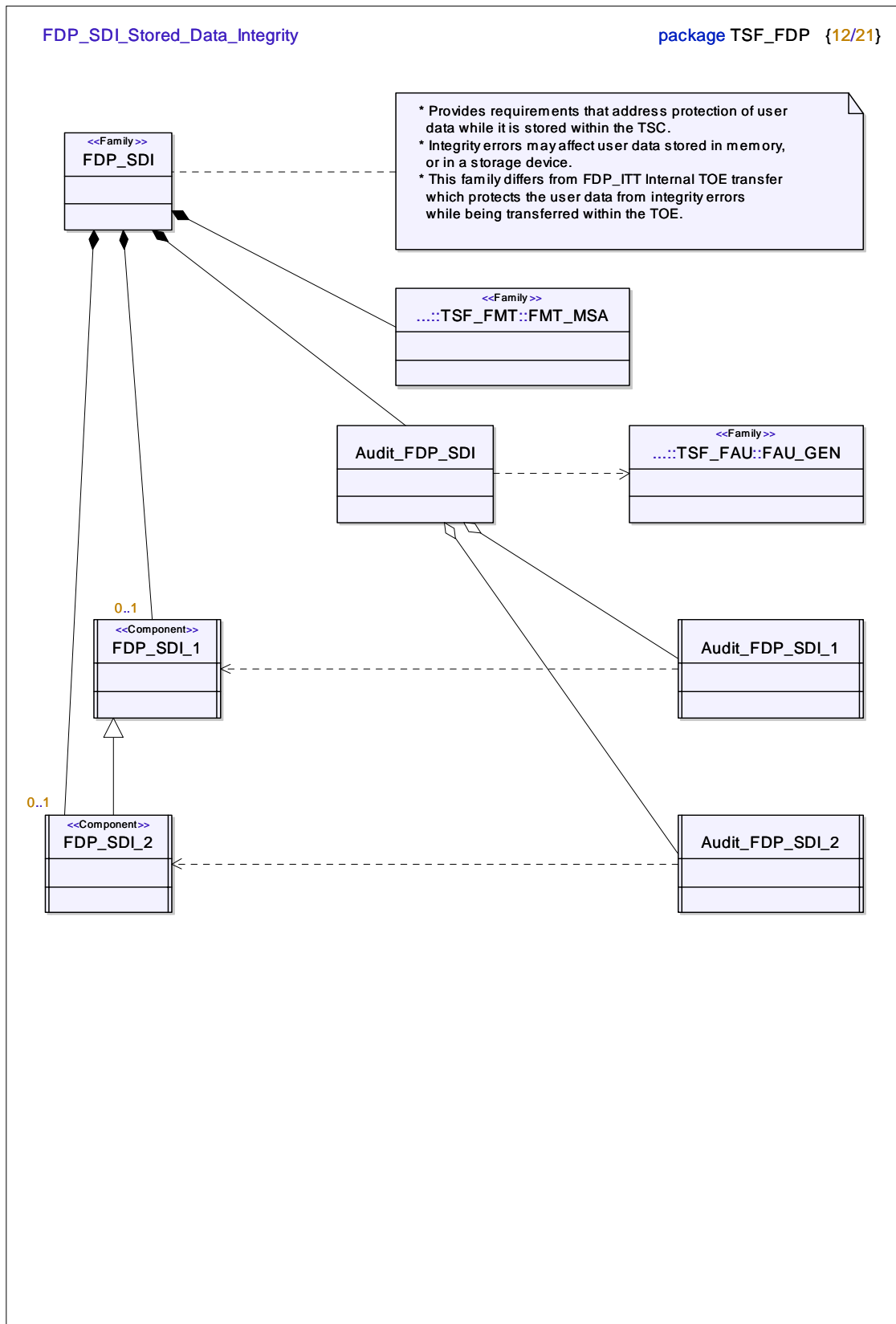


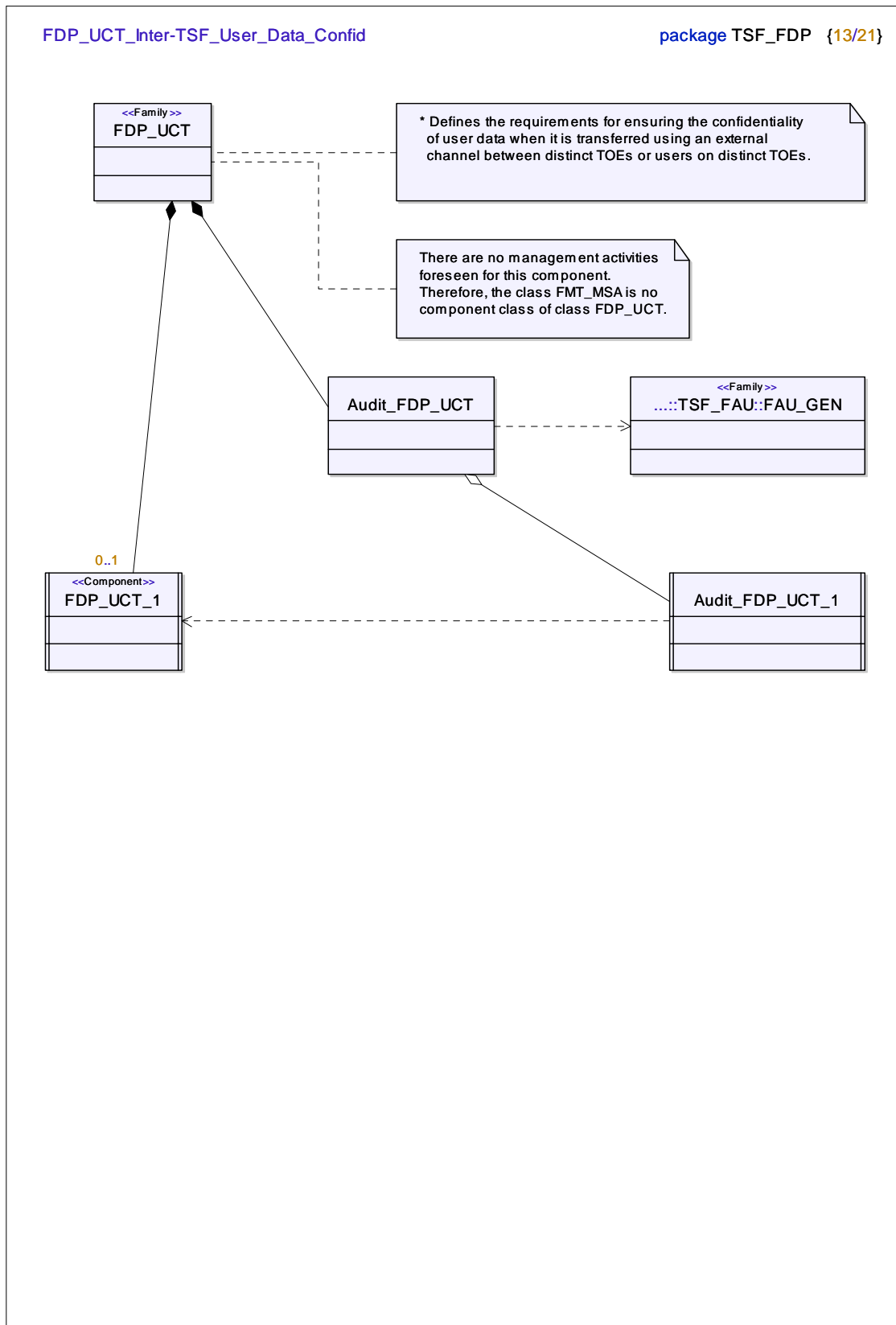


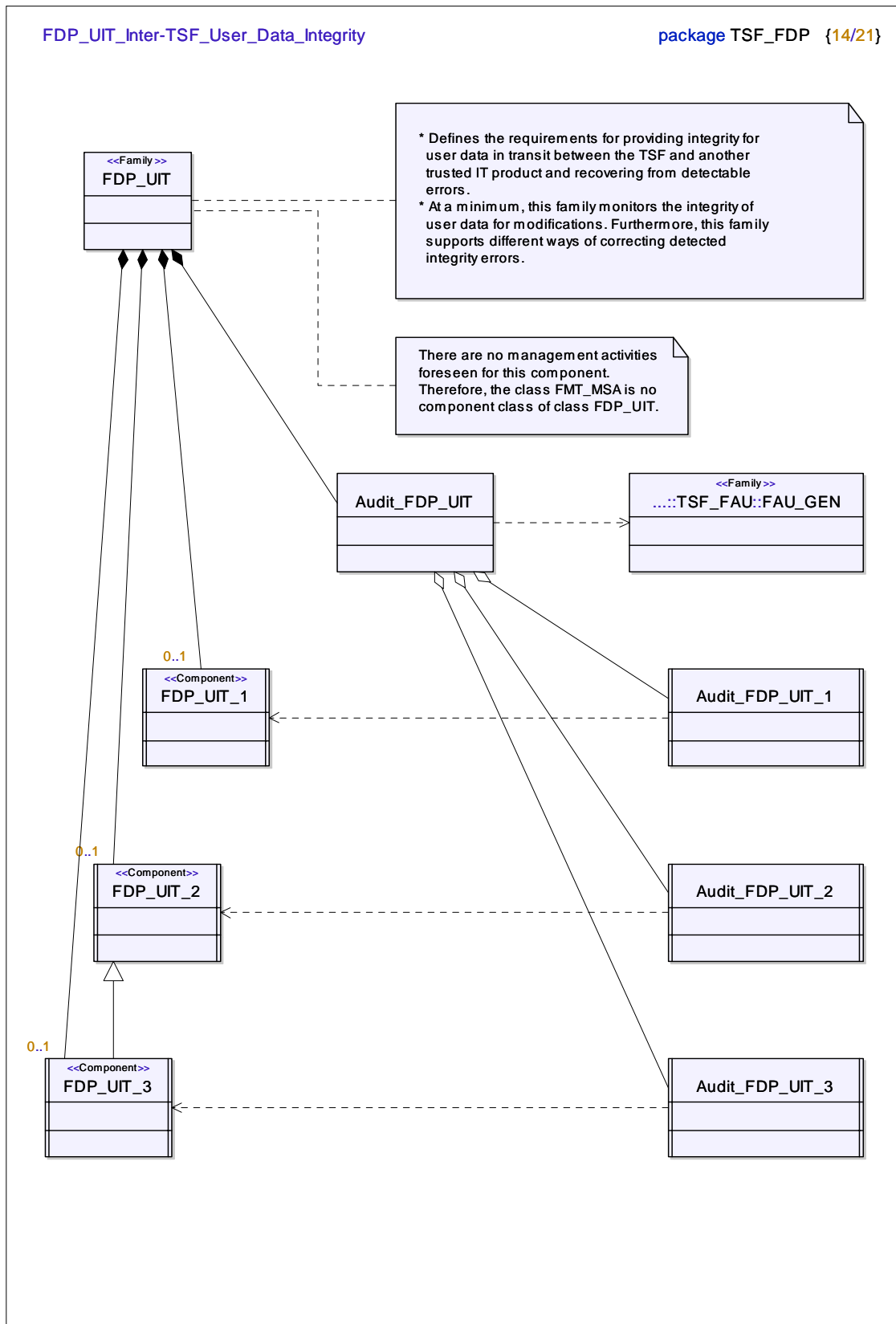


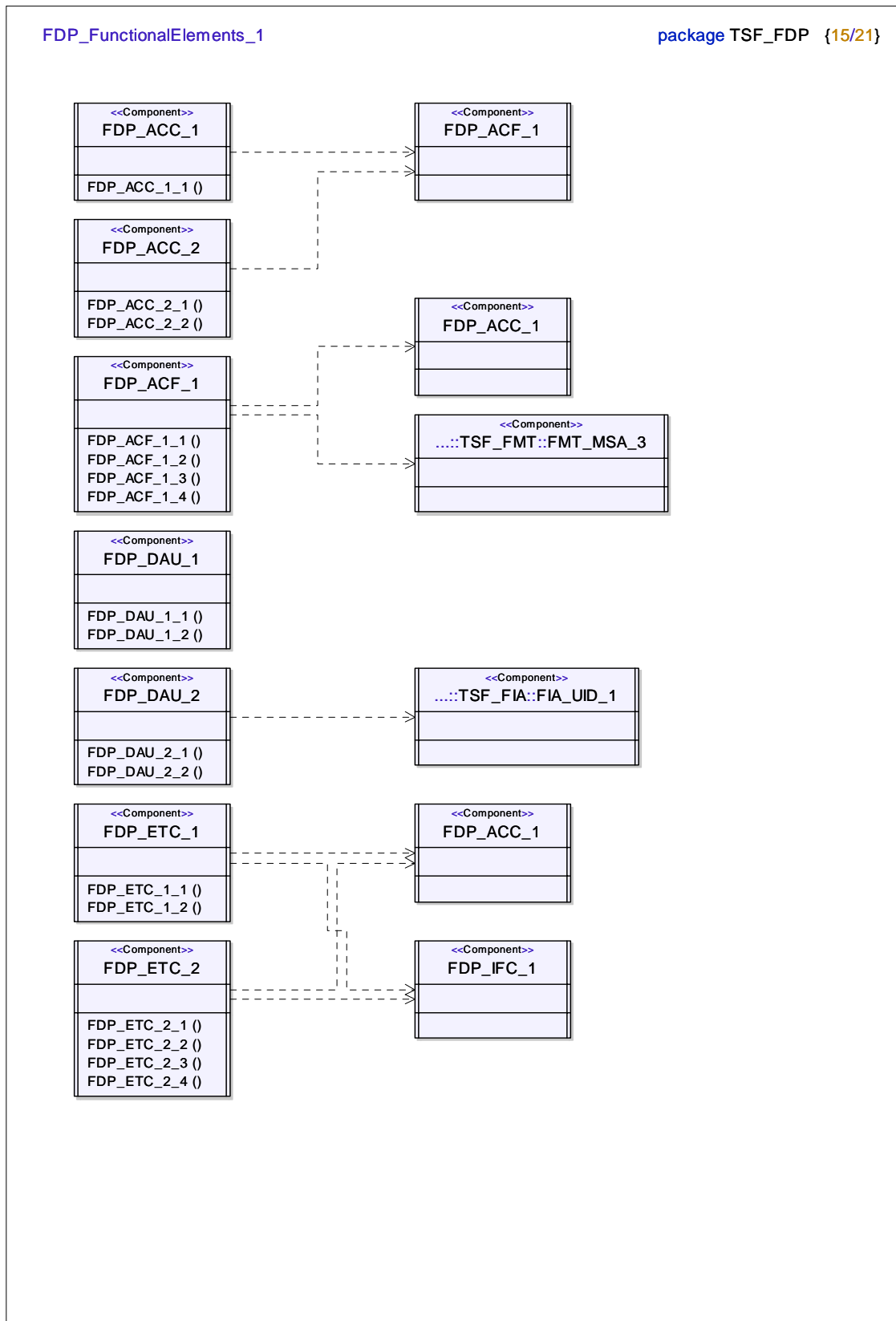


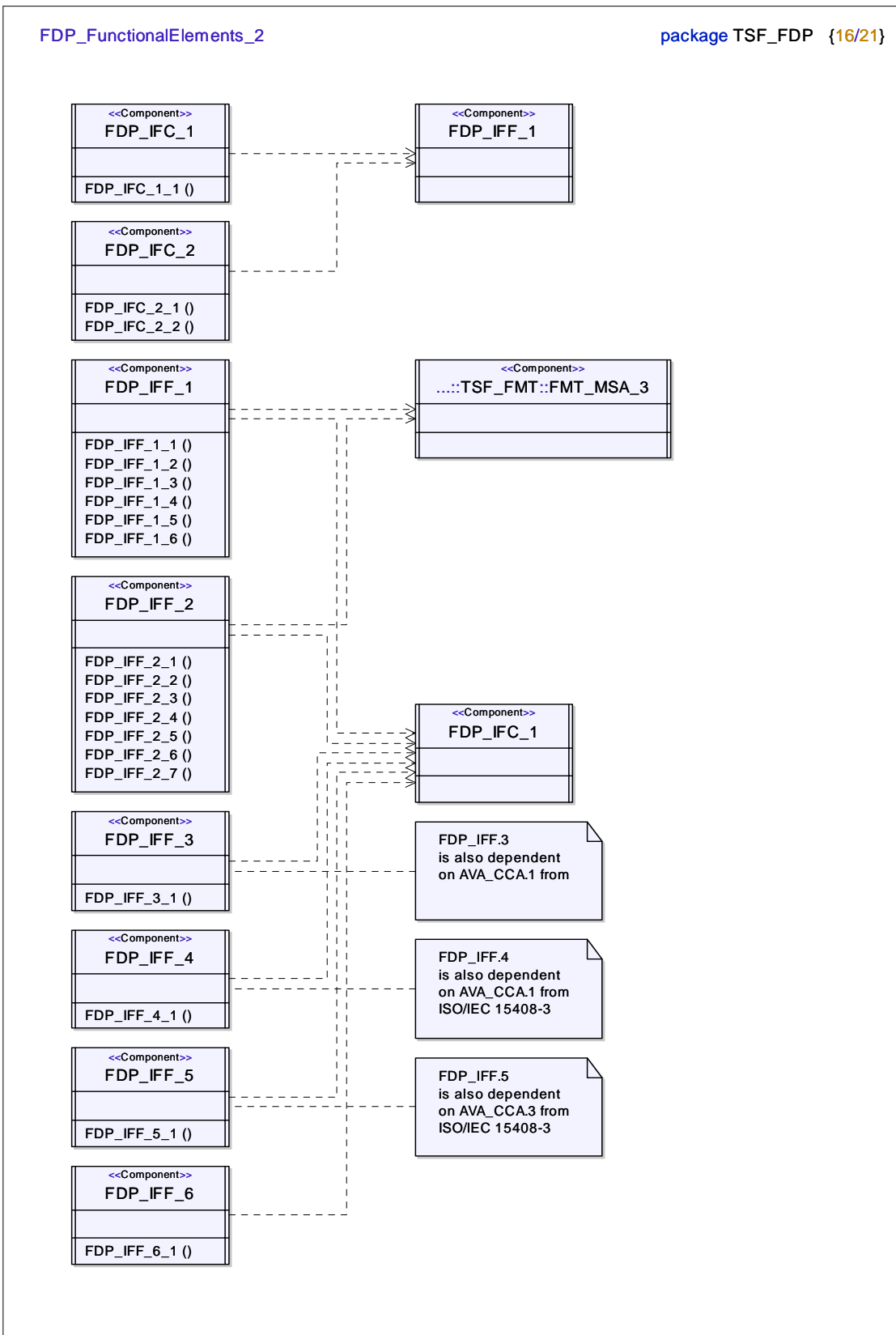


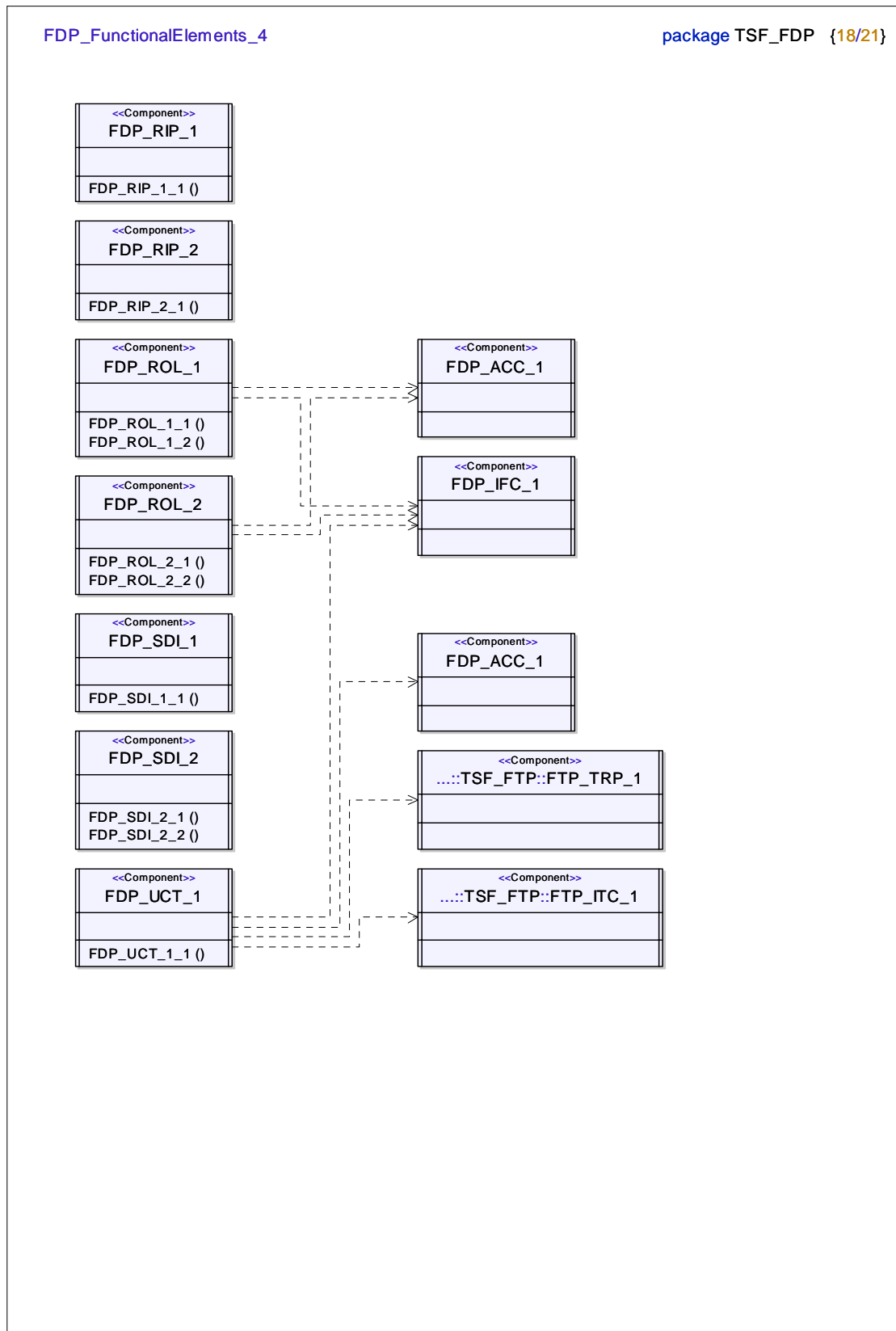


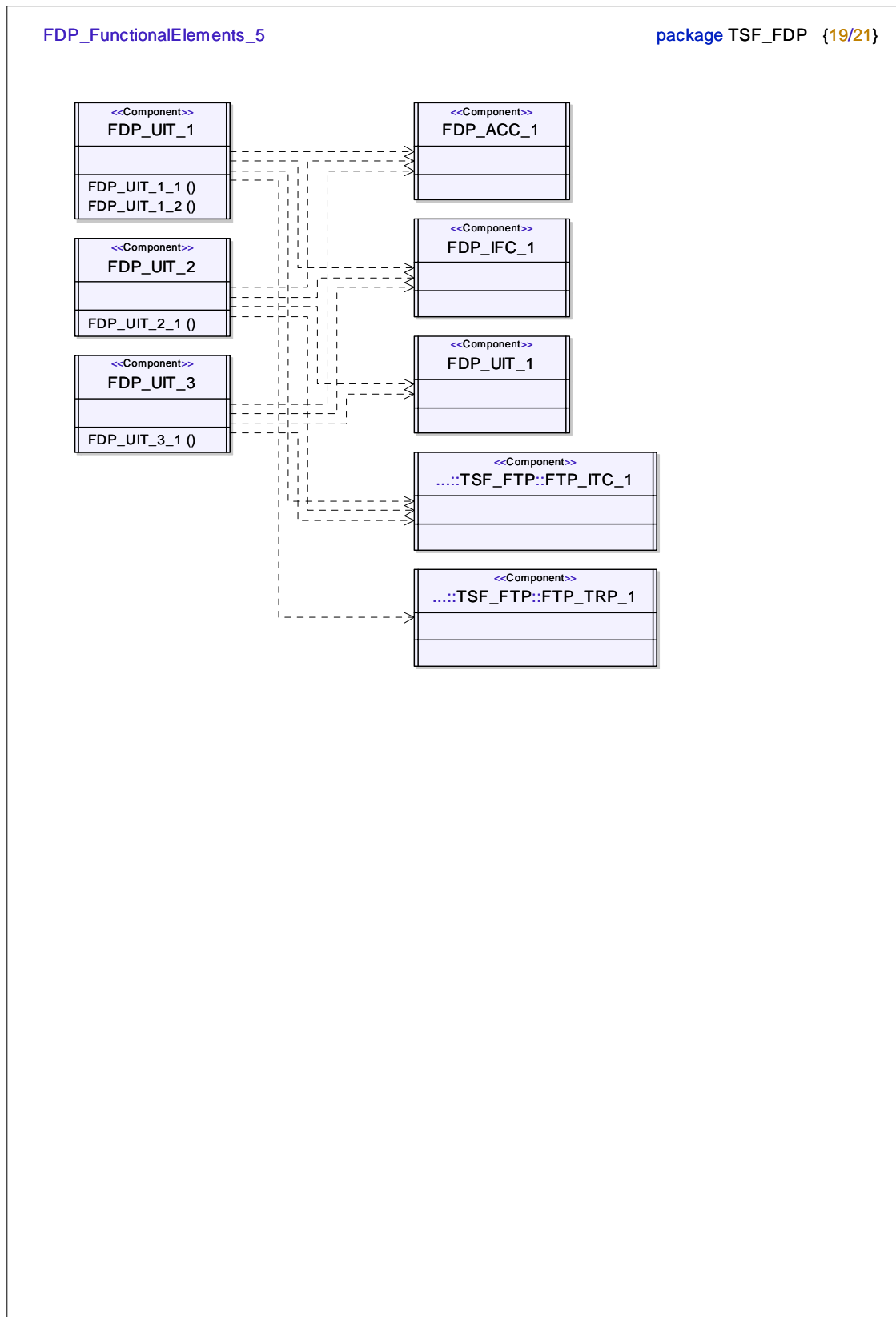












FDP_AuditEvents_1

package TSF_FDP {20/21}

Audit_FDP_ACF_1
auSuccesReqOp () auAllReqOp () auSpecSecAttr ()

Audit_FDP_DAU_1
auSuccesGenrValidEvid () auNoSuccesGenrValidEvid () auIDReqEvid ()

Audit_FDP_DAU_2
auSuccesGenrValidEvid () auNoSuccesGenrValidEvid () auIDReqEvid ()

Audit_FDP_ETC_1
auSuccesInfoExprt () auAllEprtAttmpt ()

Audit_FDP_ETC_2
auSuccesInfoExprt () auAllEprtAttmpt ()

Audit_FDP_IFF_1
auDecsnPermitInfoFlow () auAllDecsnReqInfoFlow () auSpecSecAttrInfoFlow () auSpecInfoSubset ()

Audit_FDP_IFF_2
auDecsnPermitInfoFlow () auAllDecsnReqInfoFlow () auSpecSecAttrInfoFlow () auSpecInfoSubset ()

Audit_FDP_IFF_3
auDecsnPermitInfoFlow () auAllDecsnReqInfoFlow () auUseIllicitInfoCH () auSpecSecAttrInfoFlow () auSpecInfoSubset () auUseIllicitCHExcdCapcty ()

Audit_FDP_IFF_4
auAllDecsnReqInfoFlow () auAllDecsnReqInfoFlow () auUseIllicitInfoCH () auSpecSecAttrInfoFlow () auSpecInfoSubset () auUseIllicitCHExcdCapcty ()

Audit_FDP_IFF_5
auDecsnPermitInfoFlow () auAllDecsnReqInfoFlow () auSpecSecAttrInfoFlow () auSpecInfoSubset ()

Audit_FDP_IFF_6
auDecsnPermitInfoFlow () auAllDecsnReqInfoFlow () auUseIllicitInfoCH () auSpecSecAttrInfoFlow () auSpecInfoSubset () auUseIllicitCHExcdCapcty ()

Audit_FDP_ITC_1
auSuccesImprtUserData () auAllAtmptImprtUserData () auSpecSecAttrImprt ()

Audit_FDP_ITC_2
auSuccesImprtUserData () auAllAtmptImprtUserData () auSpecSecAttrImprt ()

FDP_AuditEvents_2

package TSF_FDP {21/21}

Audit_FDP_ITT_1
auSuccesXferUsrData () auAllAtmptXferUsrData ()

Audit_FDP_ITT_2
auSuccesXferUsrData () auAllAtmptXferUsrData ()

Audit_FDP_ITT_3
auSuccesXferUsrData () auAllAtmptXferUsrData () auUnauthAtmptIntegrtyMthod () auActnOnIntegrtyErr ()

Audit_FDP_ITT_4
auSuccesXferUsrData () auAllAtmptXferUsrData () auUnauthAtmptIntegrtyMthod () auActnOnIntegrtyErr ()

Audit_FDP_ROL_1
auAllRollbck () auAllRollbckAtmpt () auAllRollbckAtmptOpType ()

Audit_FDP_ROL_2
auAllRollbck () auAllRollbckAtmpt () auAllRollbckAtmptOpType ()

Audit_FDP_SDI_1
auSuccesIntgrtyChckAtmpt () auAllIntgrtyChckAtmpt () auIntgrtyErrorType ()

Audit_FDP_SDI_2
auSuccesIntgrtyChckAtmpt () auAllIntgrtyChckAtmpt () auIntgrtyErrorType () auActnOnIntgrtyError ()

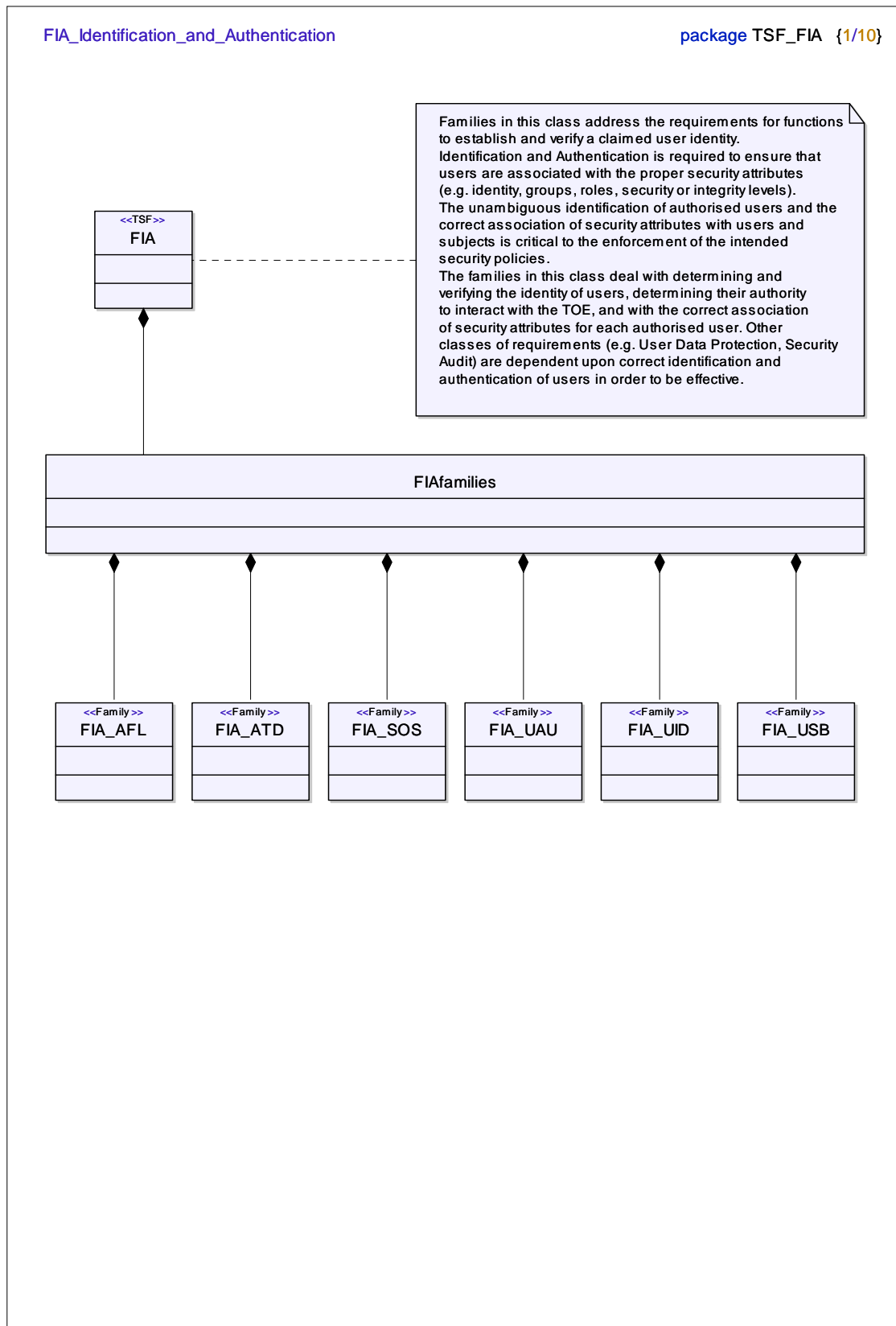
Audit_FDP_UCT_1
auIDUsrDataExchng () auIDUnauthUsr () AuRef2InfoUsrData ()

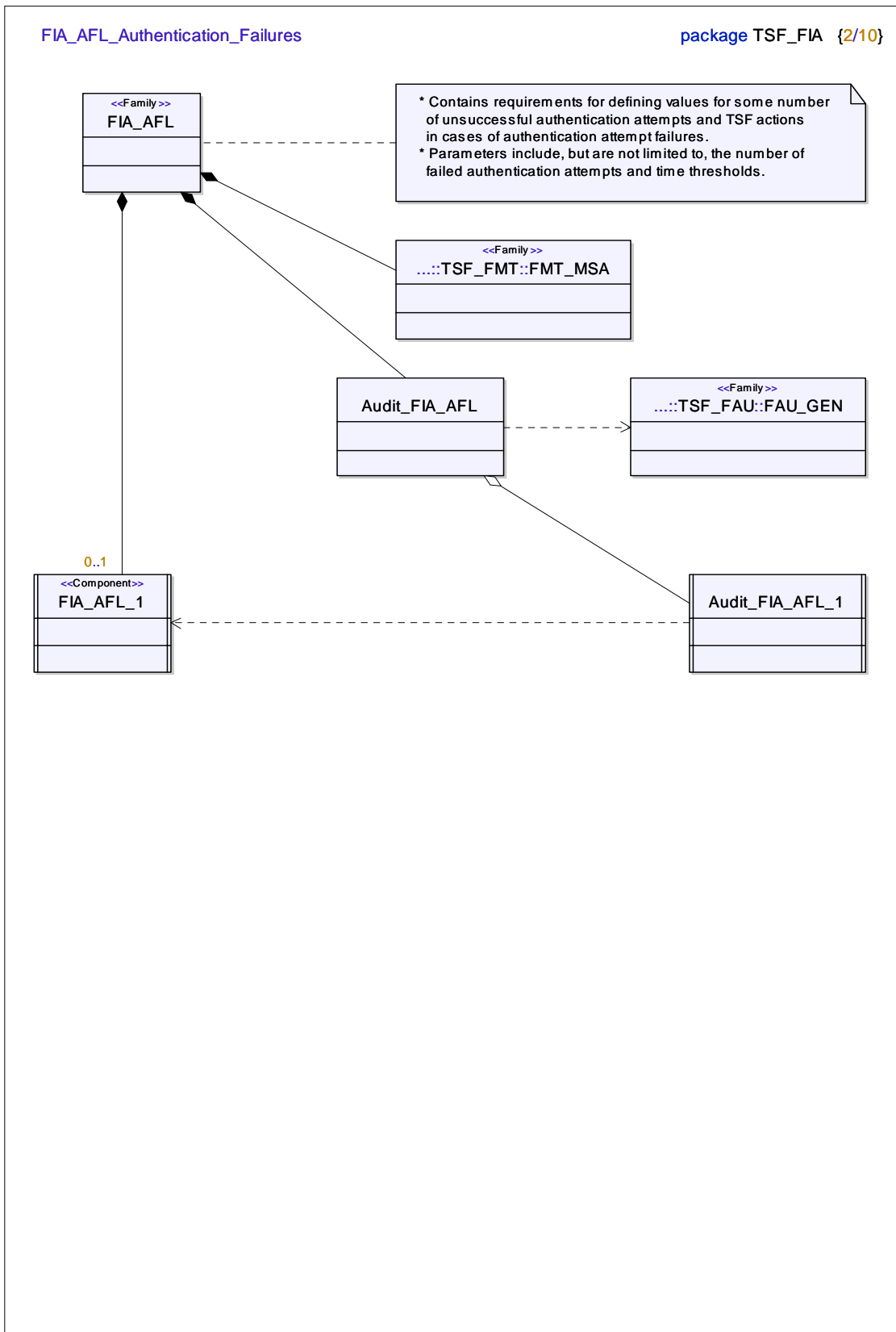
Audit_FDP_UIT_1
auIDUsrDataExchng () auIDUsrDataExchngAtmpt () auRef2InfoUsrData () auAtmptBlockXfer () auModifUsrDataType ()

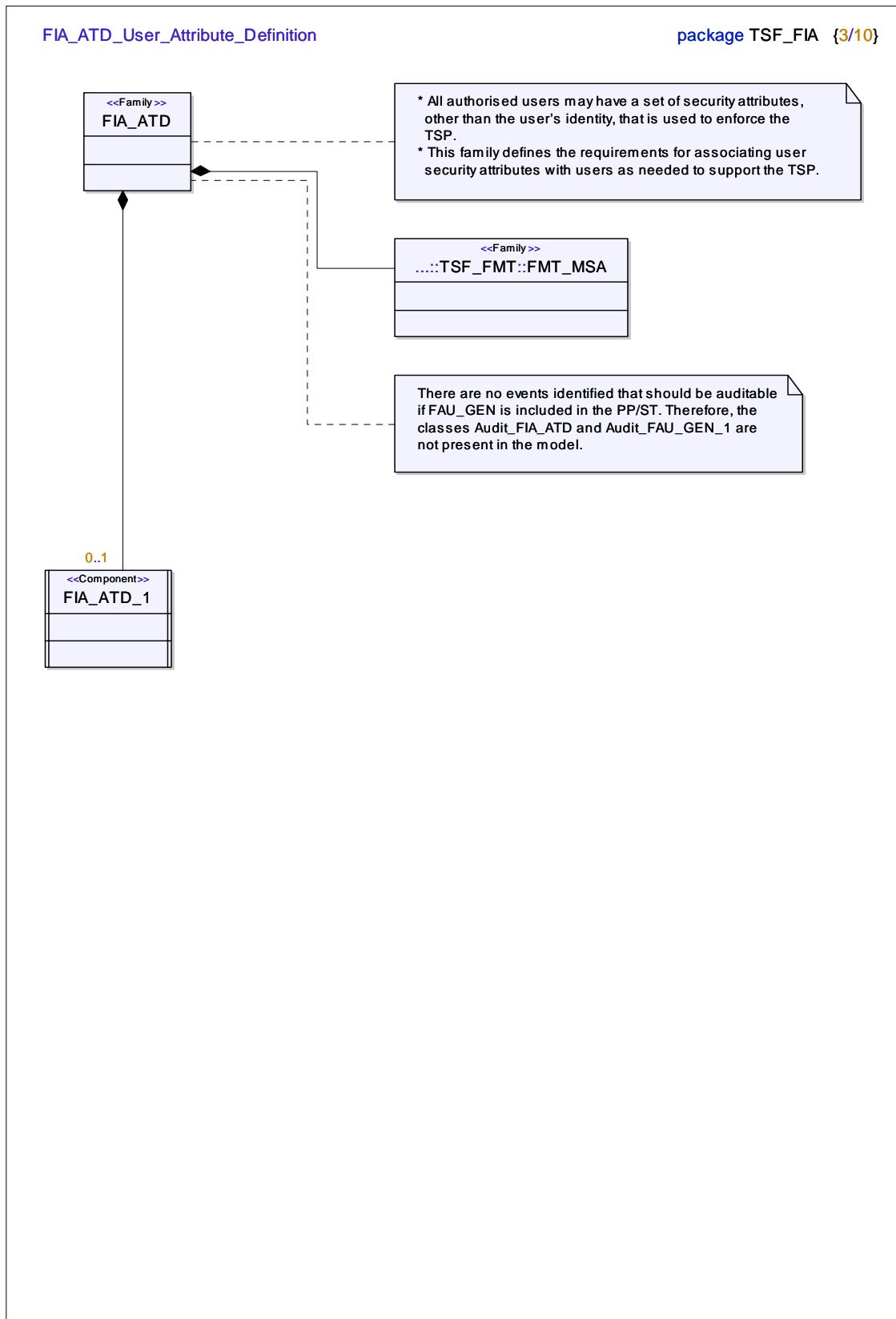
Audit_FDP_UIT_2
auIDUsrDataExchng () auSuccesErrorRecovery () auIDUsrDataExchngAtmpt () auRef2InfoUsrData () auAtmptBlockXfer () auModifUsrDataType ()

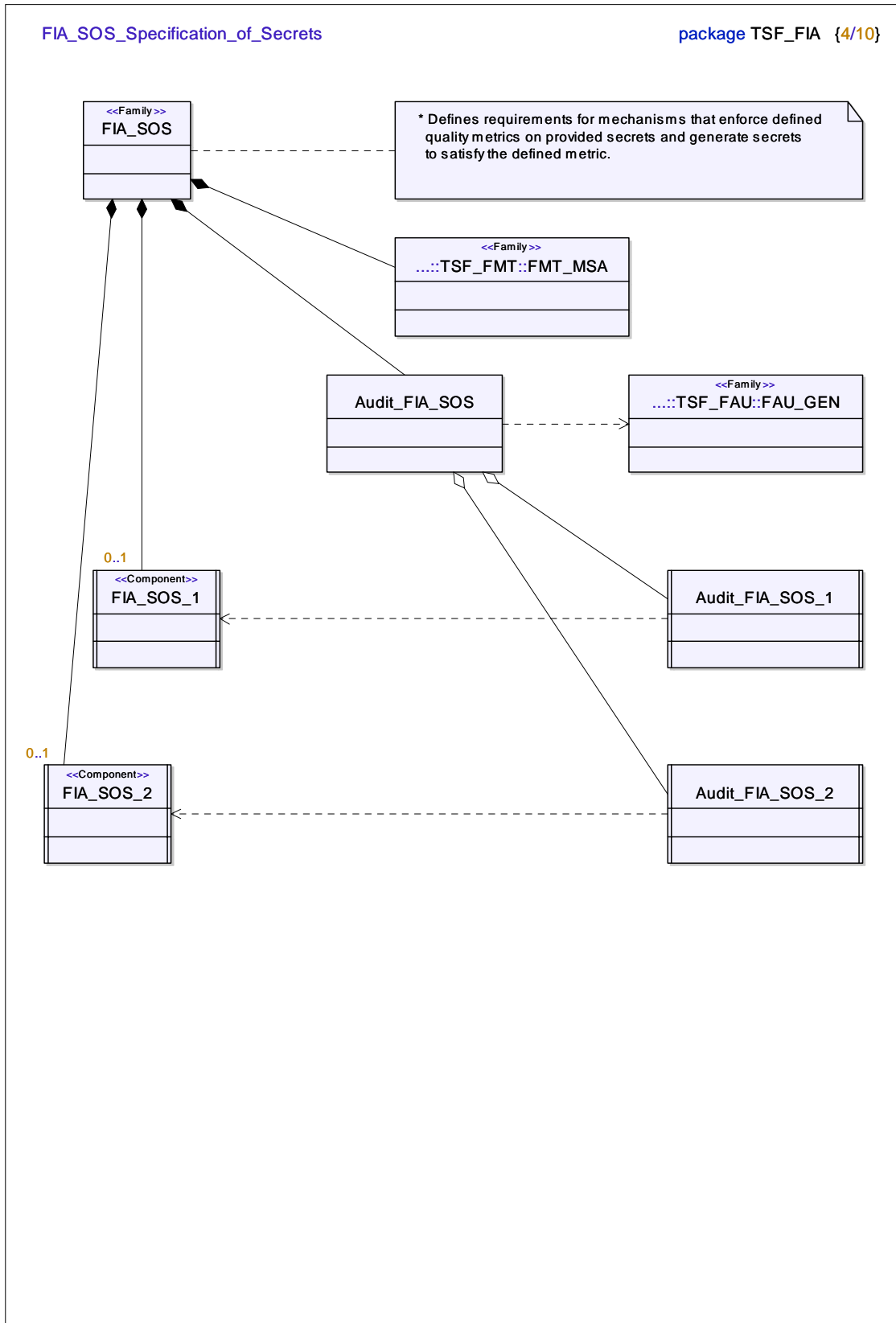
Audit_FDP_UIT_3
auIDUsrDataExchng () auSucces () auIDUsrDataExchngAtmpt () auRef2InfoUsrData () auAtmptBlockXfer () auModifUsrDataType ()

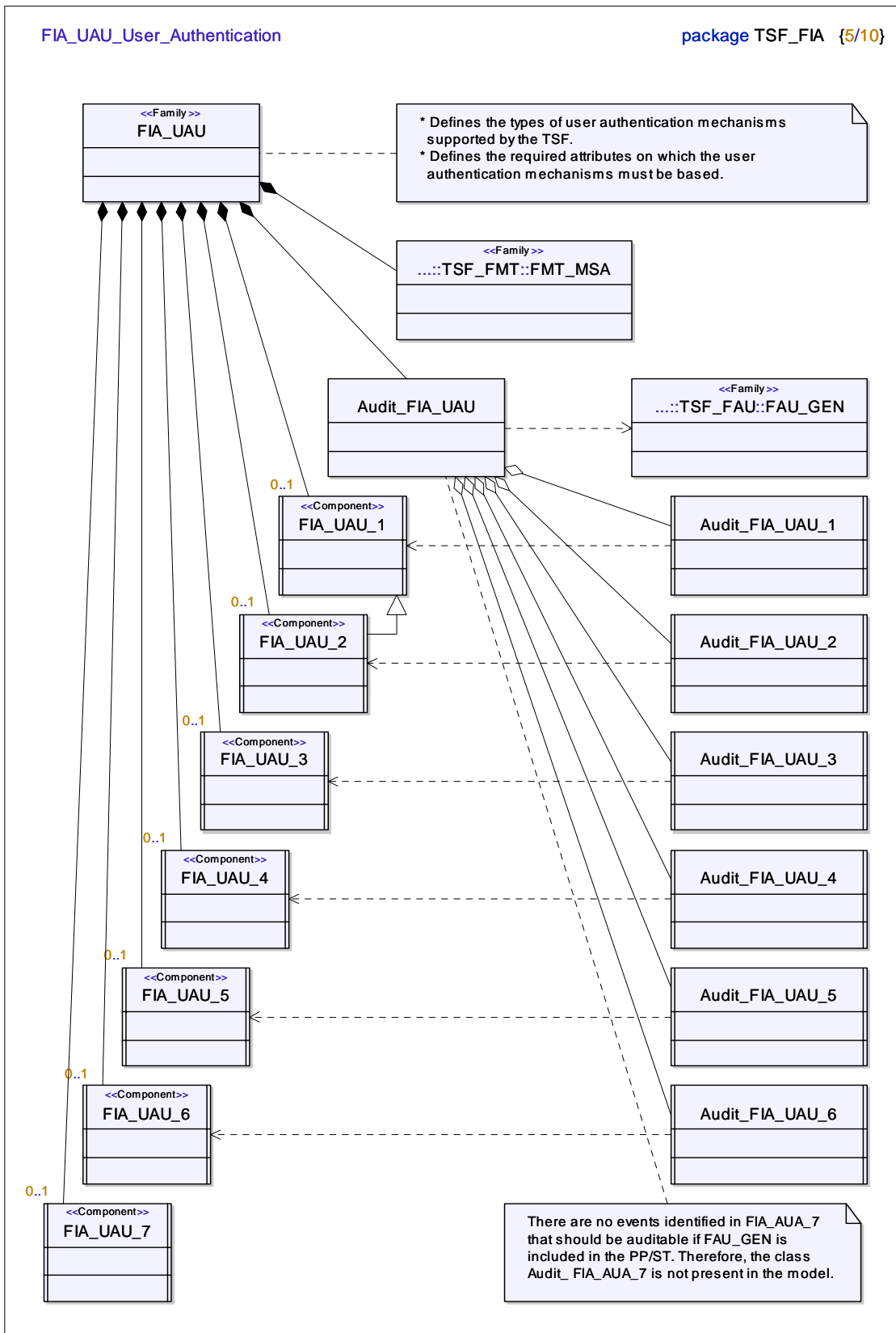
A.3.5 Package TSF_FIA

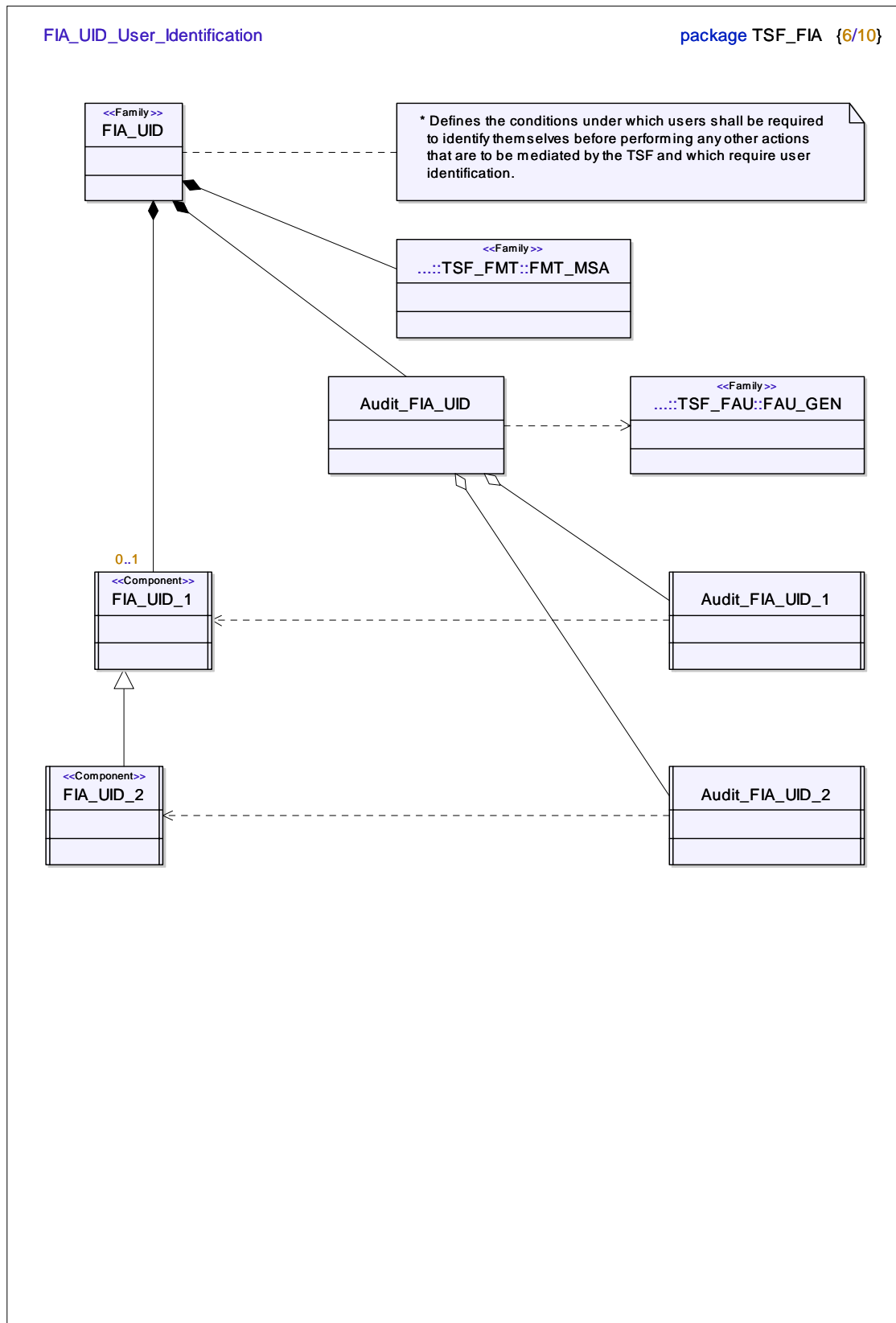


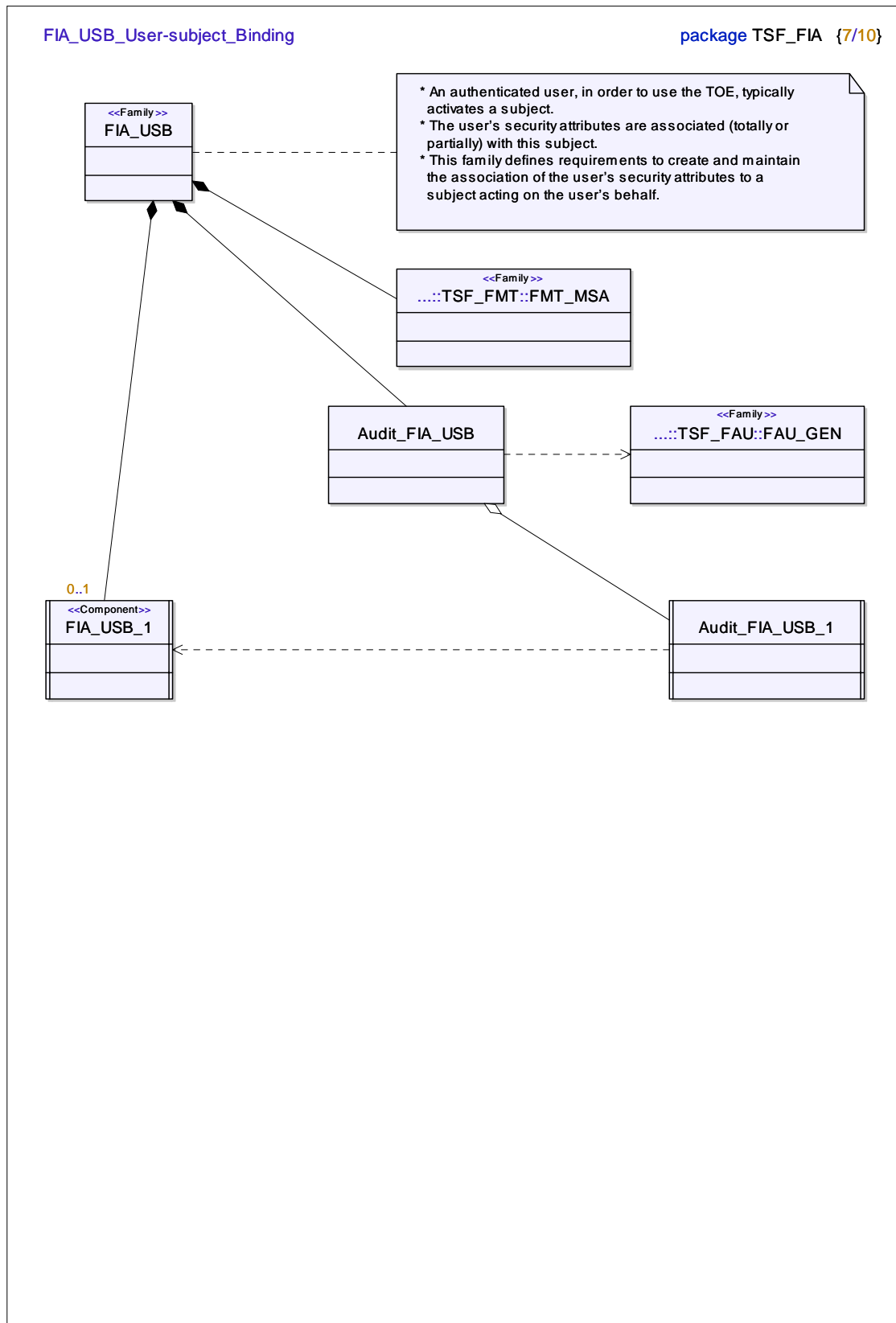


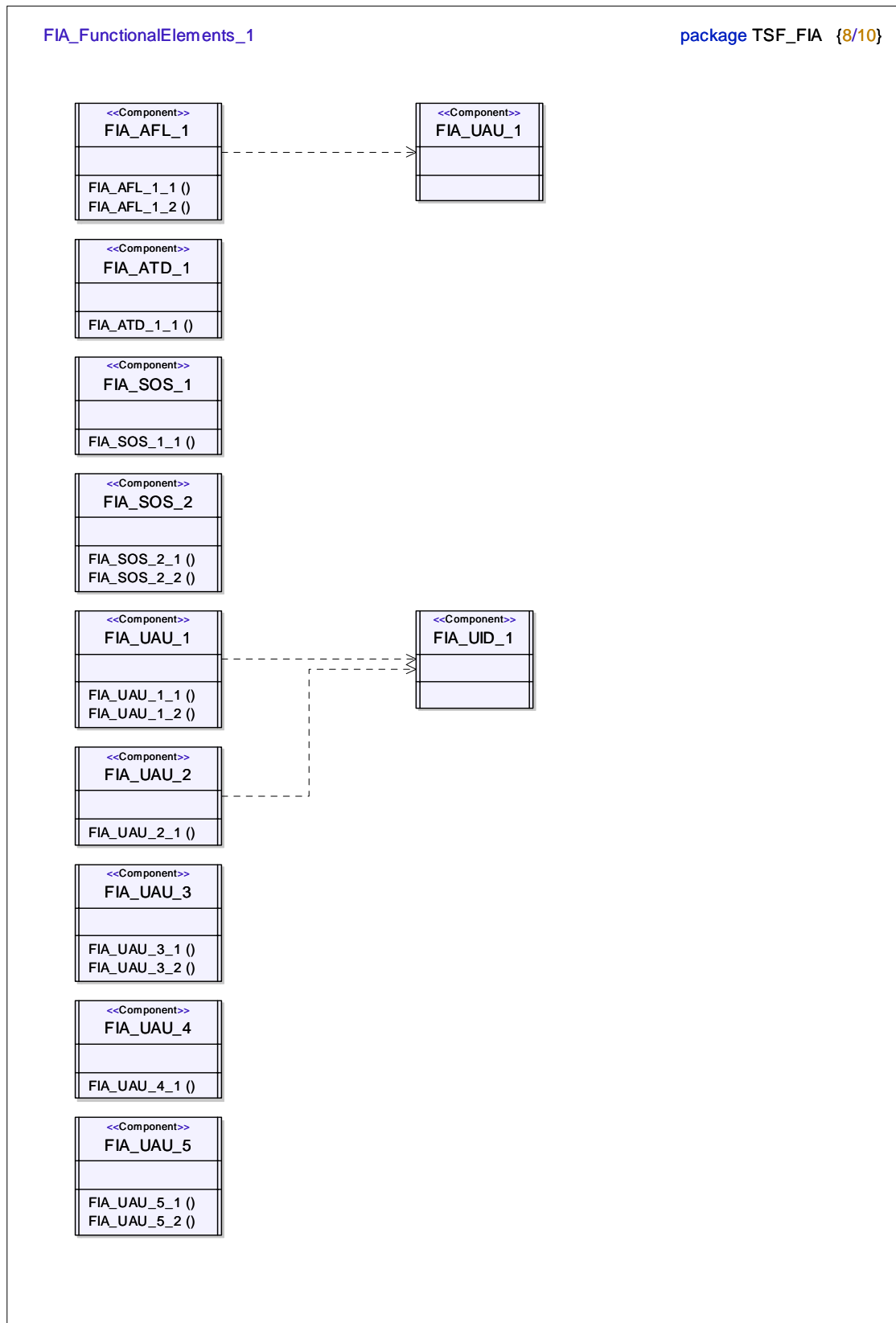


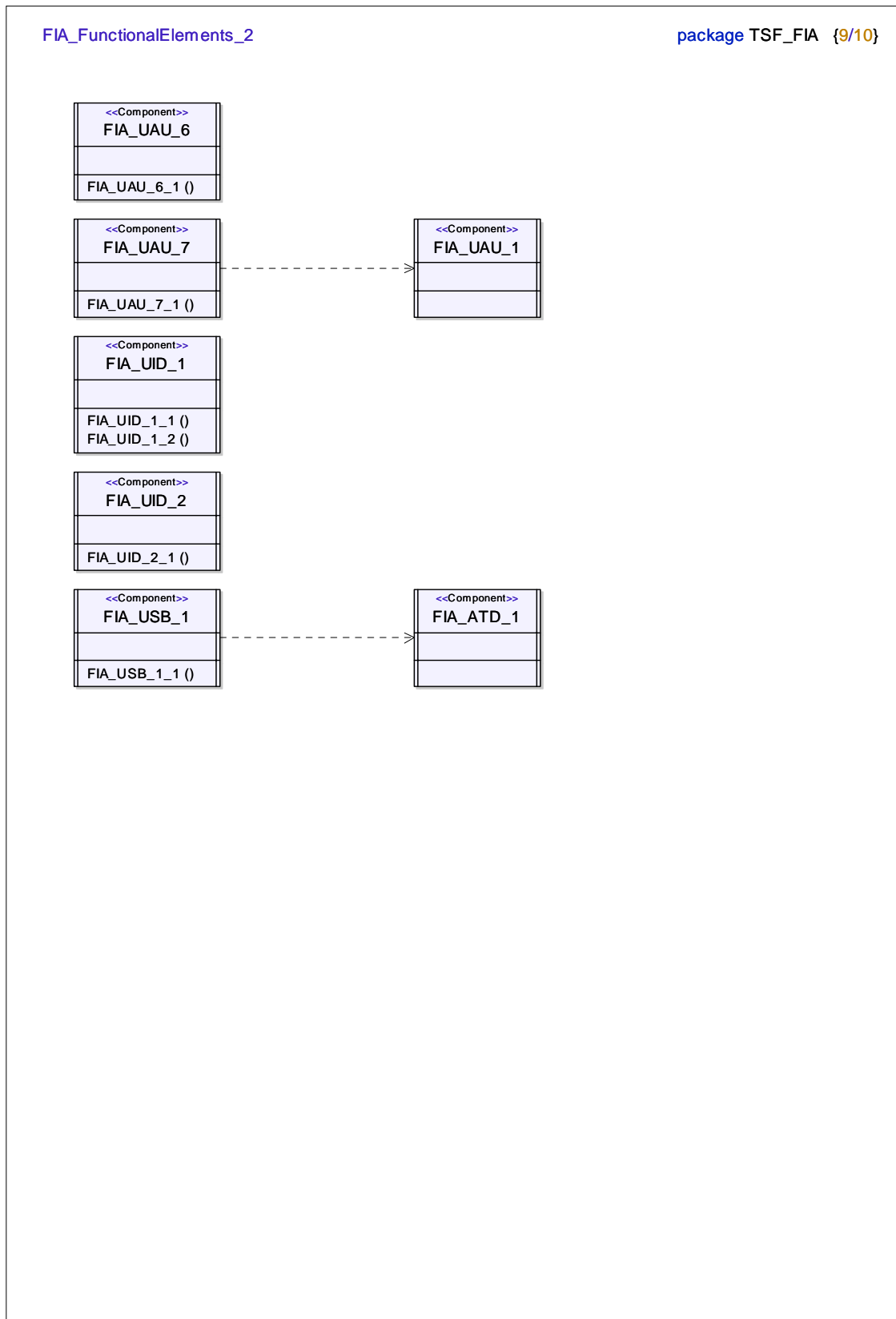












FIA_AuditEvents

package TSF_FIA {10/10}

Audit_FIA_AFL_1
auThrshUnsucAuthentAtmpt ()

Audit_FIA_SOS_1
auTestedSecretRjct () auTestedSecretAcptRjct () auDntifChngQualMetric ()

Audit_FIA_SOS_2
auTestedSecretRjct () auTestedSecretAcptRjct () auDntifChngQualMetric ()

Audit_FIA_UAU_1
auUnsuccUseAuthMech () auAllUseAuthMech () auAllActnBeforeAuth ()

Audit_FIA_UAU_2
auUnsuccUseAuthMech () auAllUseAuthMech ()

Audit_FIA_UAU_3
auDetctnFraudAuthData () auAllActnOnFraudAuthData ()

Audit_FIA_UAU_4
auAtmptReuseAuthData ()

Audit_FIA_UAU_5
auFinalDecsnOnAuth () auActvtdMechFinalDecsn ()

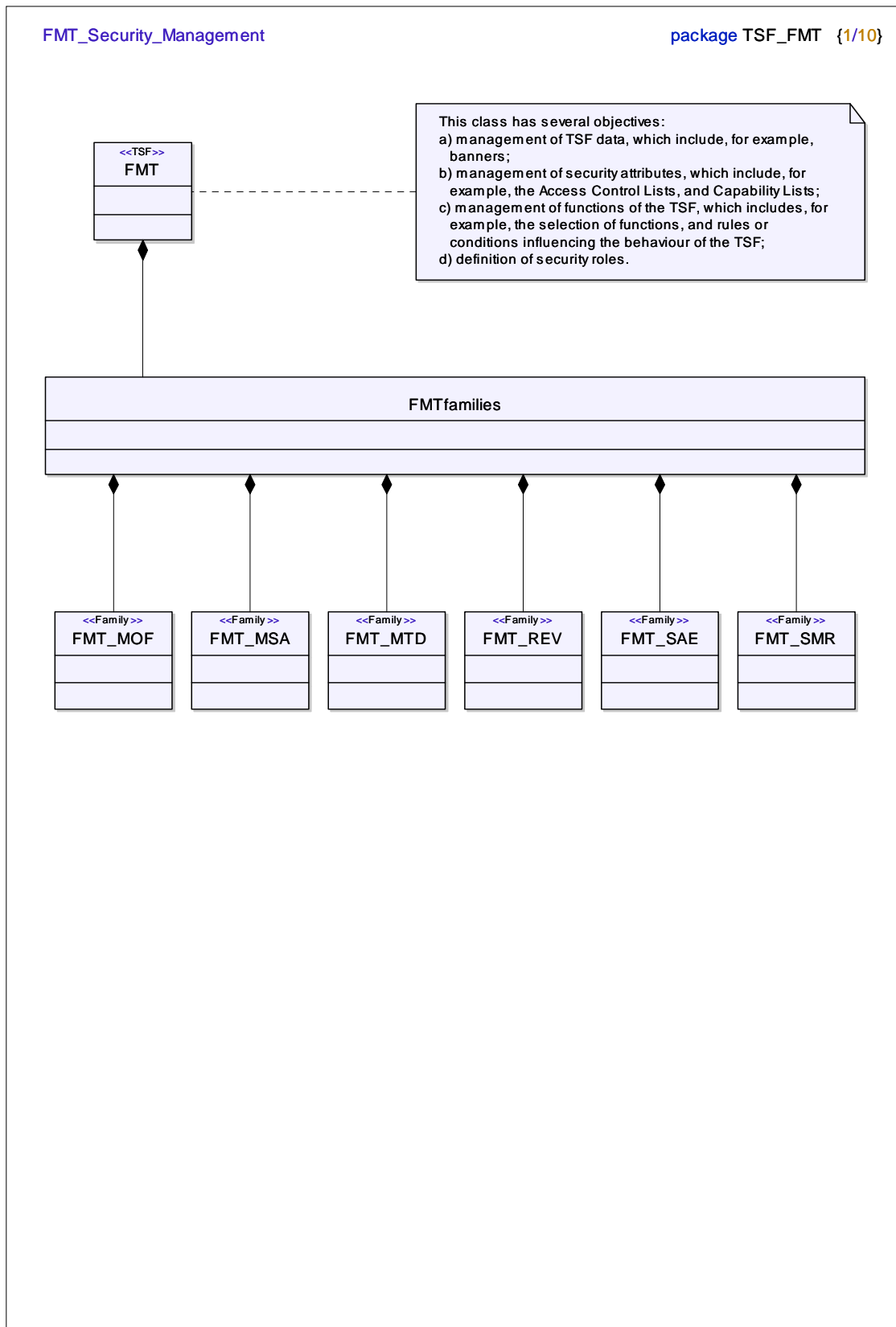
Audit_FIA_UAU_6
auAllReauthenticationAtmpt () auReauthenticationFailure ()

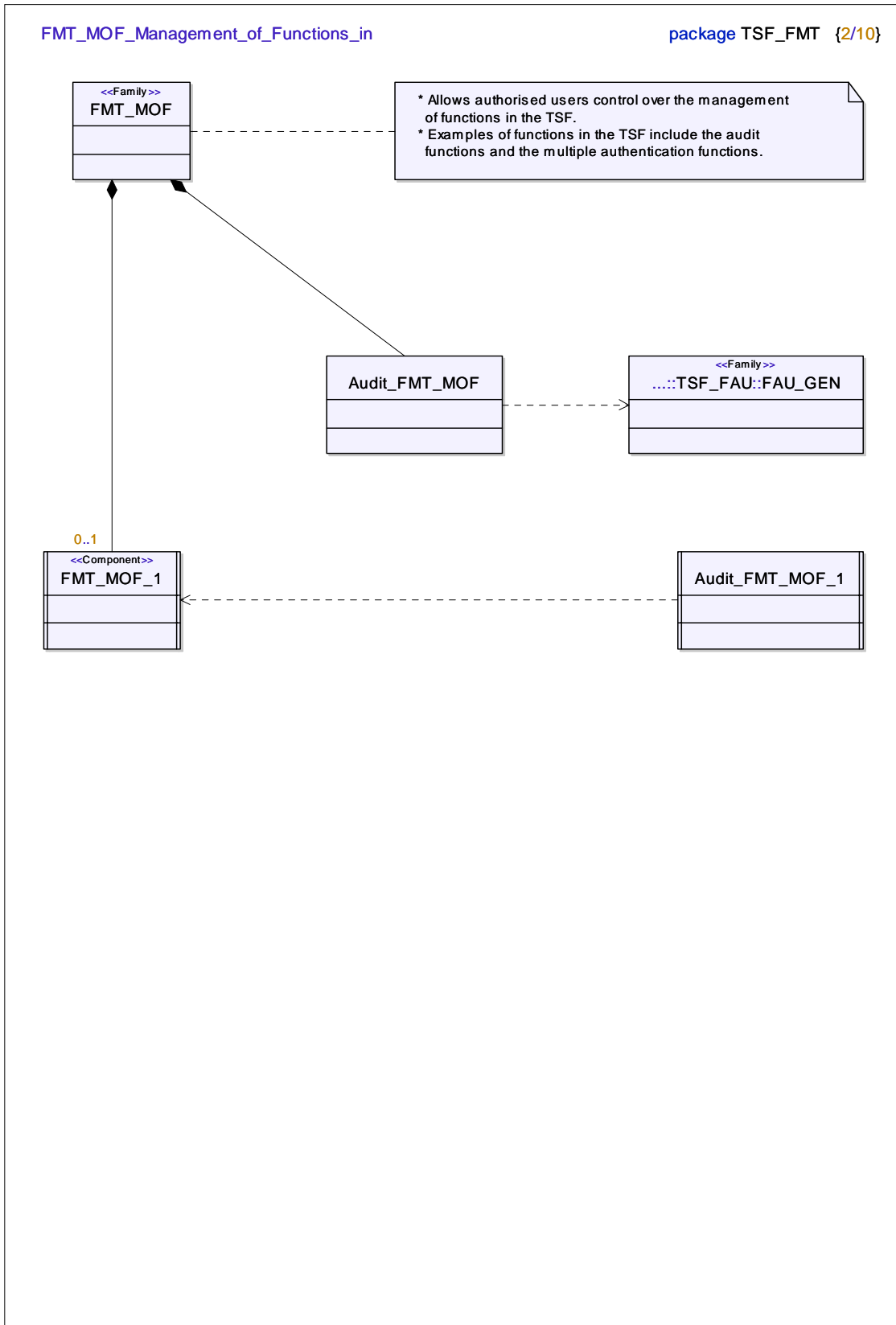
Audit_FIA_UID_1
auUnsuccUseUsrldntif () auAllUseUsrldntif ()

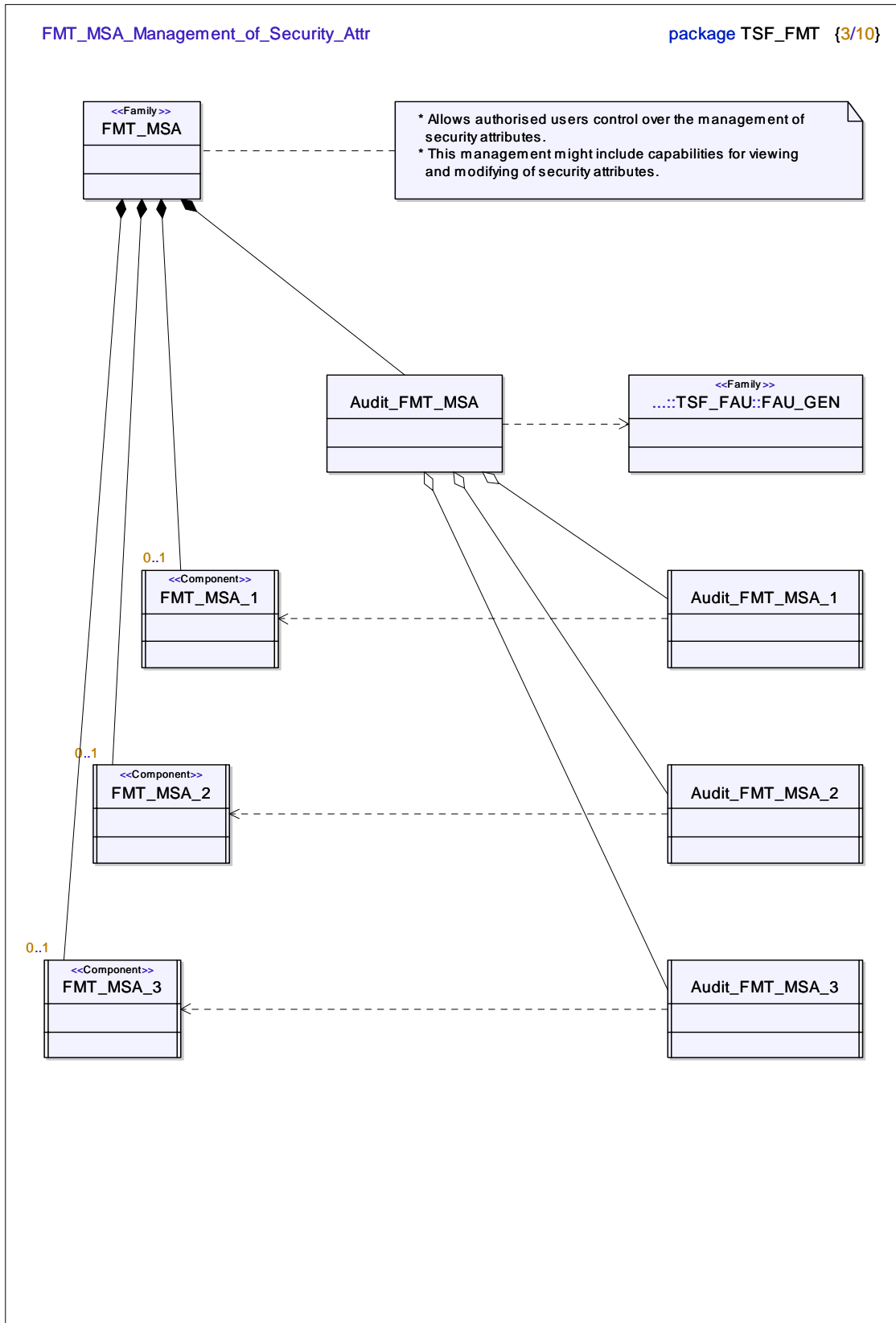
Audit_FIA_UID_2
auUnsuccUseUsrldntif () auAllUseUsrldntif ()

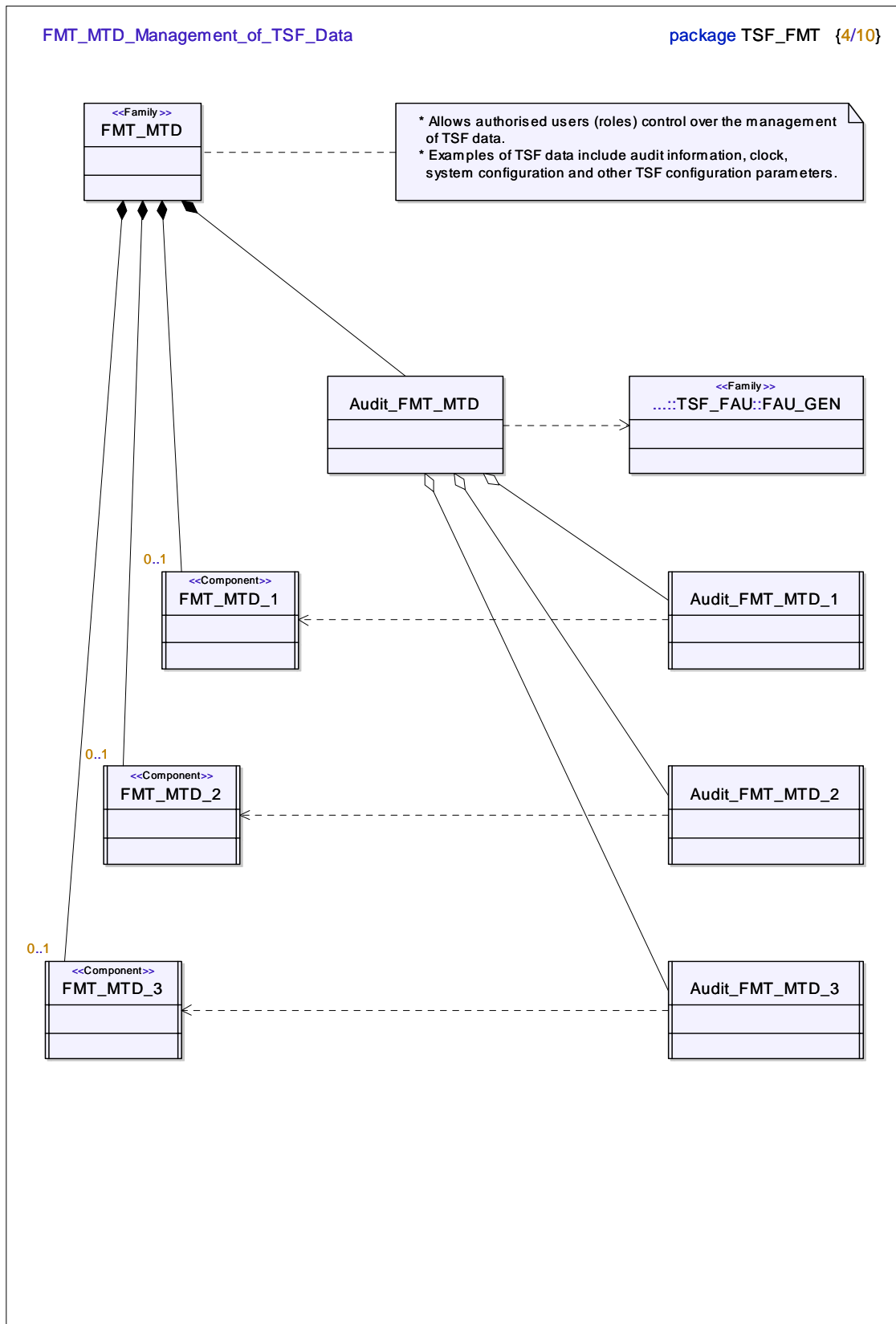
Audit_FIA_USB_1
auUnsuccBindUsrSecAttr () auBindUsrSecAttrSuccFail ()

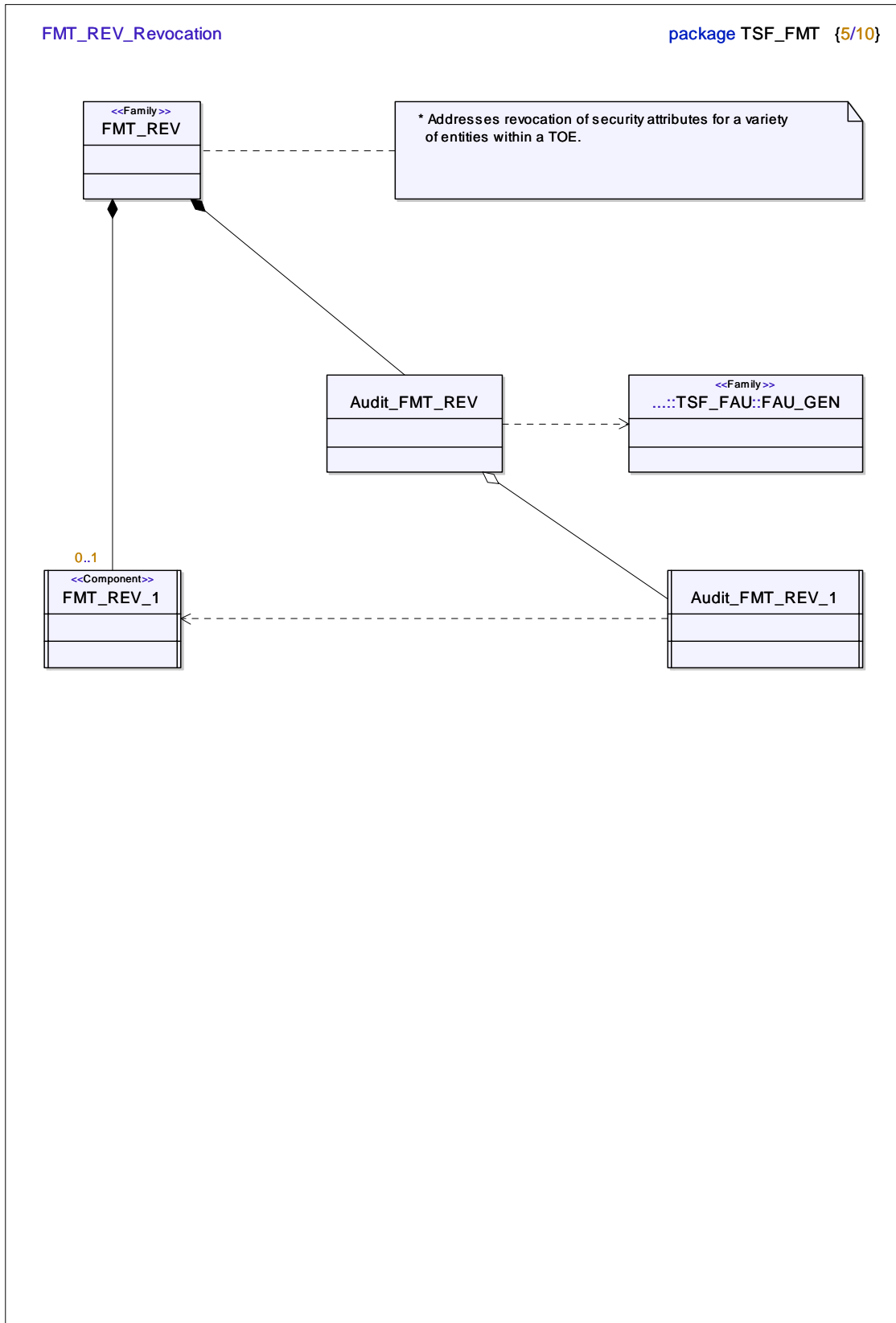
A.3.6 Package TSF_FMT

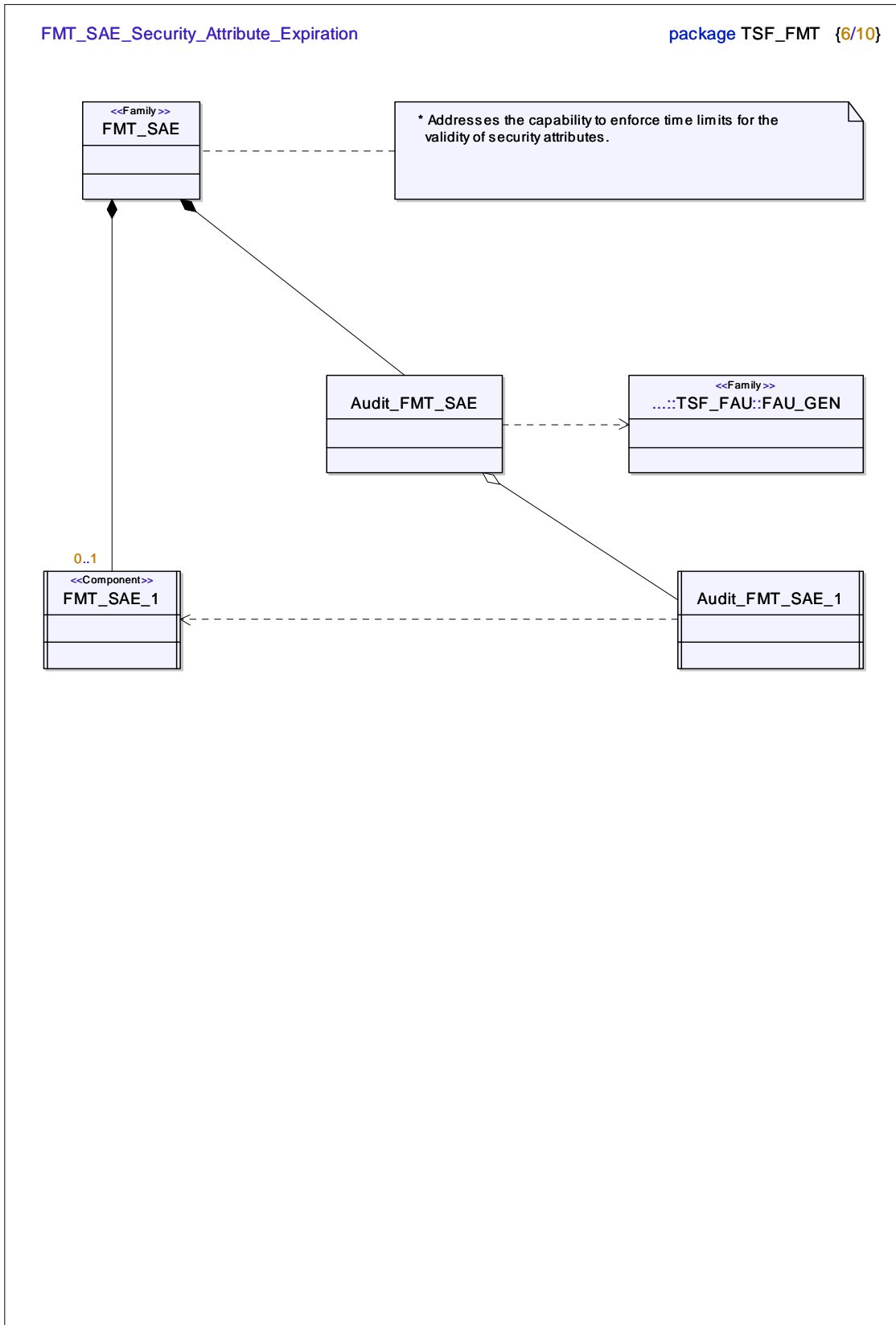


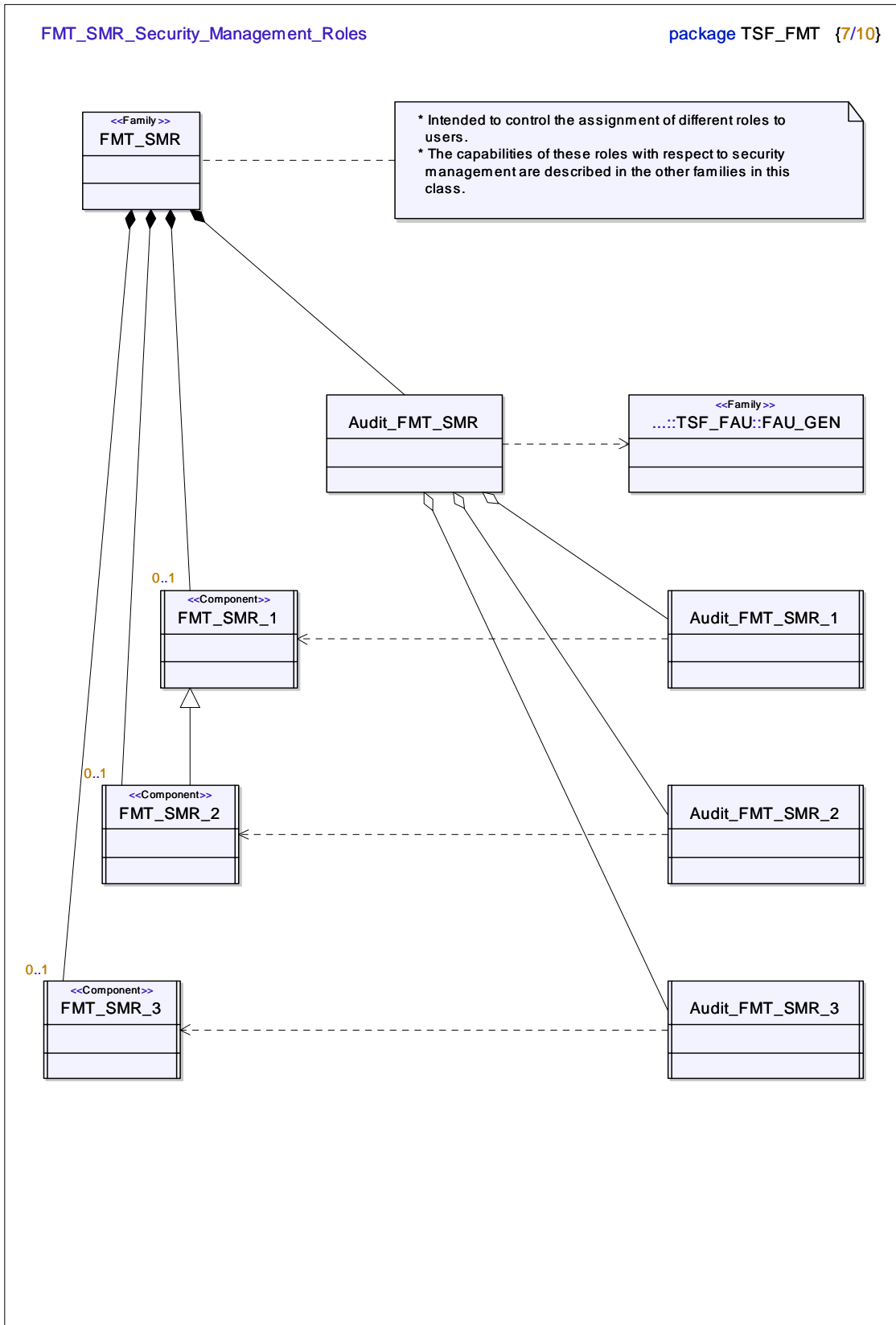


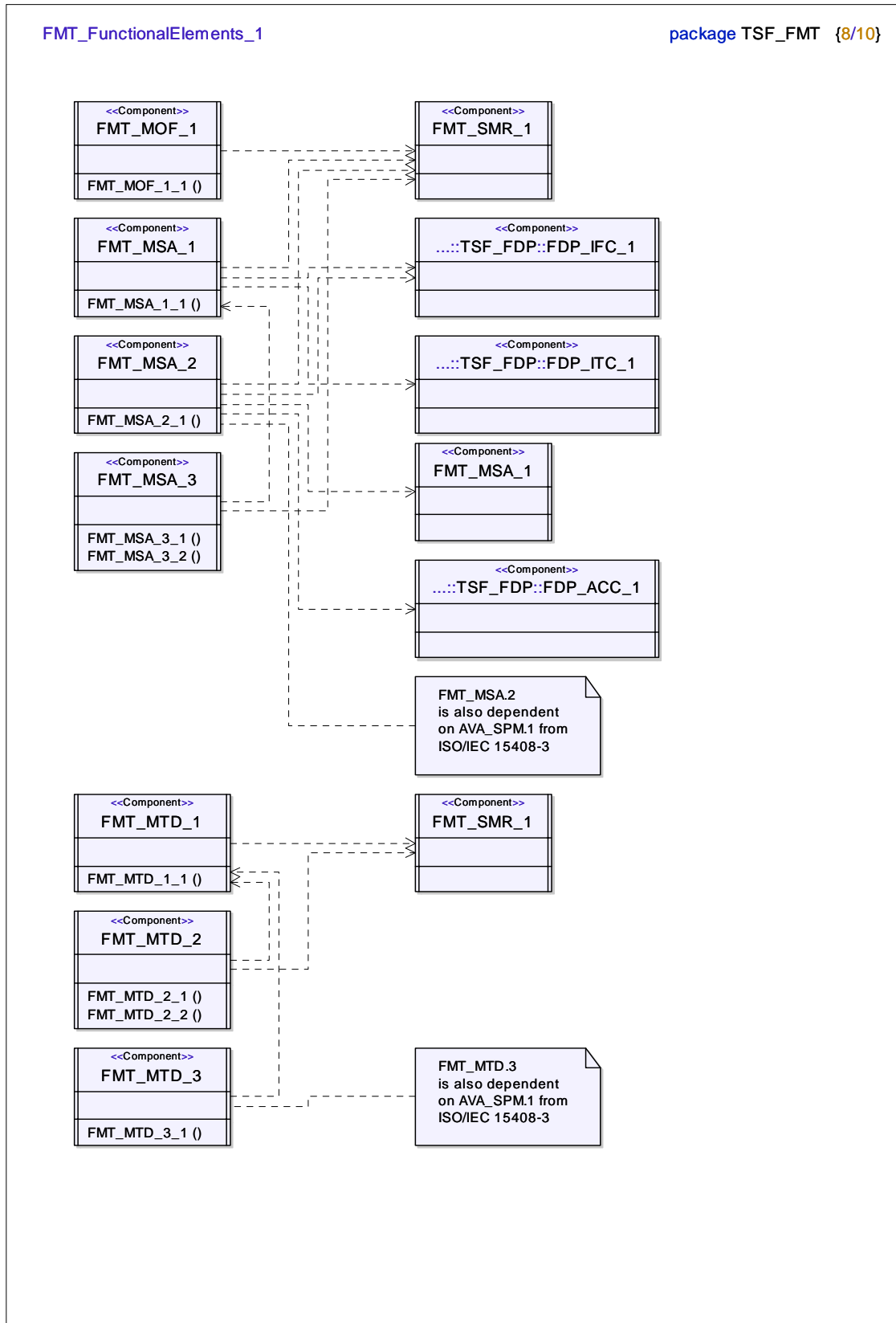


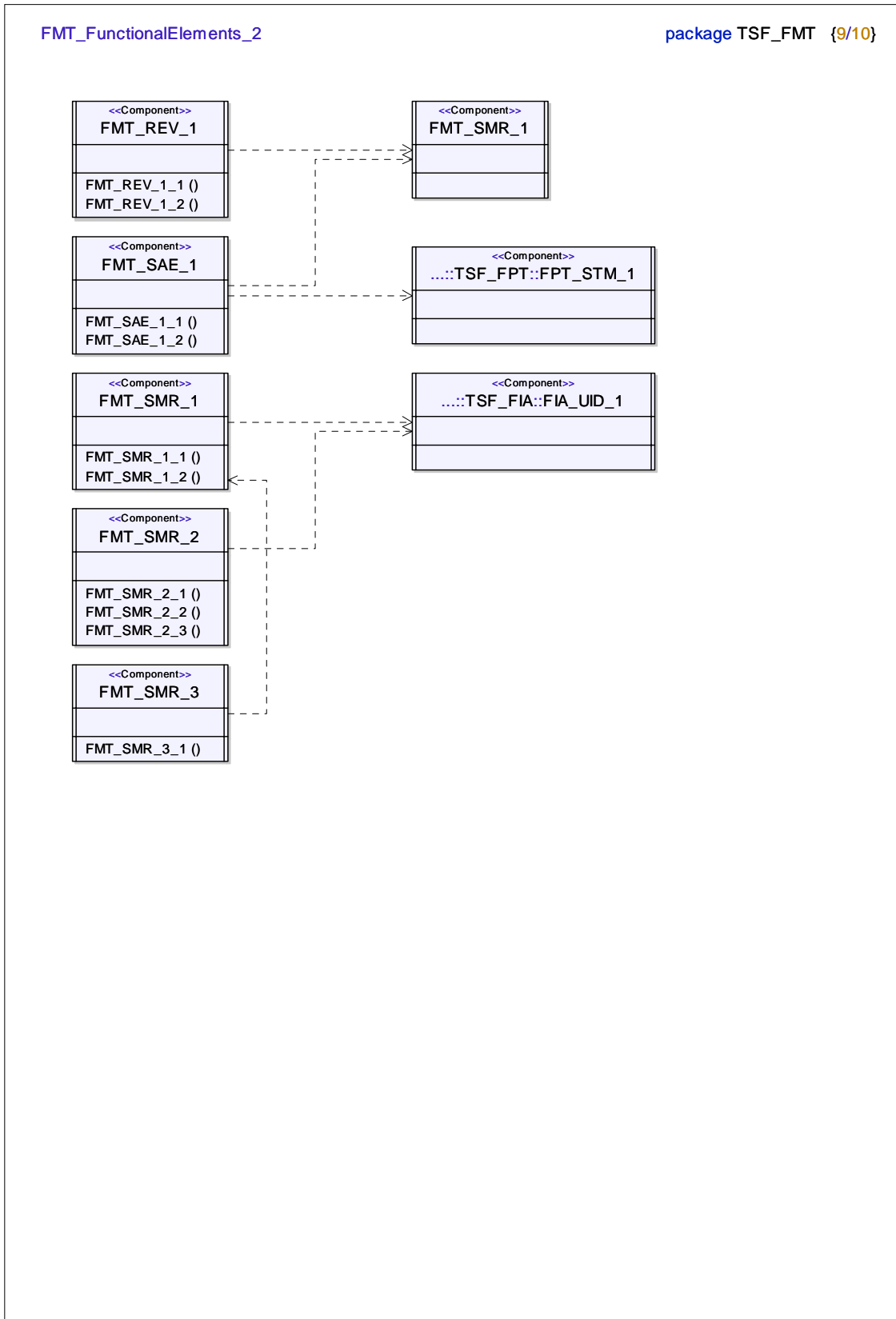












FMT_AuditEvents

package TSF_FMT {10/10}

Audit_FMT_MOF_1
auAllModsToBehaviour ()

Audit_FMT_MSA_1
auAllModsToSecAttrValues ()

Audit_FMT_MSA_2
auAllSecAttrValuesReject ()
auAllSecAttrValuesAccept ()

Audit_FMT_MSA_3
auModsToDefaultRules ()
auAllModsInitSecAttrValues ()

Audit_FMT_MTD_1
auAllModsToValues ()

Audit_FMT_MTD_2
auAllModsDataLimits ()
auAllModsLimitViolation ()

Audit_FMT_MTD_3
auAllRejectedValues ()

Audit_FMT_REV_1
auUnsucRevkSecAttrValue ()
auAllAtmptRevkSecAttr ()

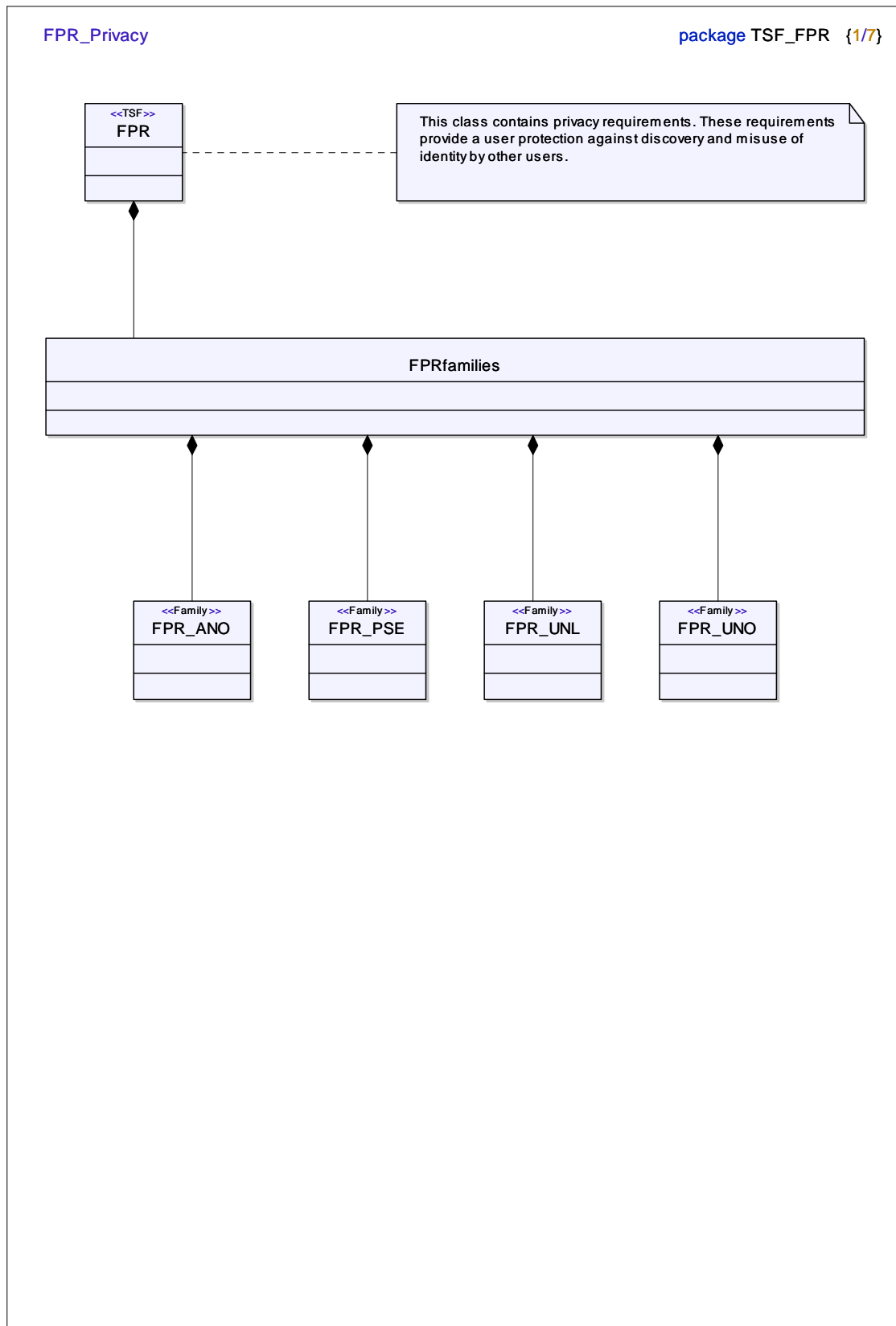
Audit_FMT_SAE_1
auSpecAttrExpiration ()
auActnAttrExpiry ()

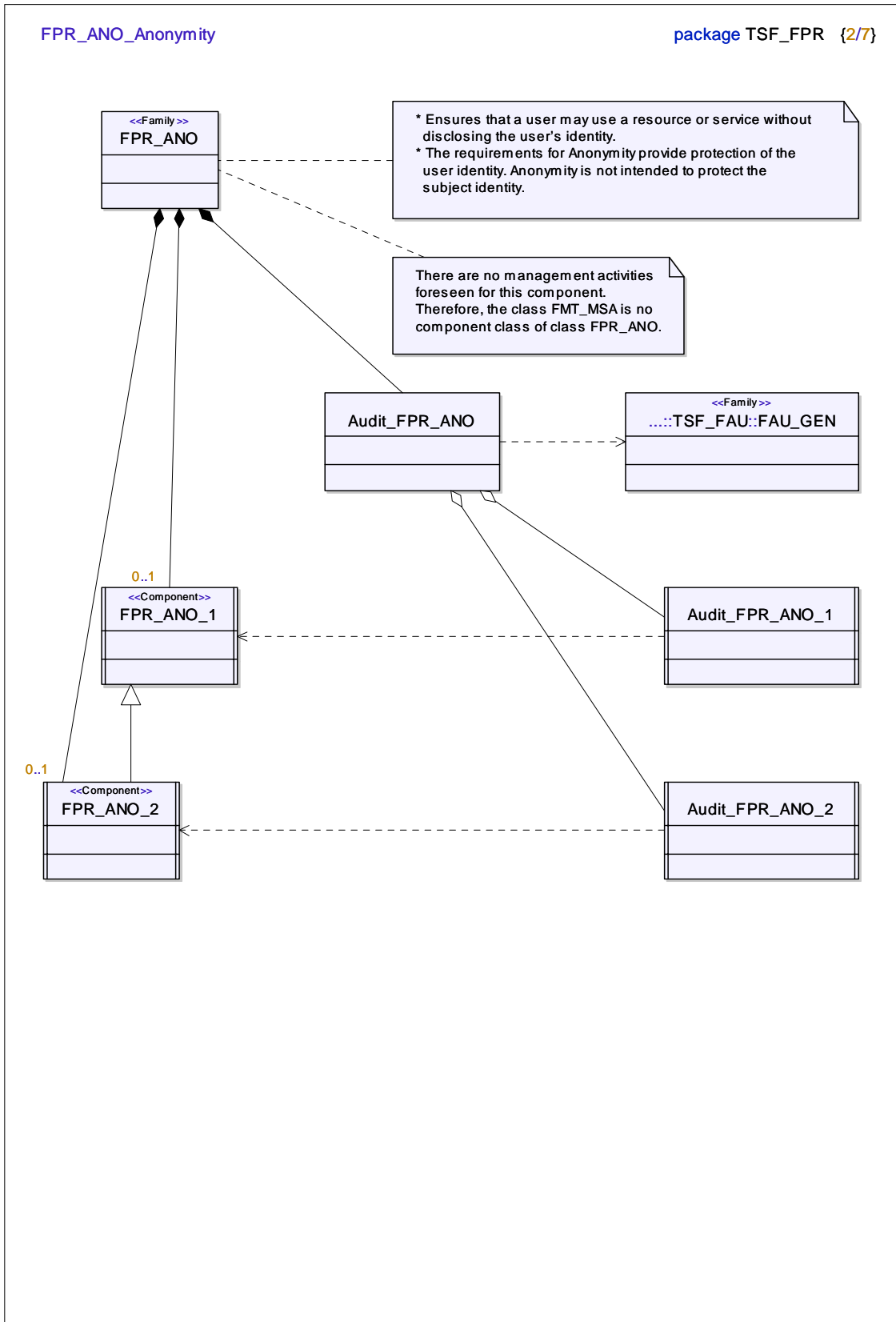
Audit_FMT_SMR_1
auModsRoleUsr ()
auEvryUseRightsOfRole ()

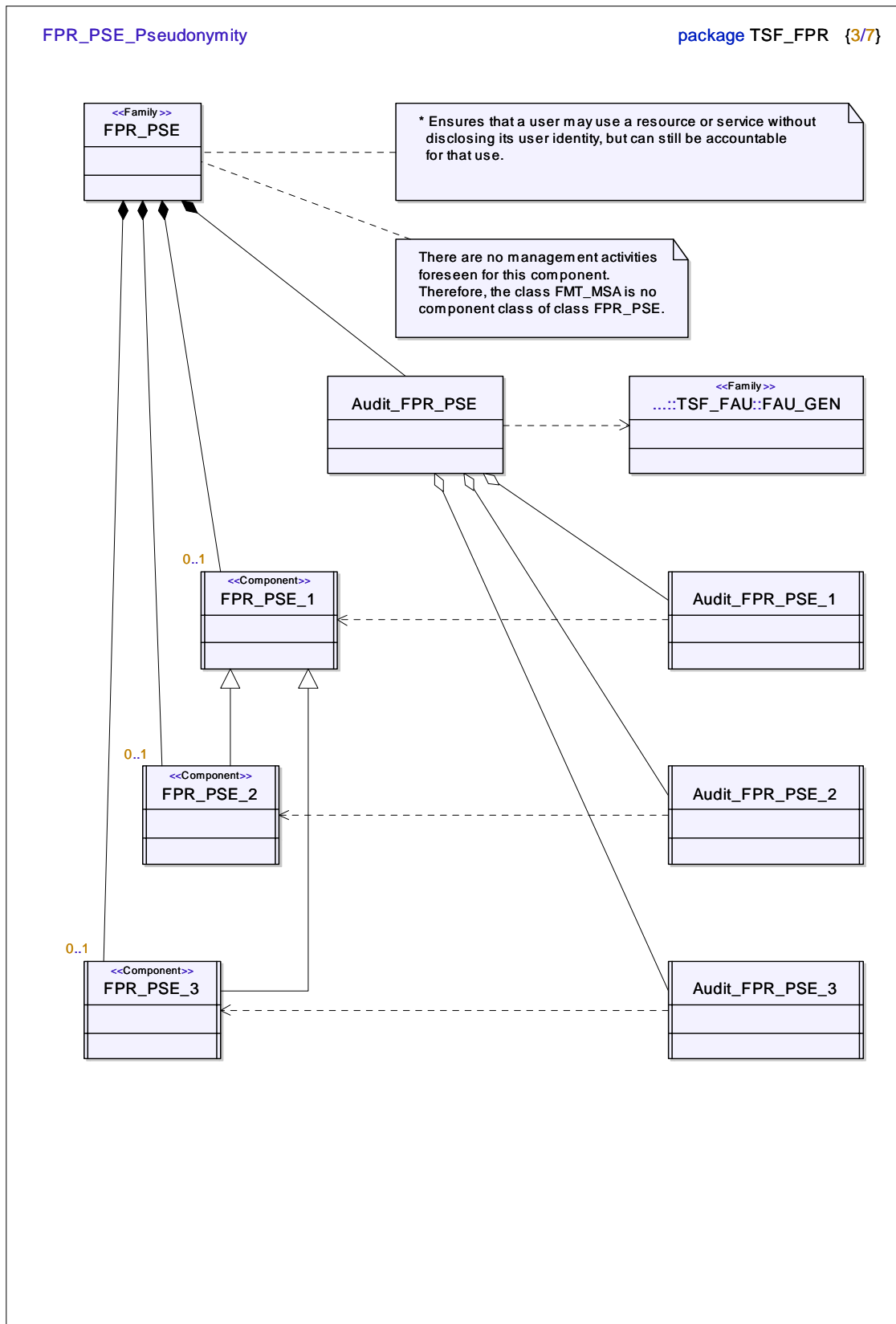
Audit_FMT_SMR_2
auModsRoleUsr ()
auUnsuccAtmptUseOfRole ()
auEvryUseRightsOfRole ()

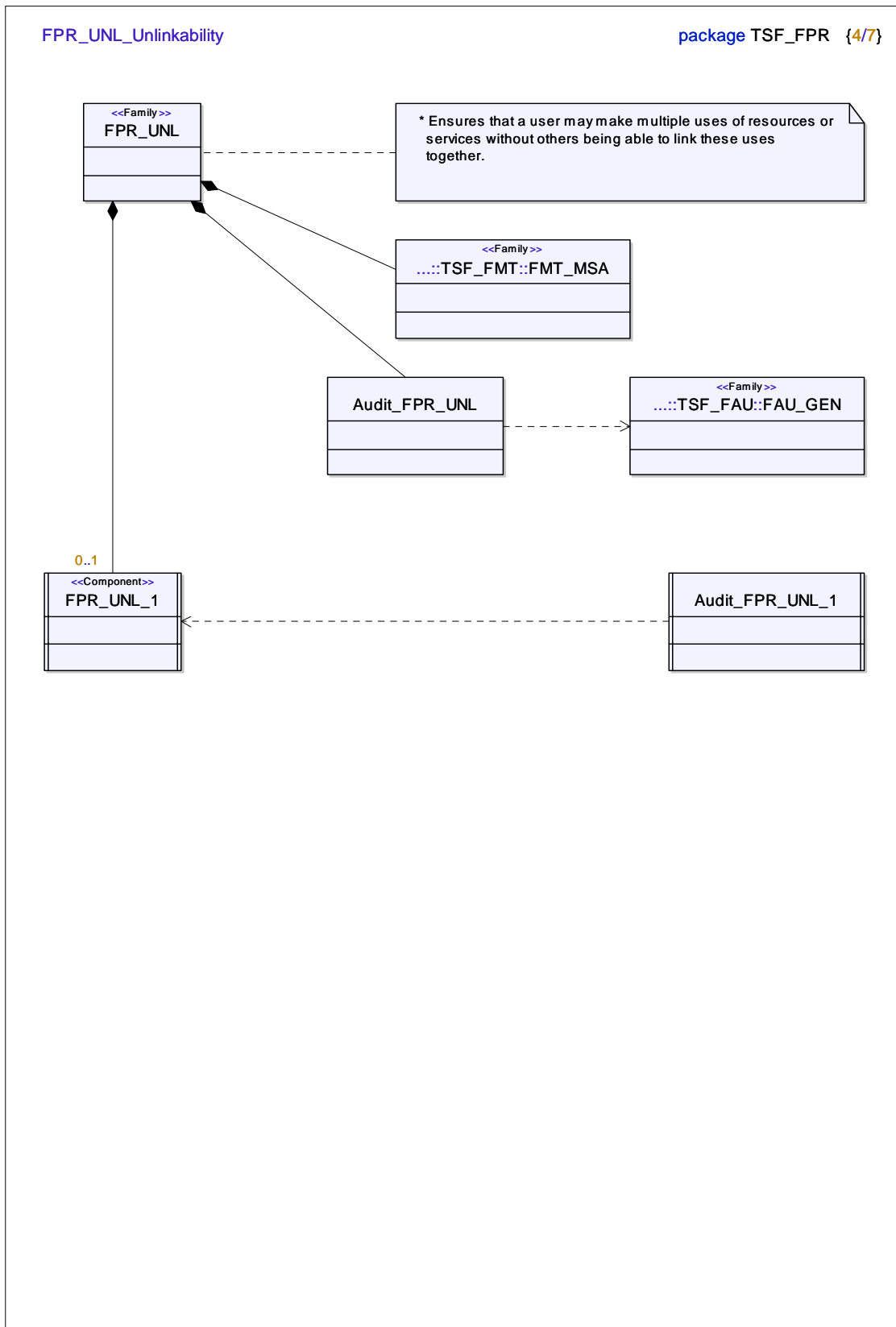
Audit_FMT_SMR_3
auExpIReqUseOfRole ()

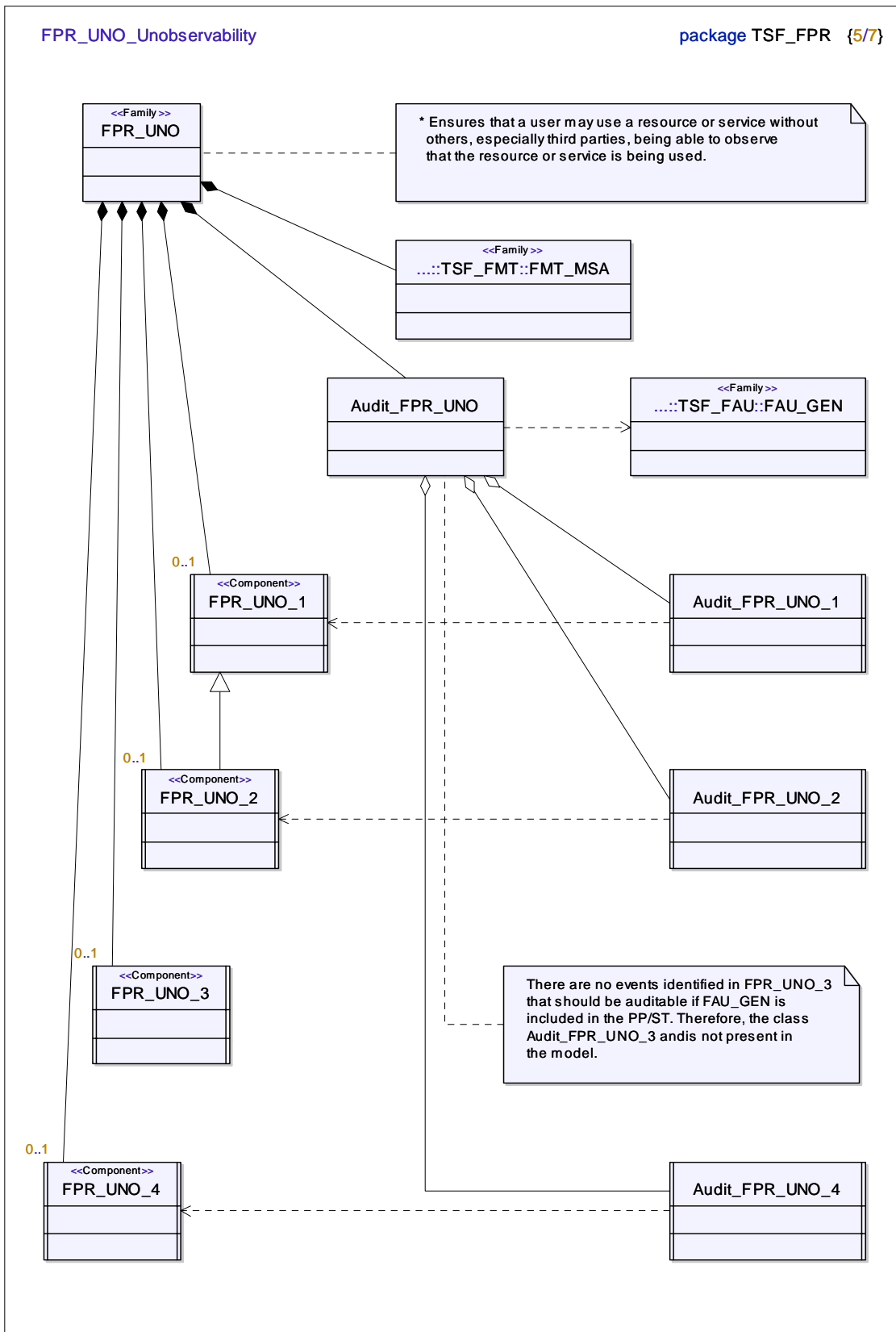
A.3.7 Package TSF_FPR

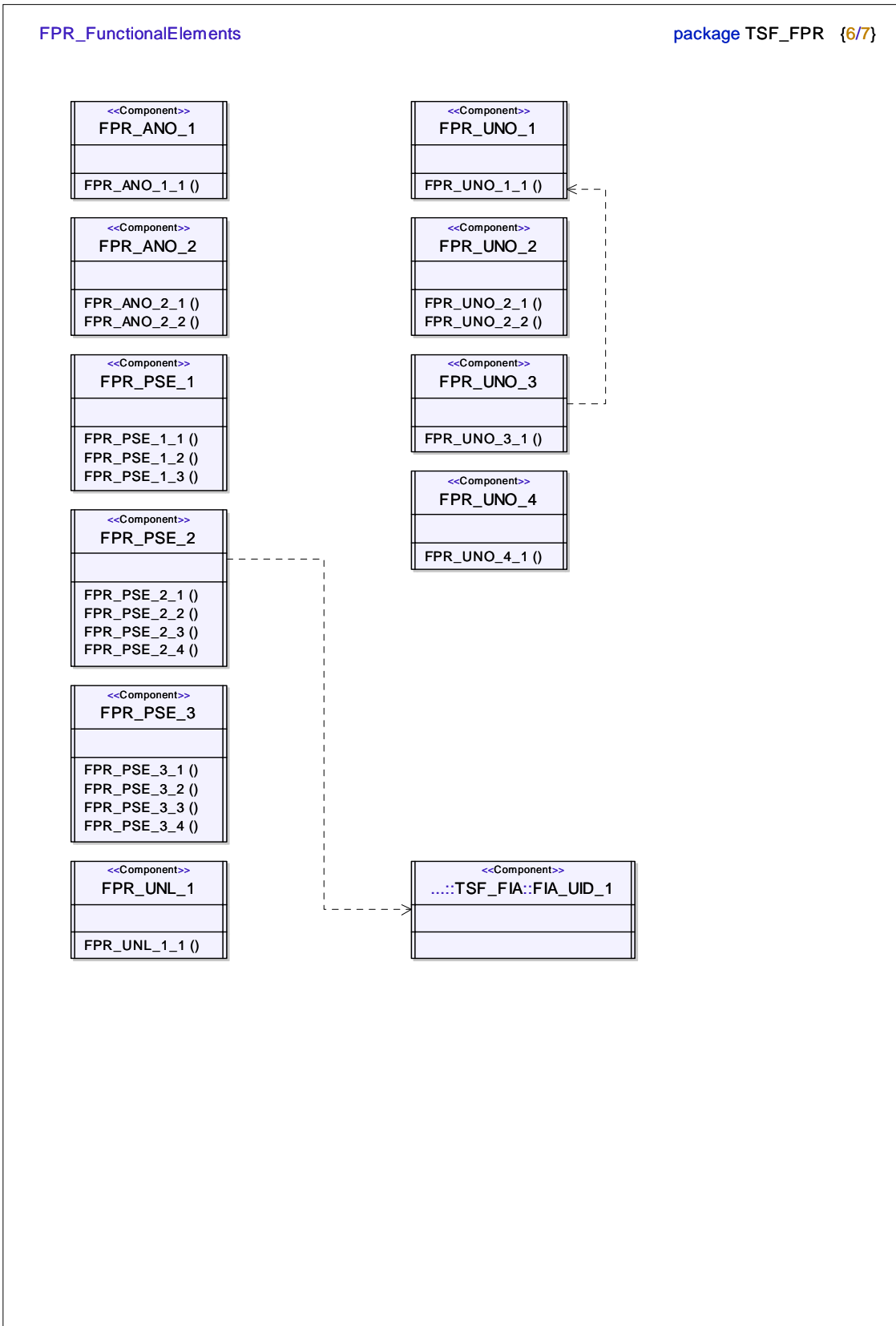












FPR_AuditEvents

package TSF_FPR {7/7}

Audit_FPR_ANO_1
unInvkAnonmtyMech ()

Audit_FPR_UNL_1
unInvkUnlinkabilityMech ()

Audit_FPR_ANO_2
unInvkAnonmtyMech ()

Audit_FPR_UNO_1
unInvkUnobservabtyMech ()

Audit_FPR_PSE_1
unIdntityRequestorID ()

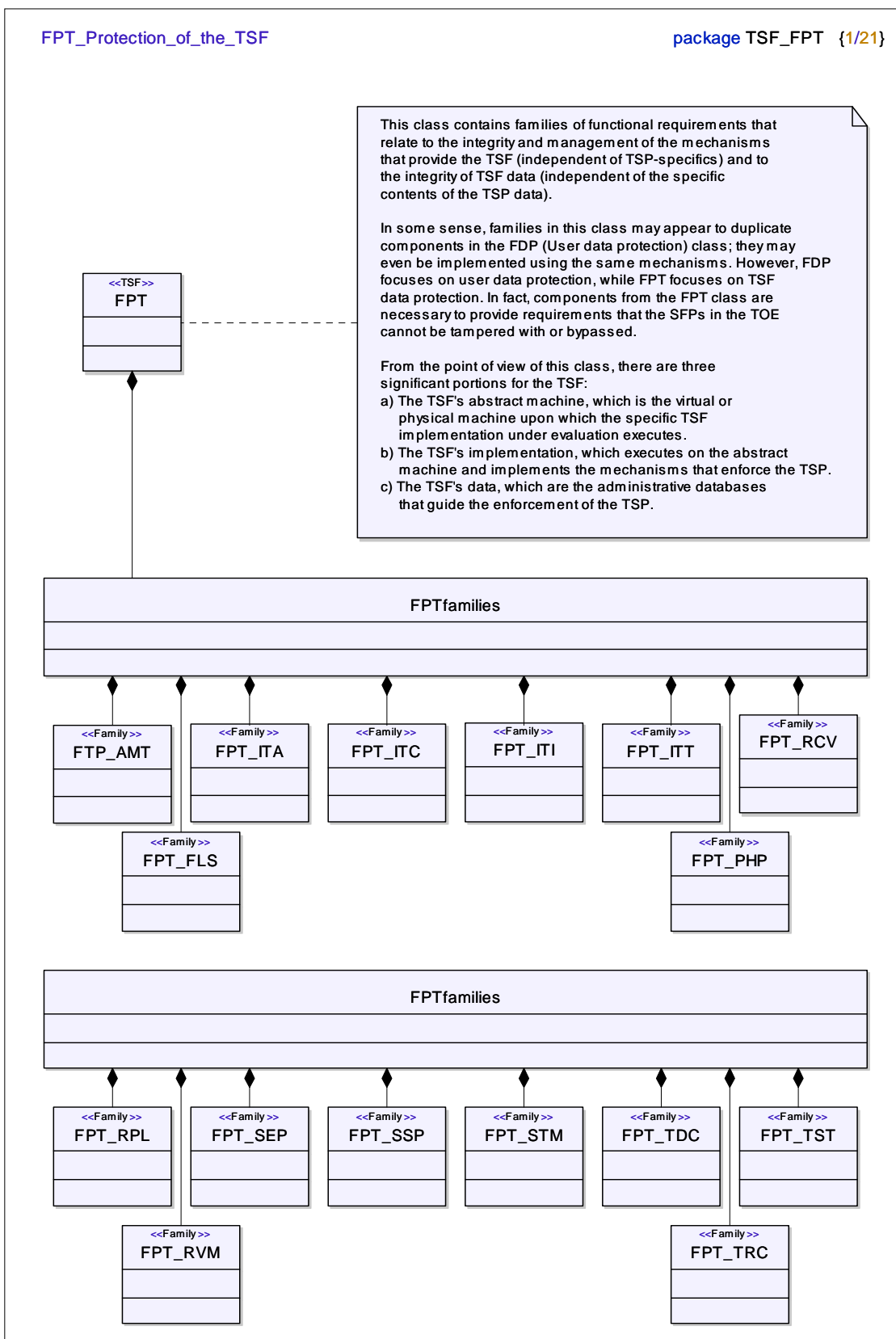
Audit_FPR_UNO_2
unInvkUnobservabtyMech ()

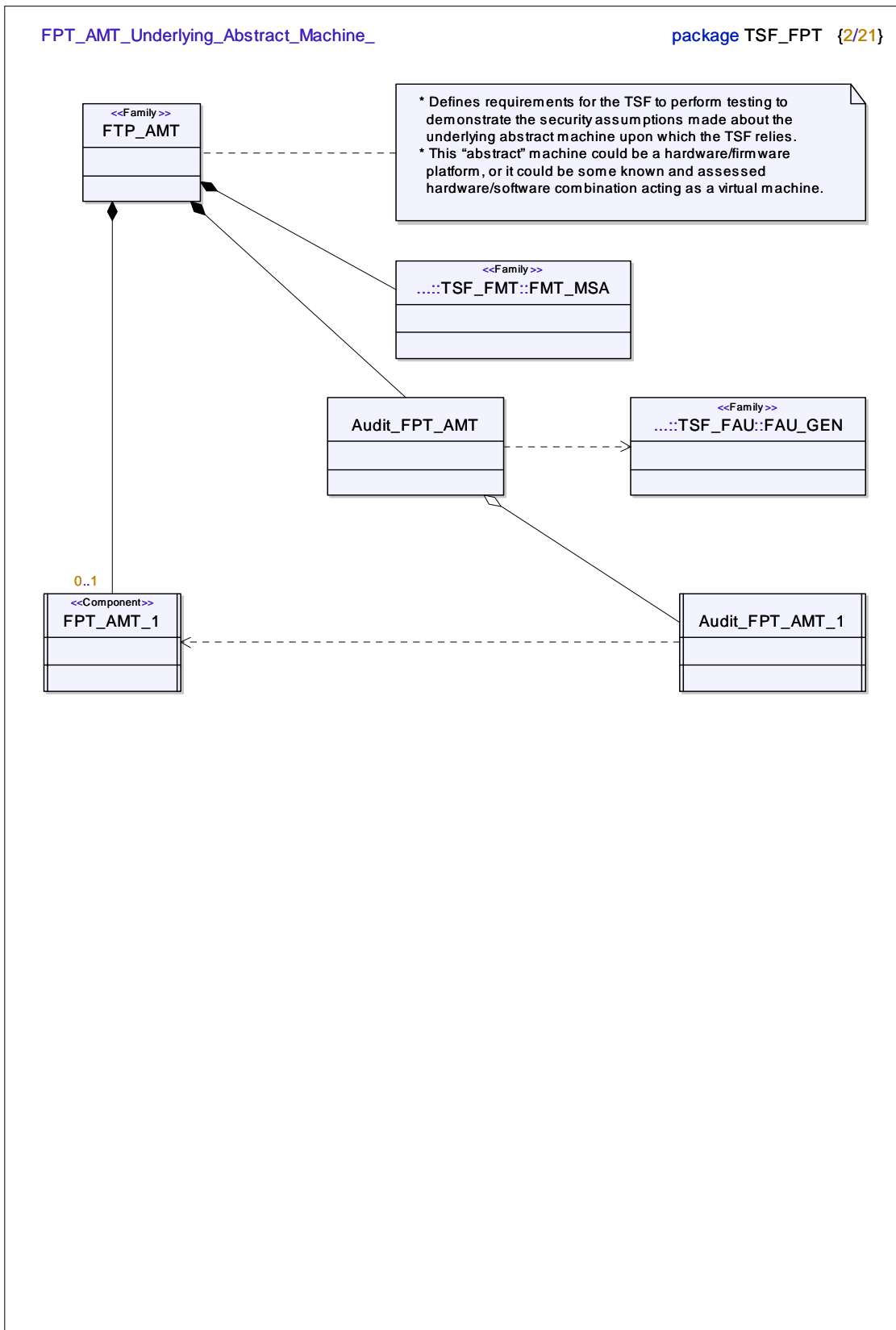
Audit_FPR_PSE_2
unIdntityRequestorID ()

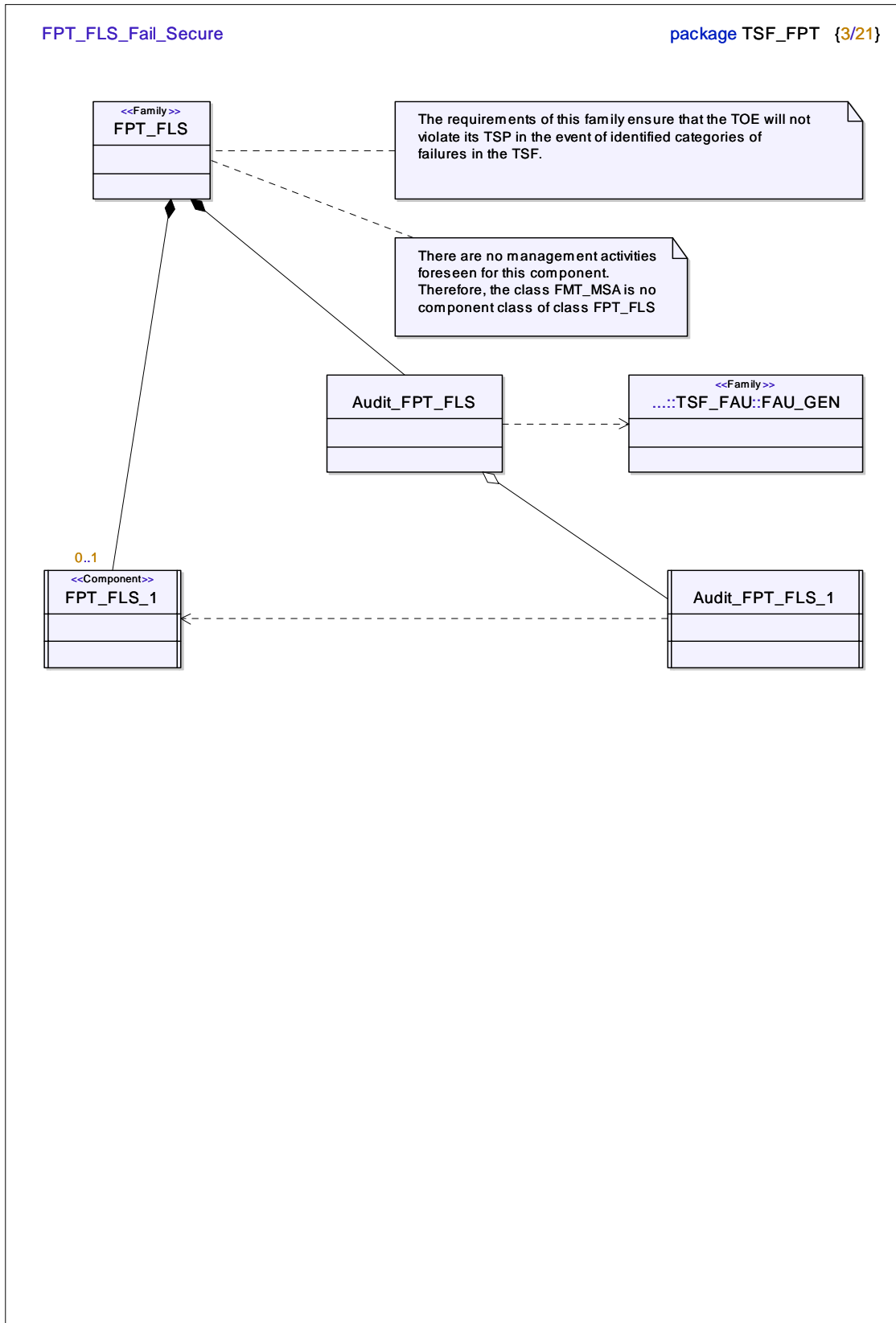
Audit_FPR_UNO_4
unObservationOfUse ()

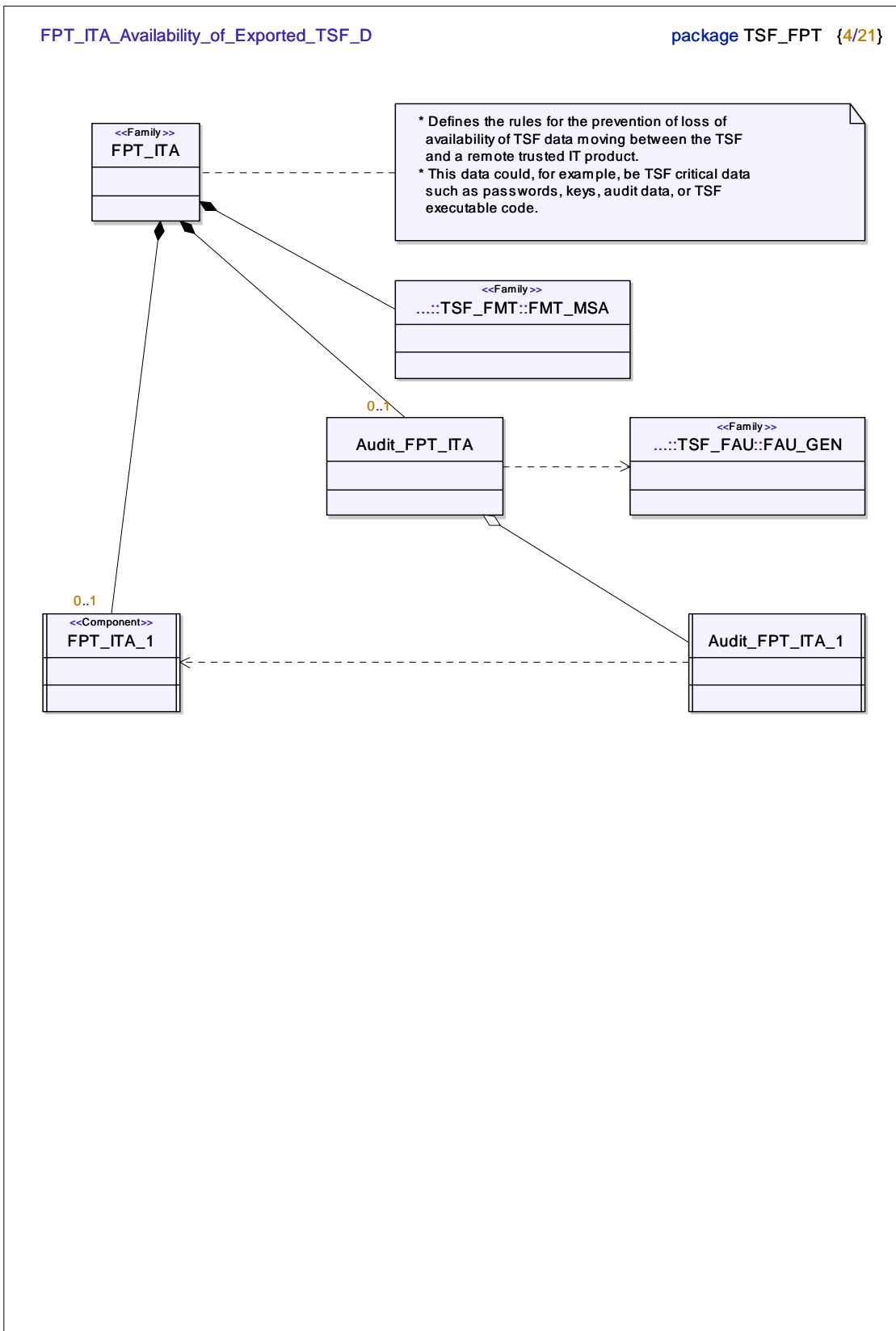
Audit_FPR_PSE_3
unIdntityRequestorID ()

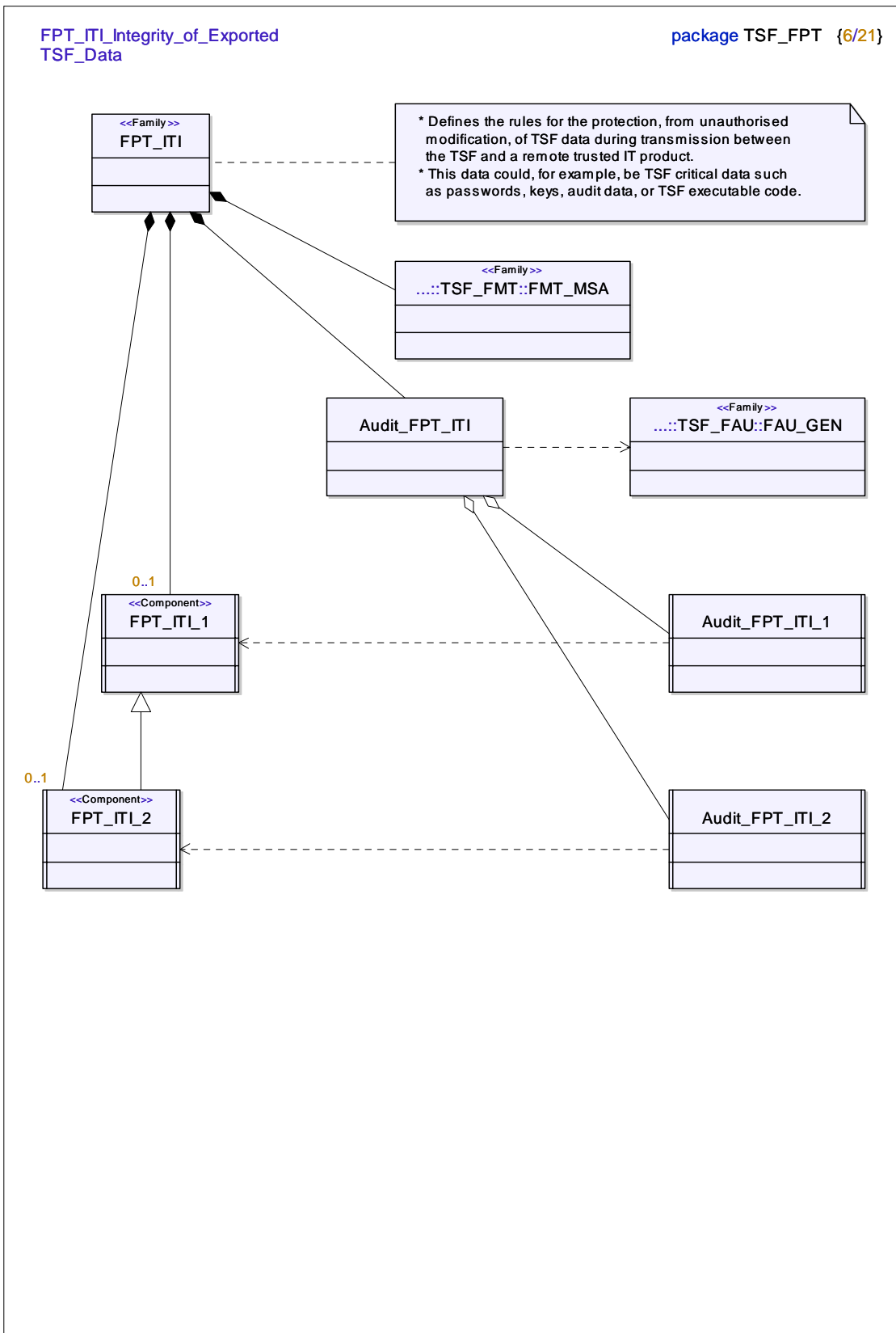
A.3.8 Package TSF_FPT

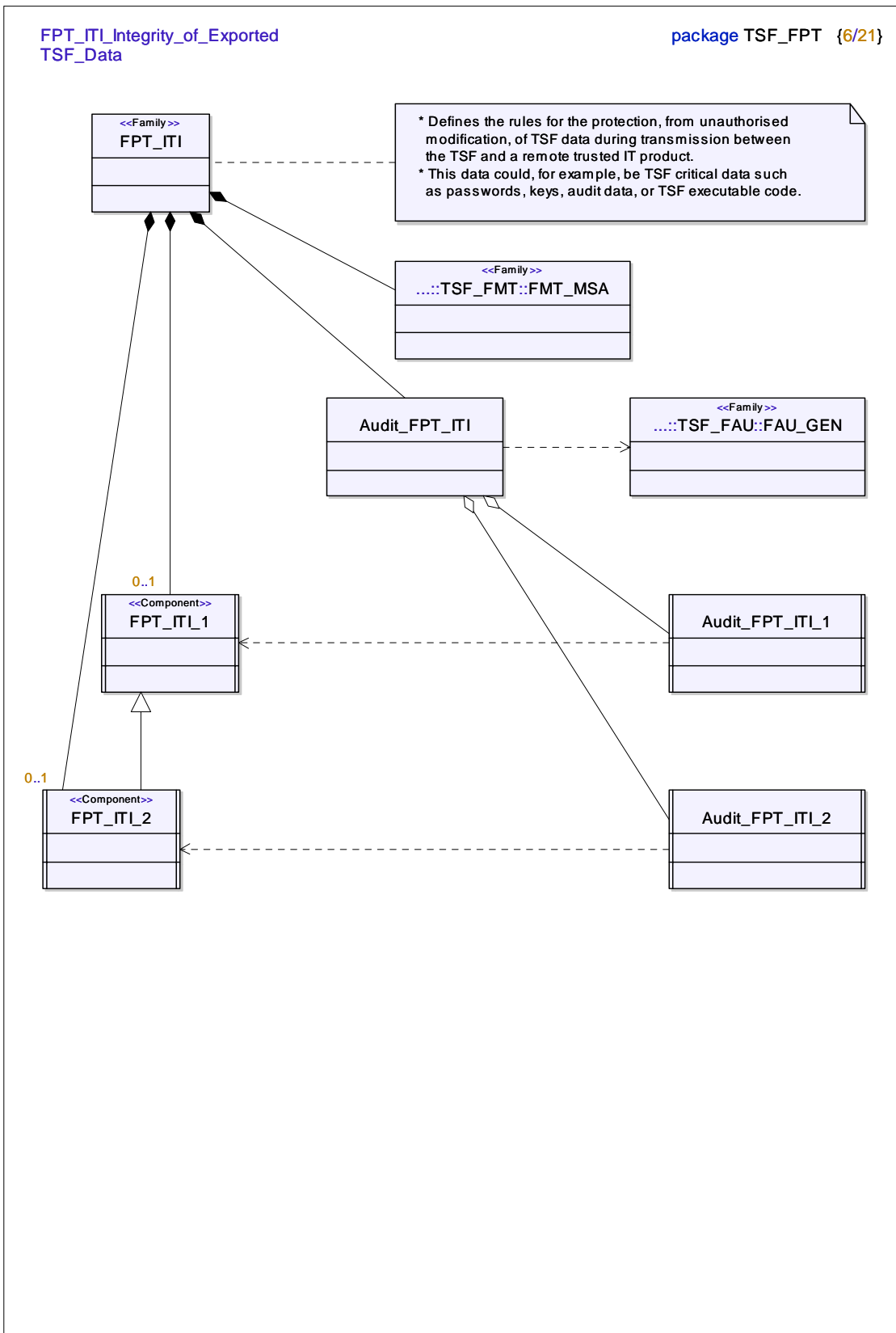


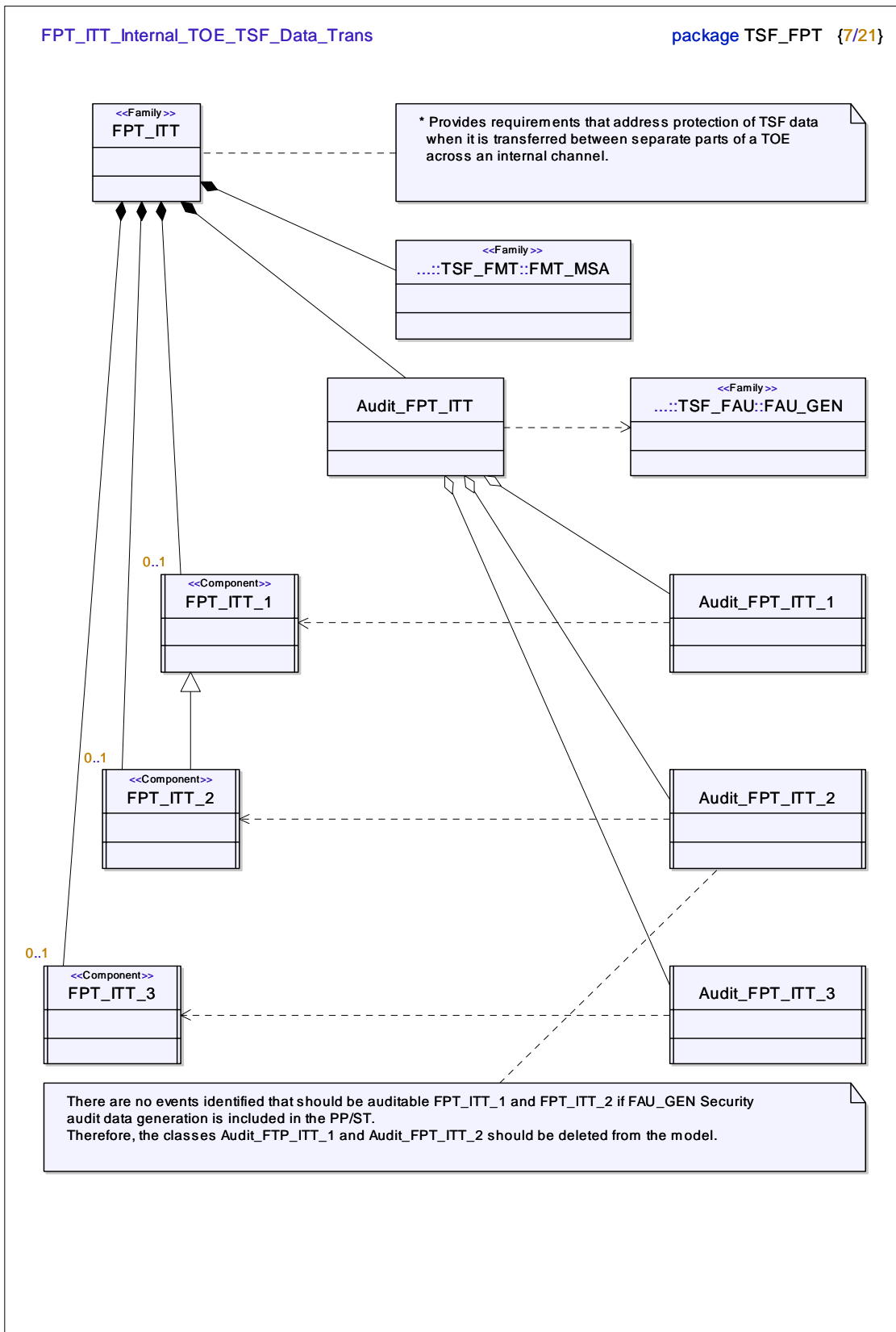


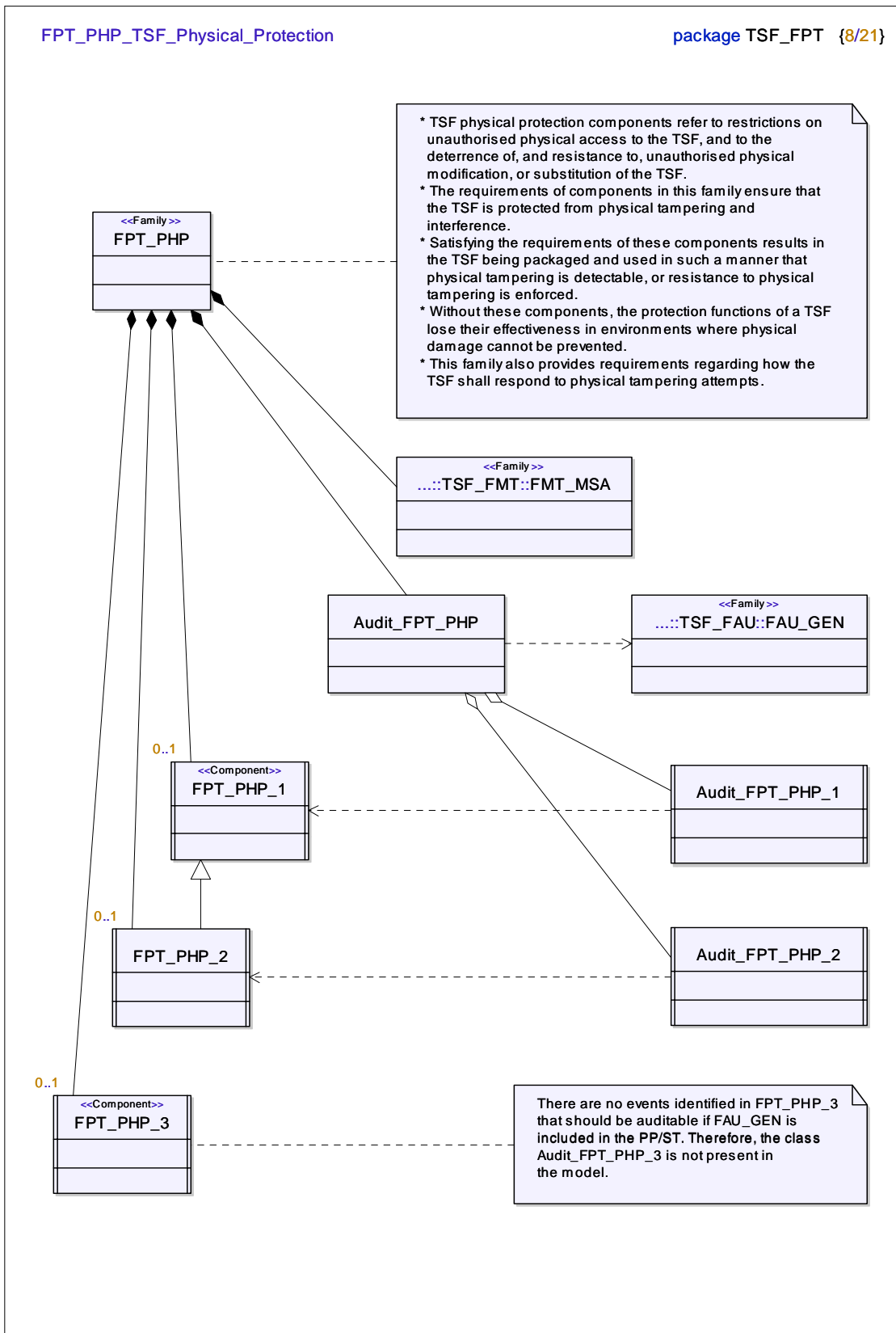


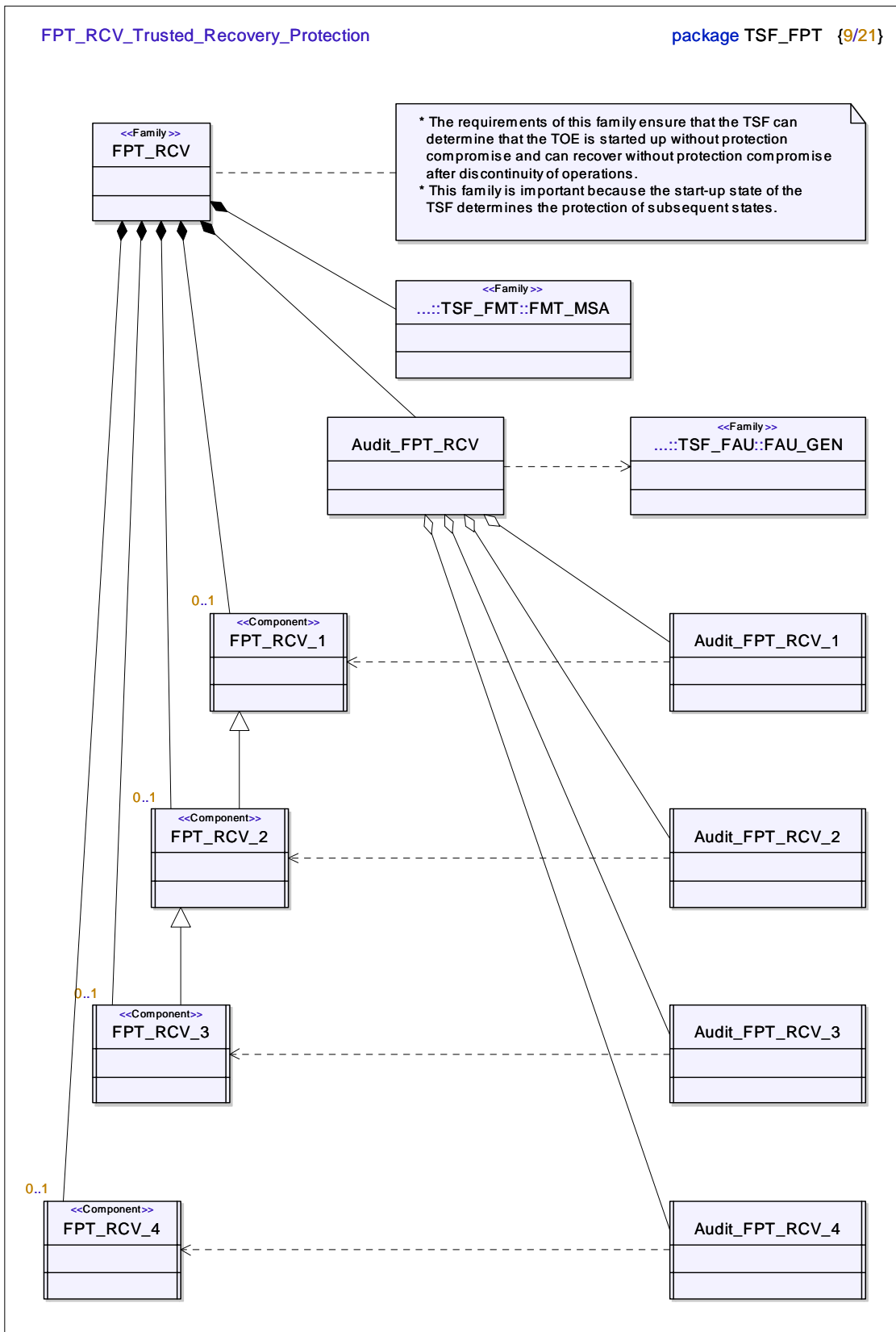


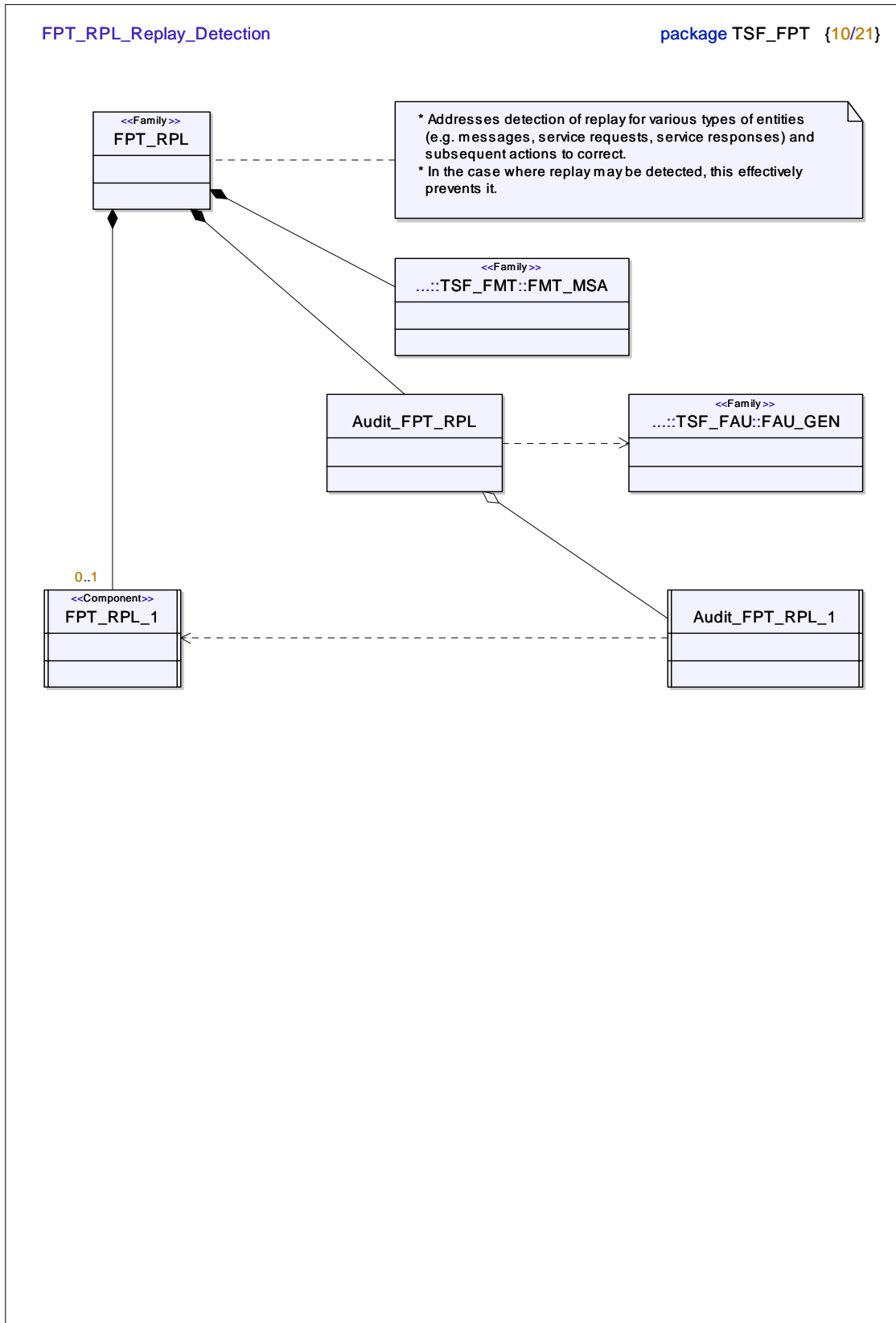


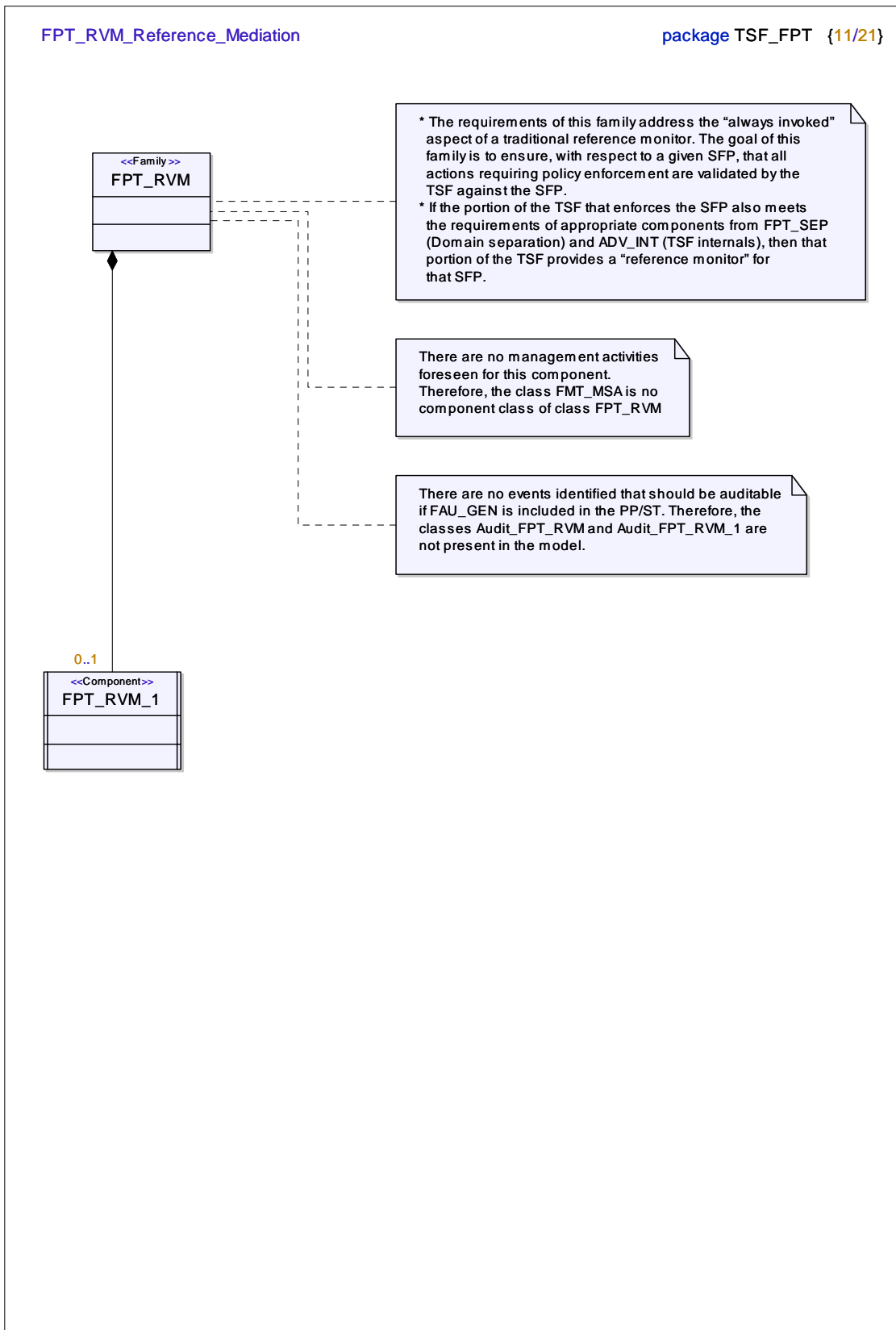


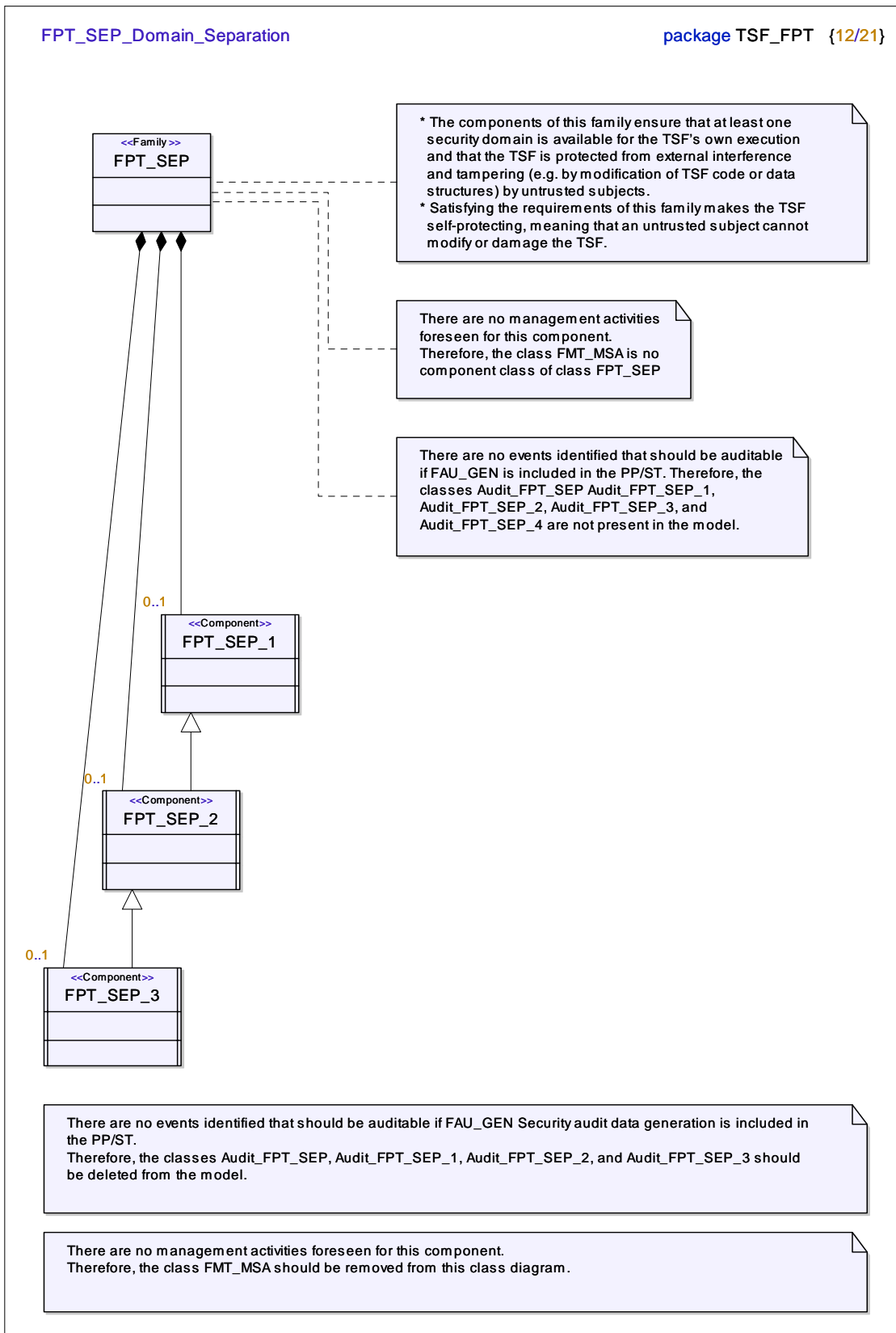


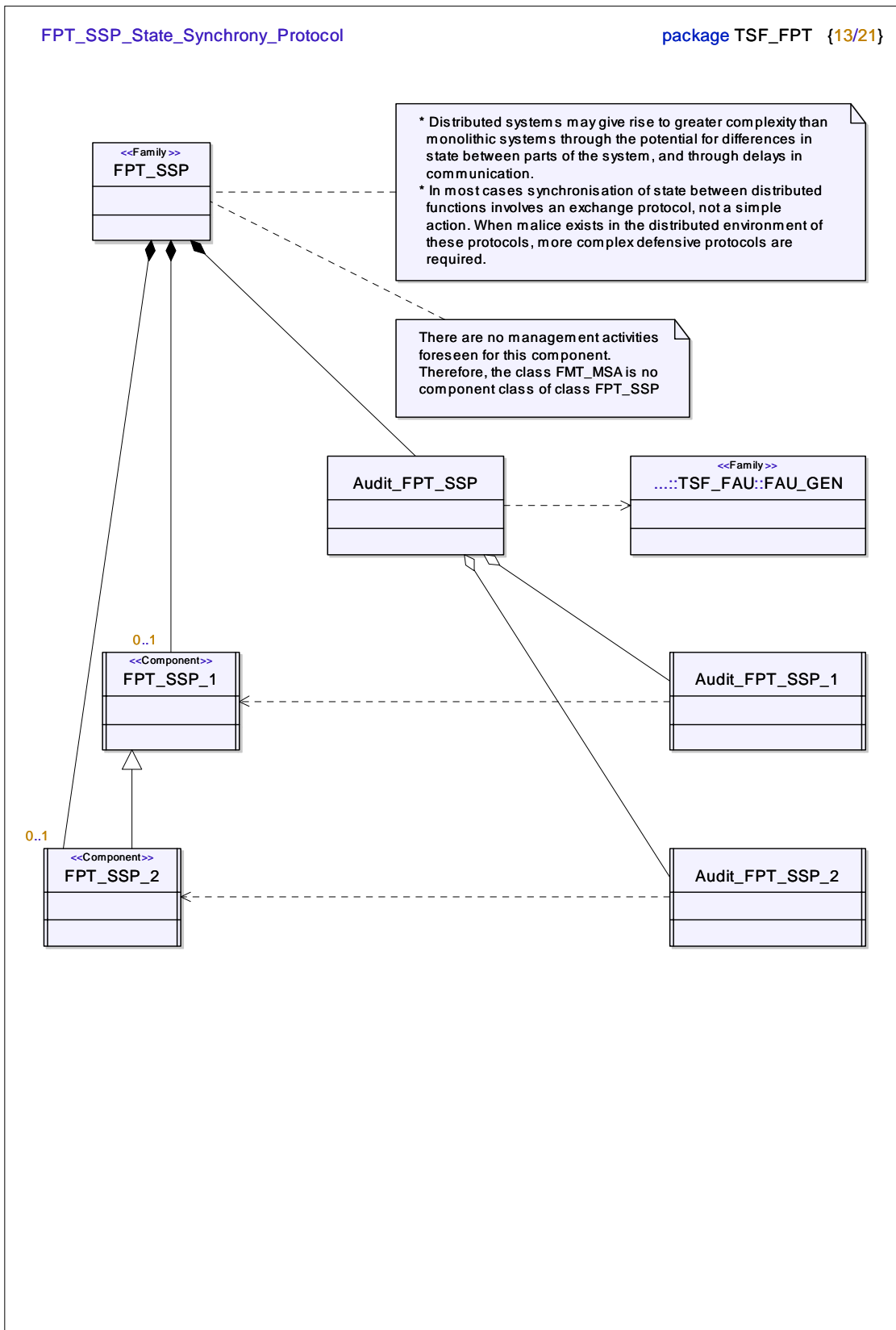


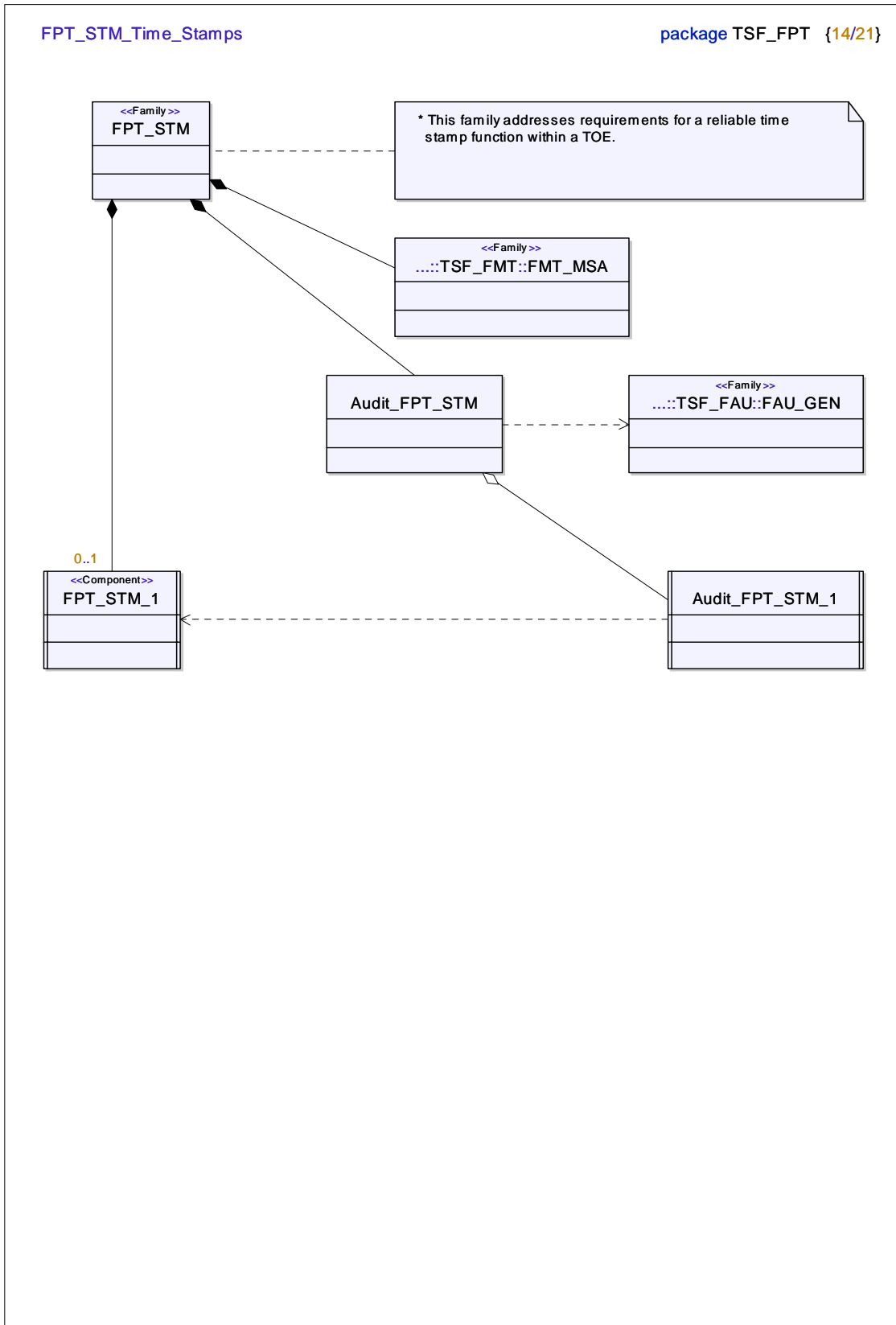


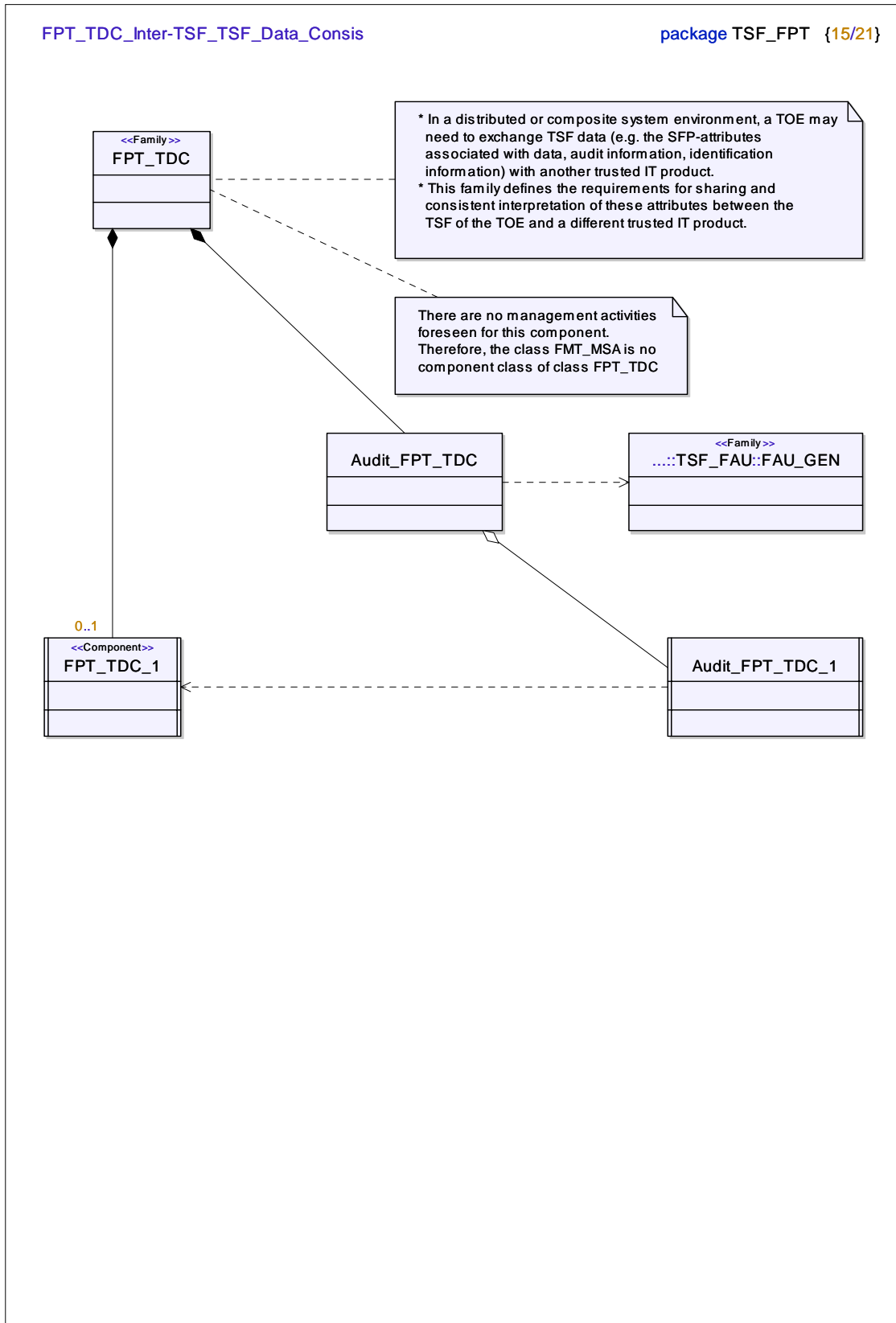


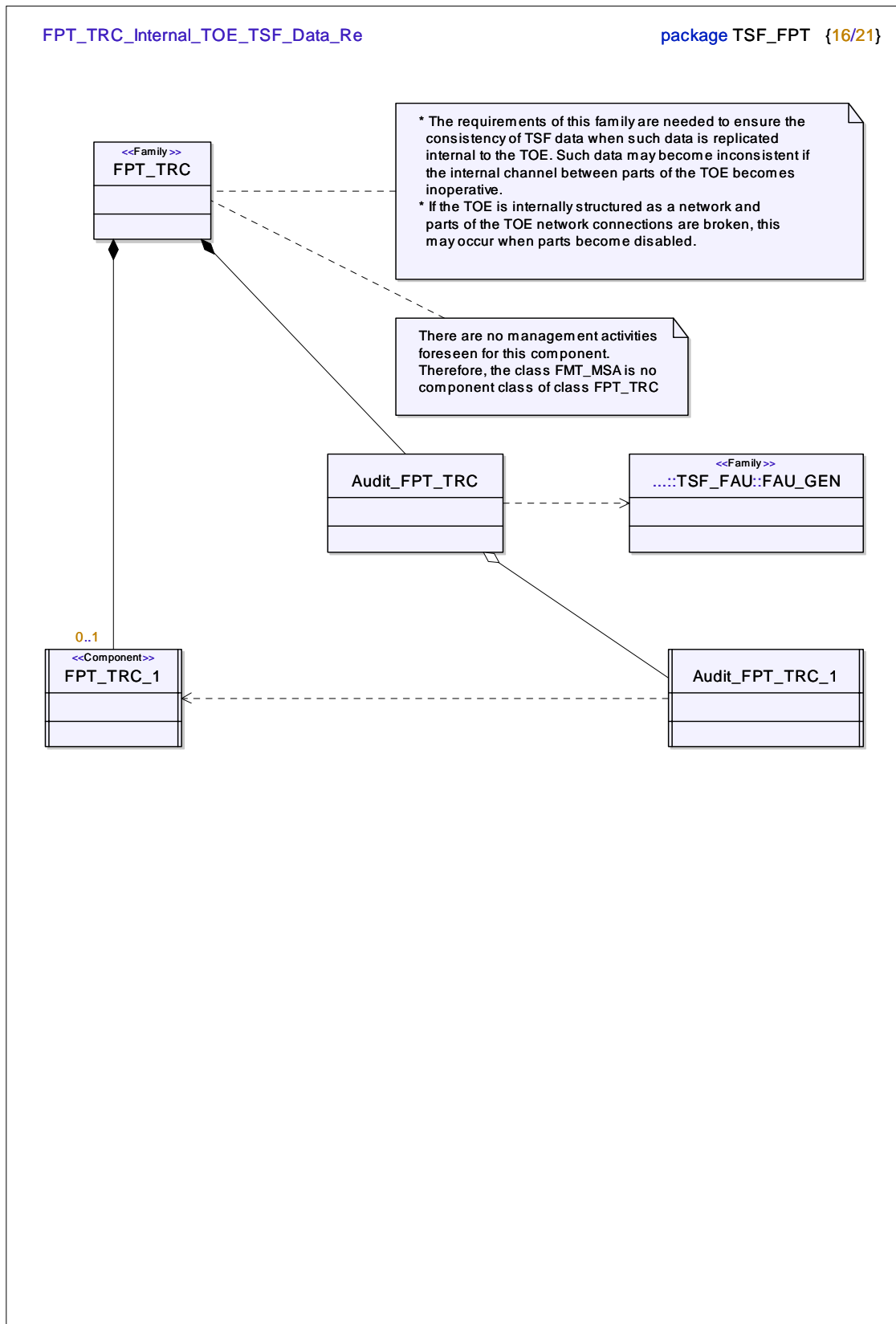


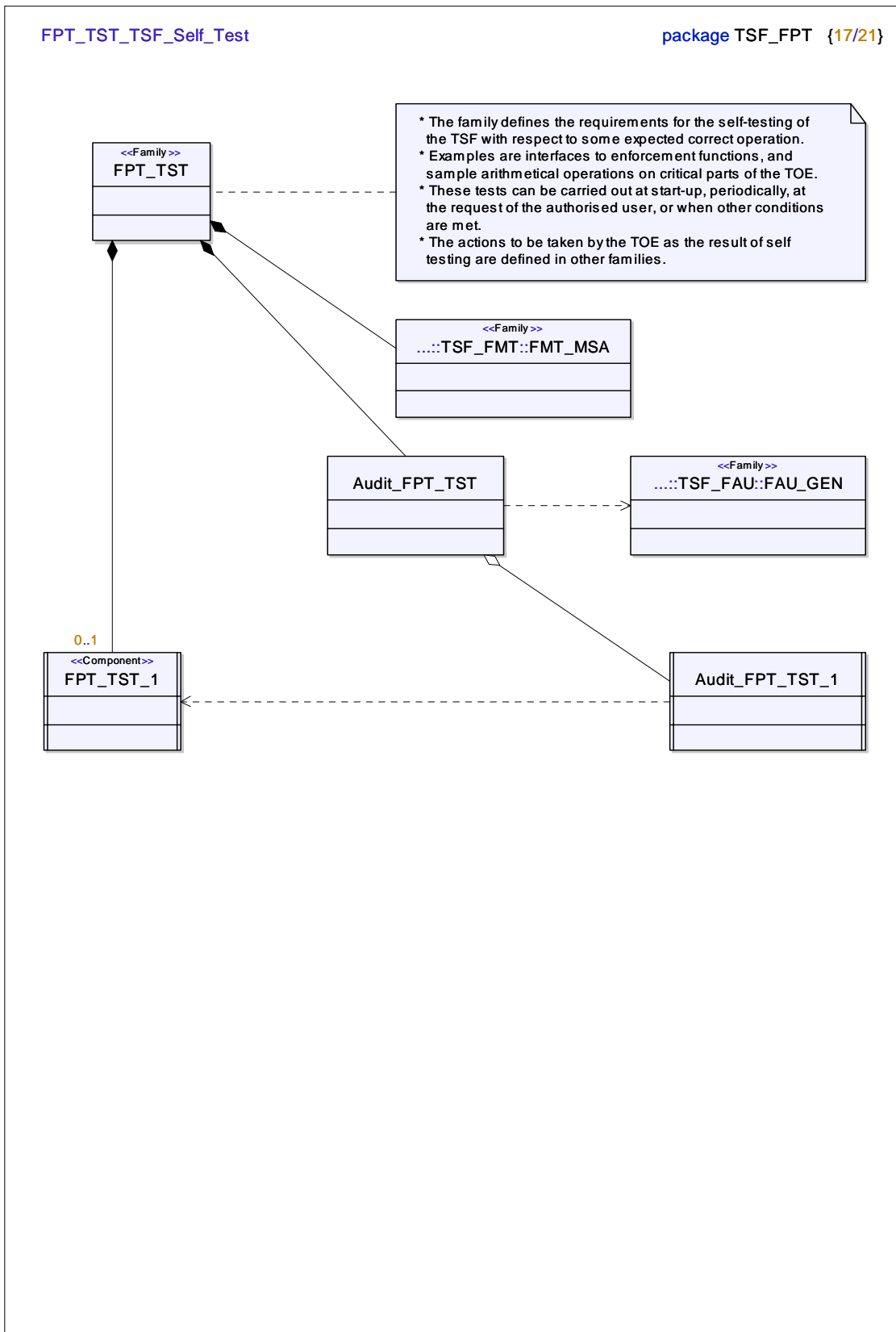


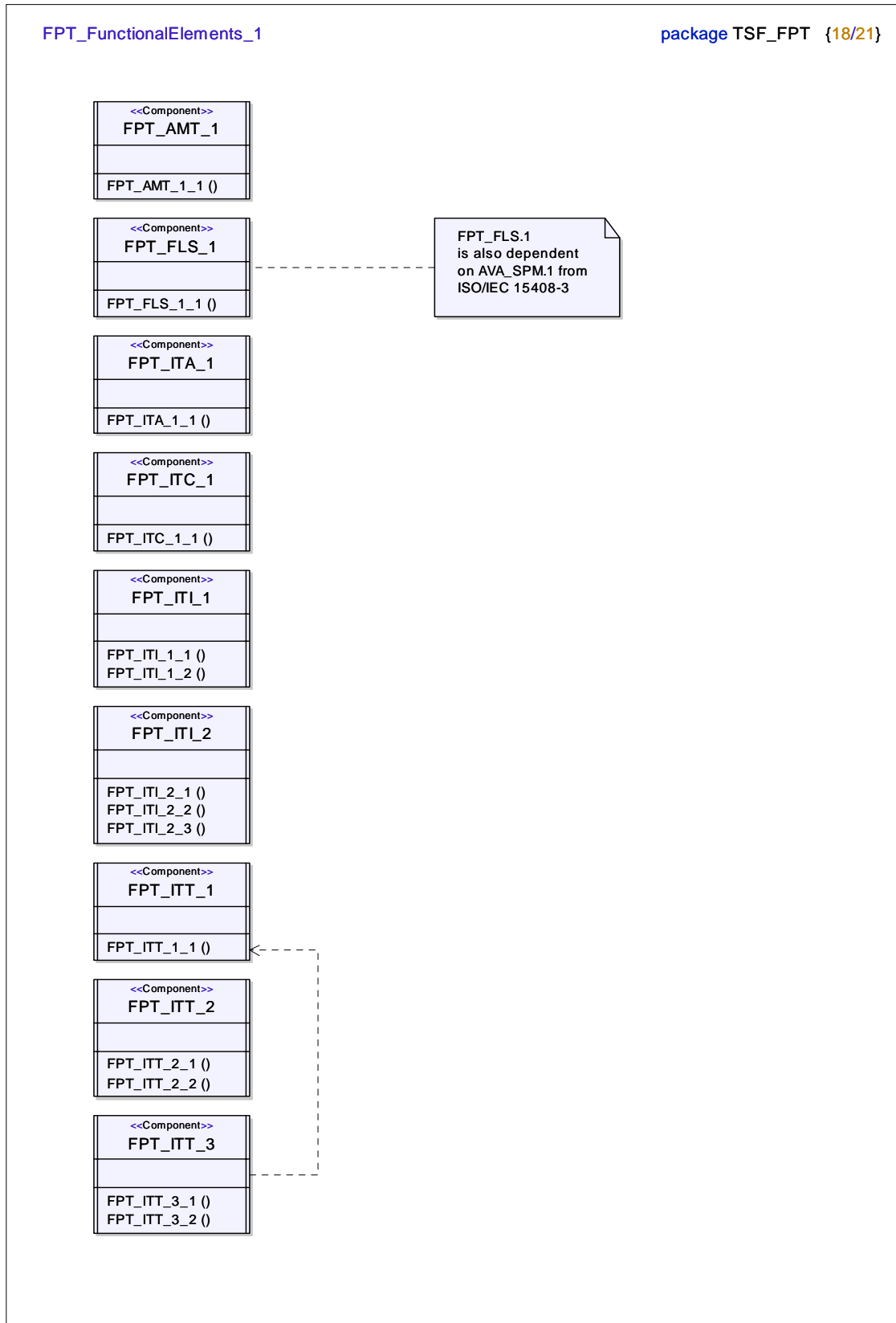


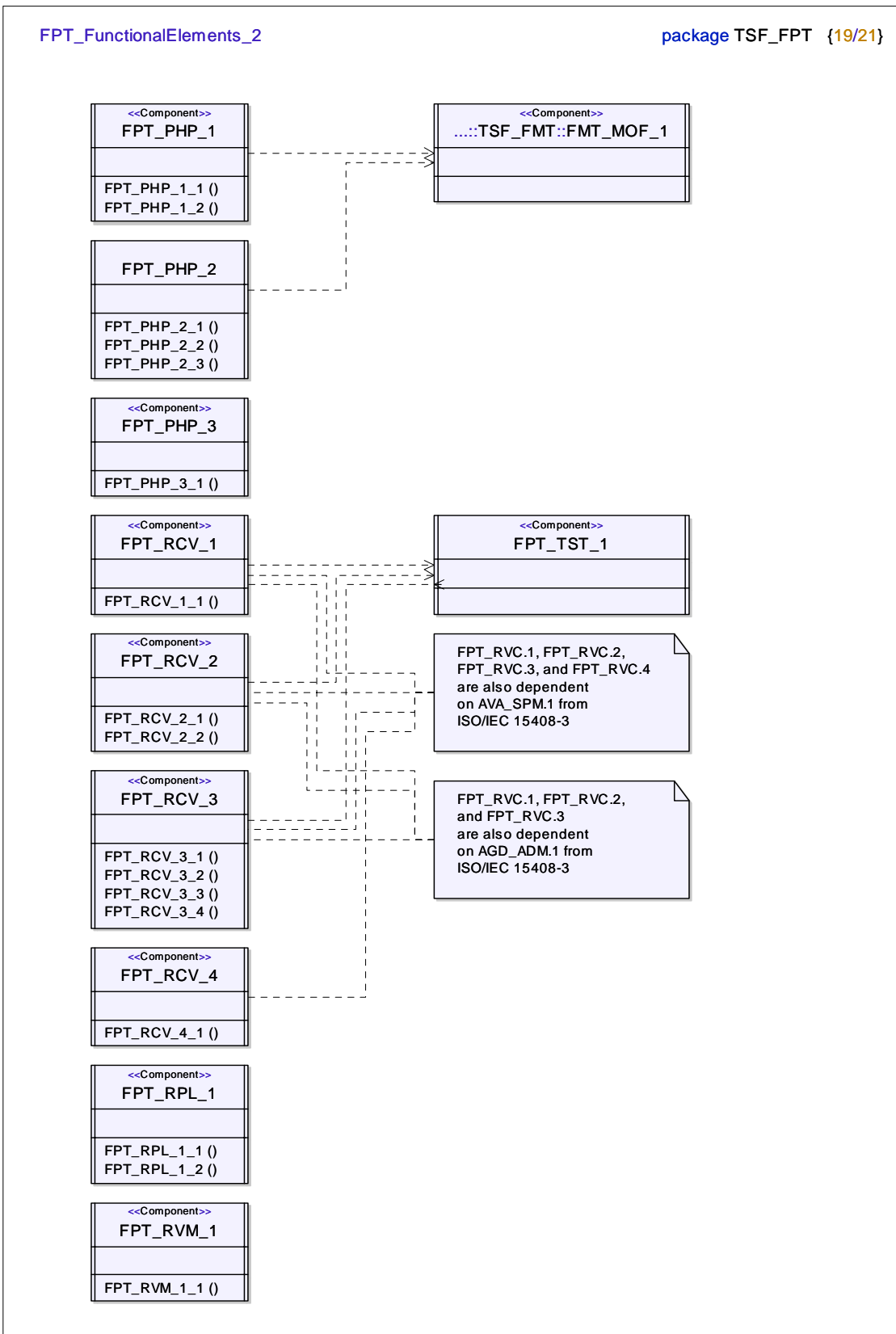


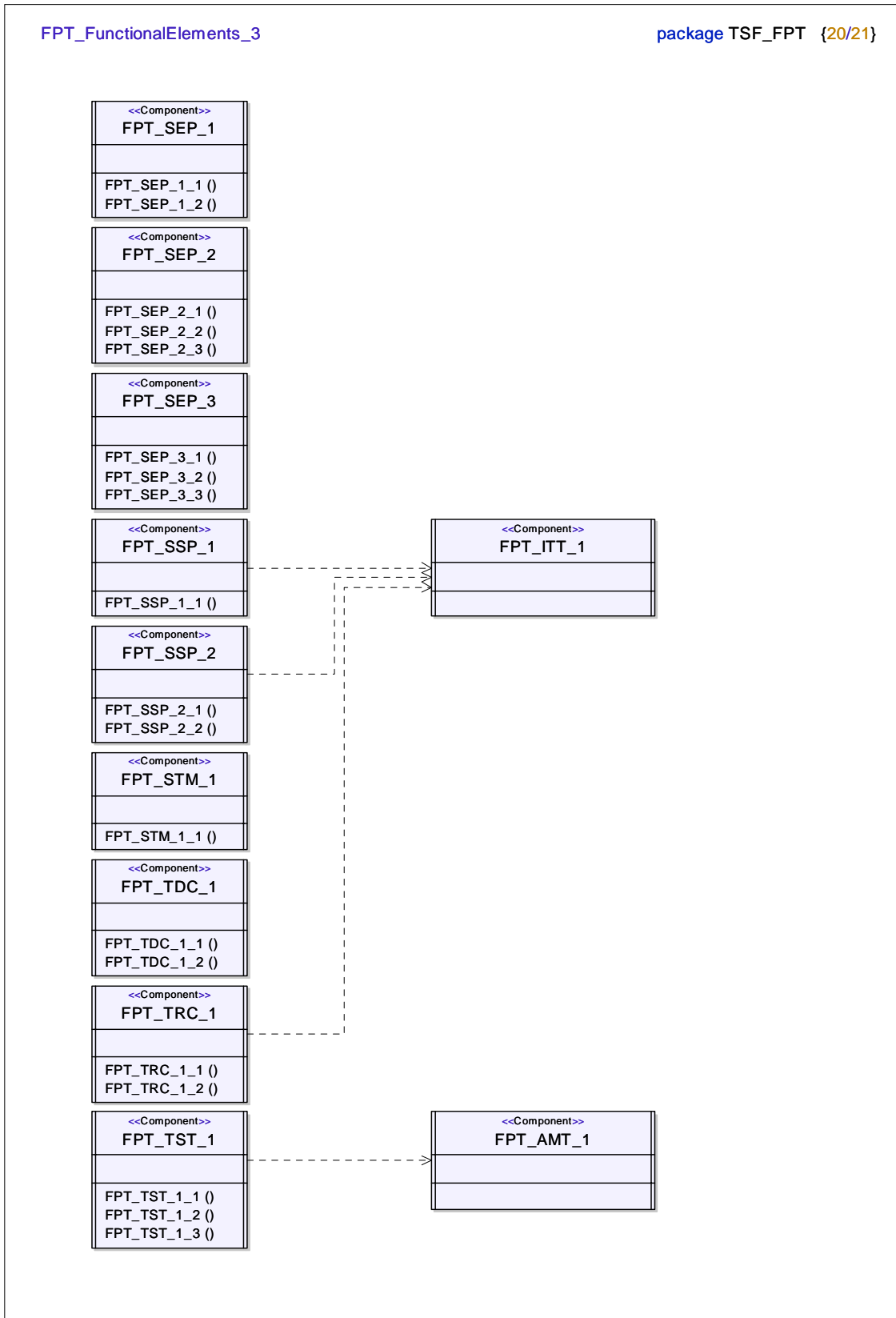










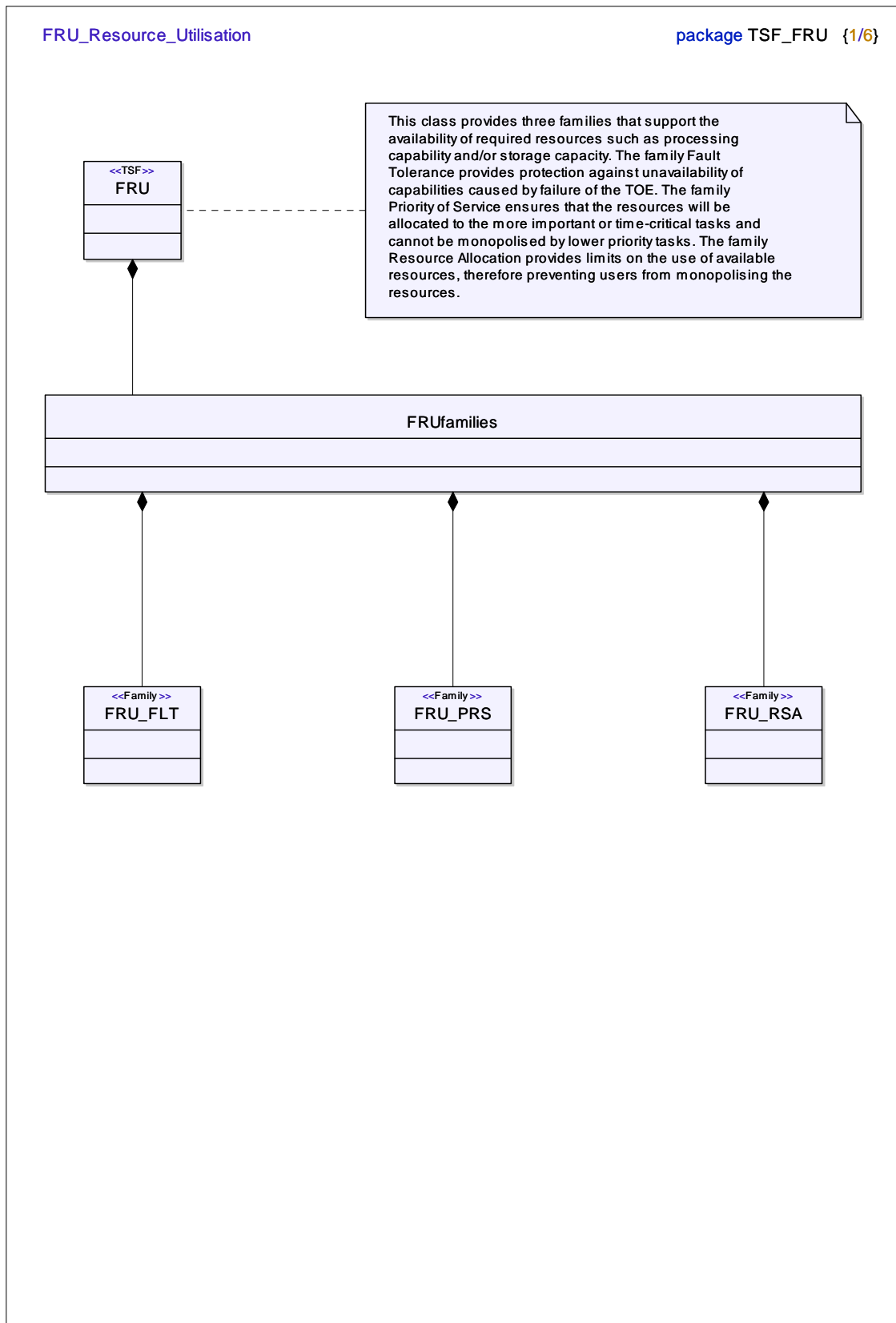


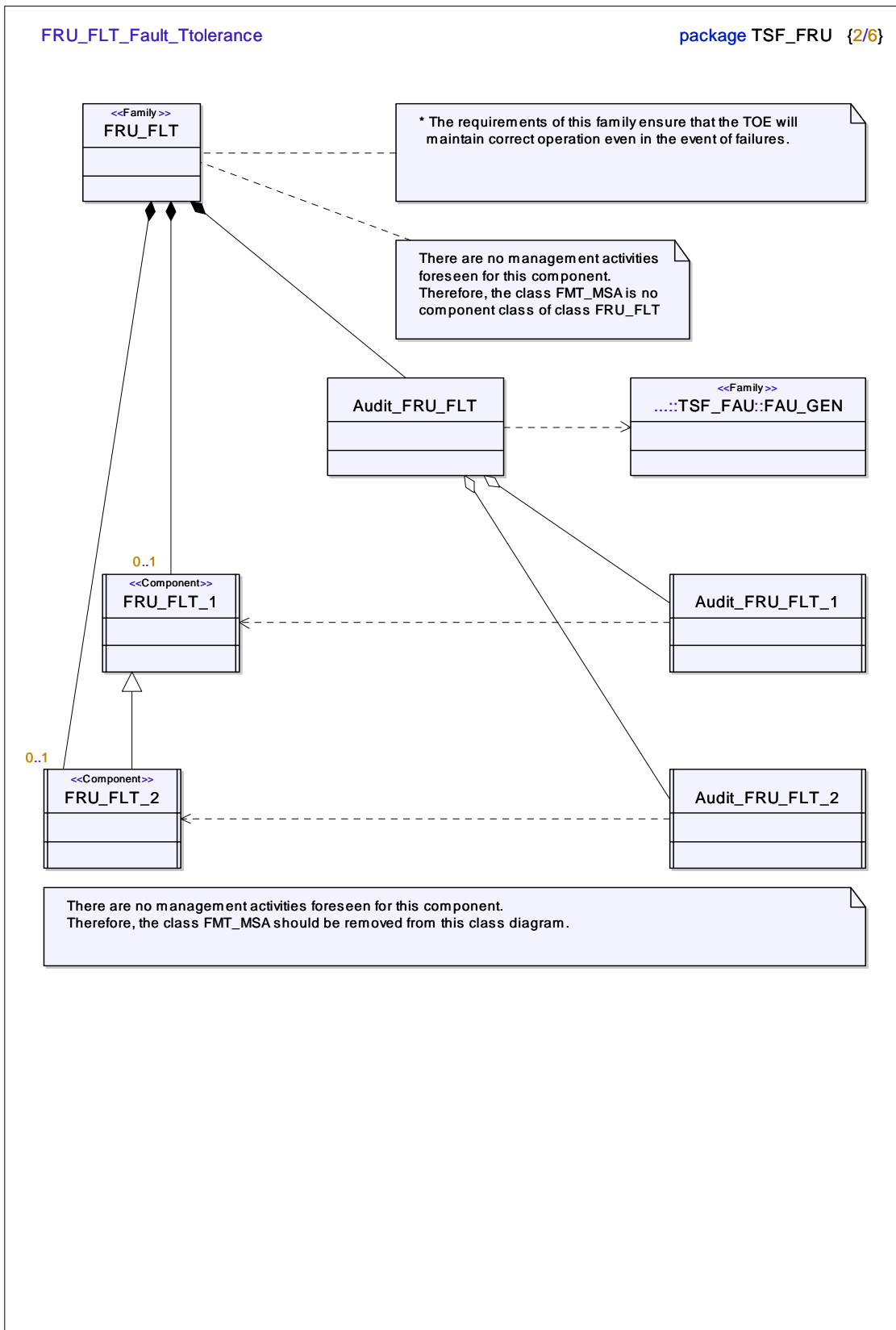
FPT_AuditEvents

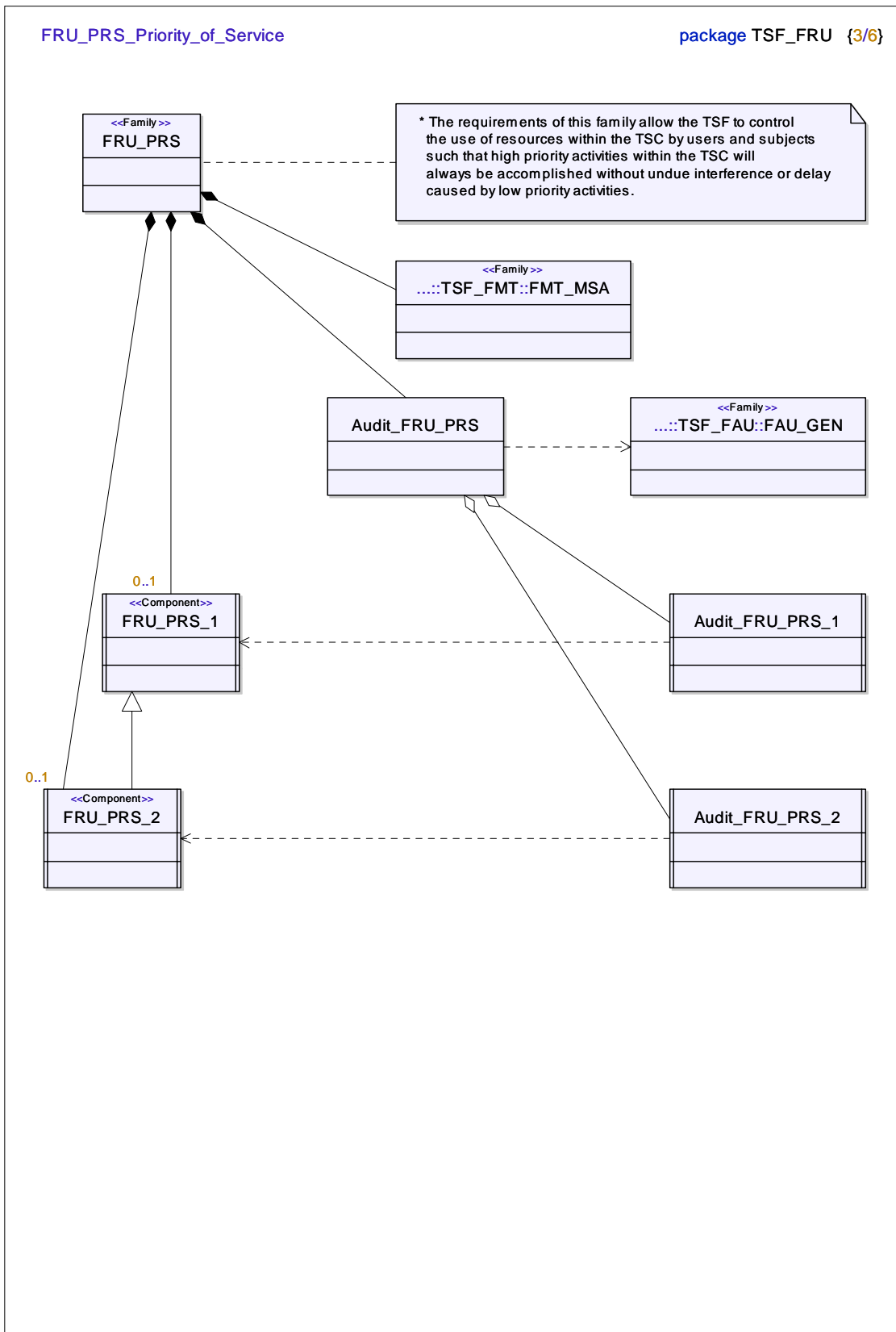
package TSF_FPT {21/21}

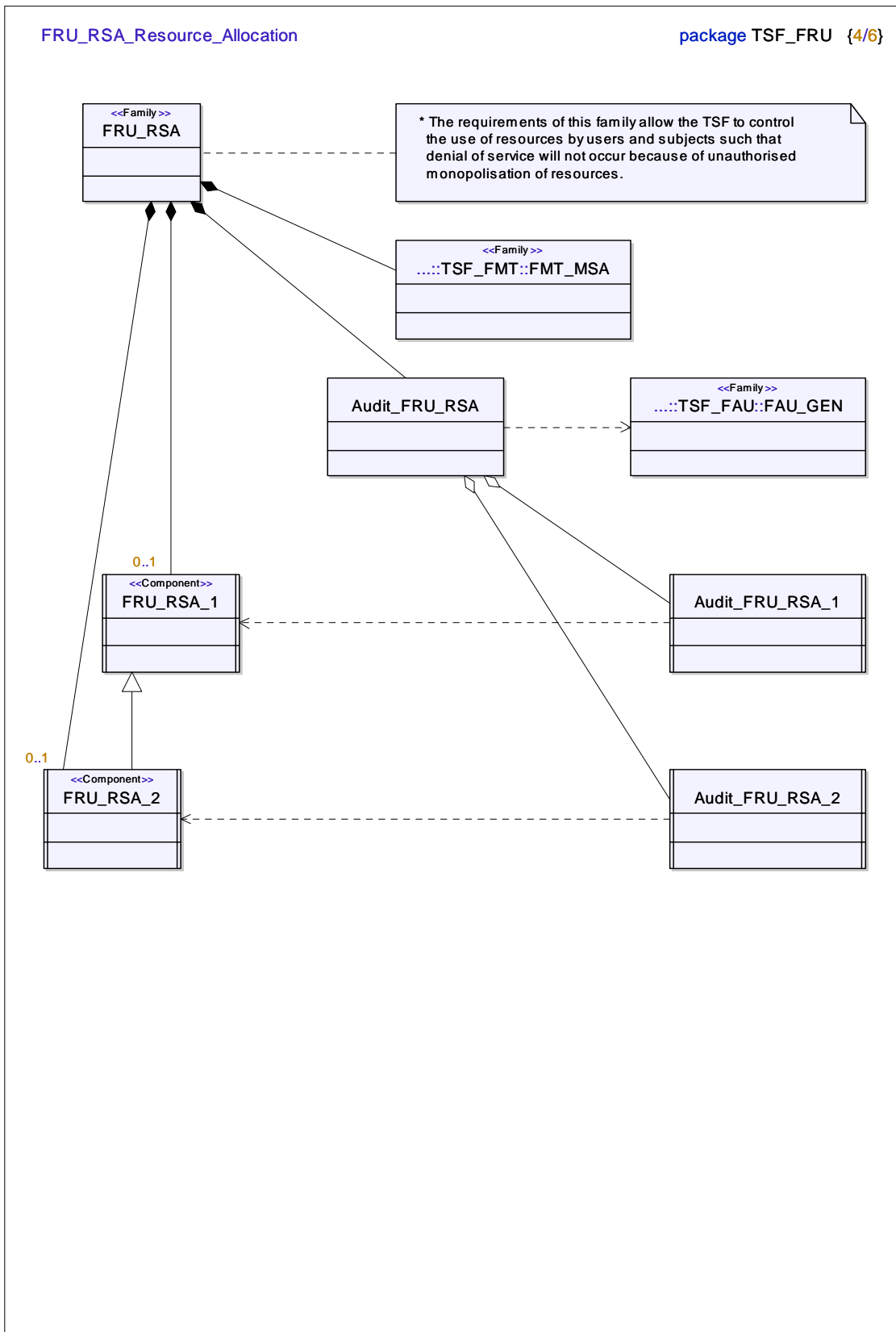


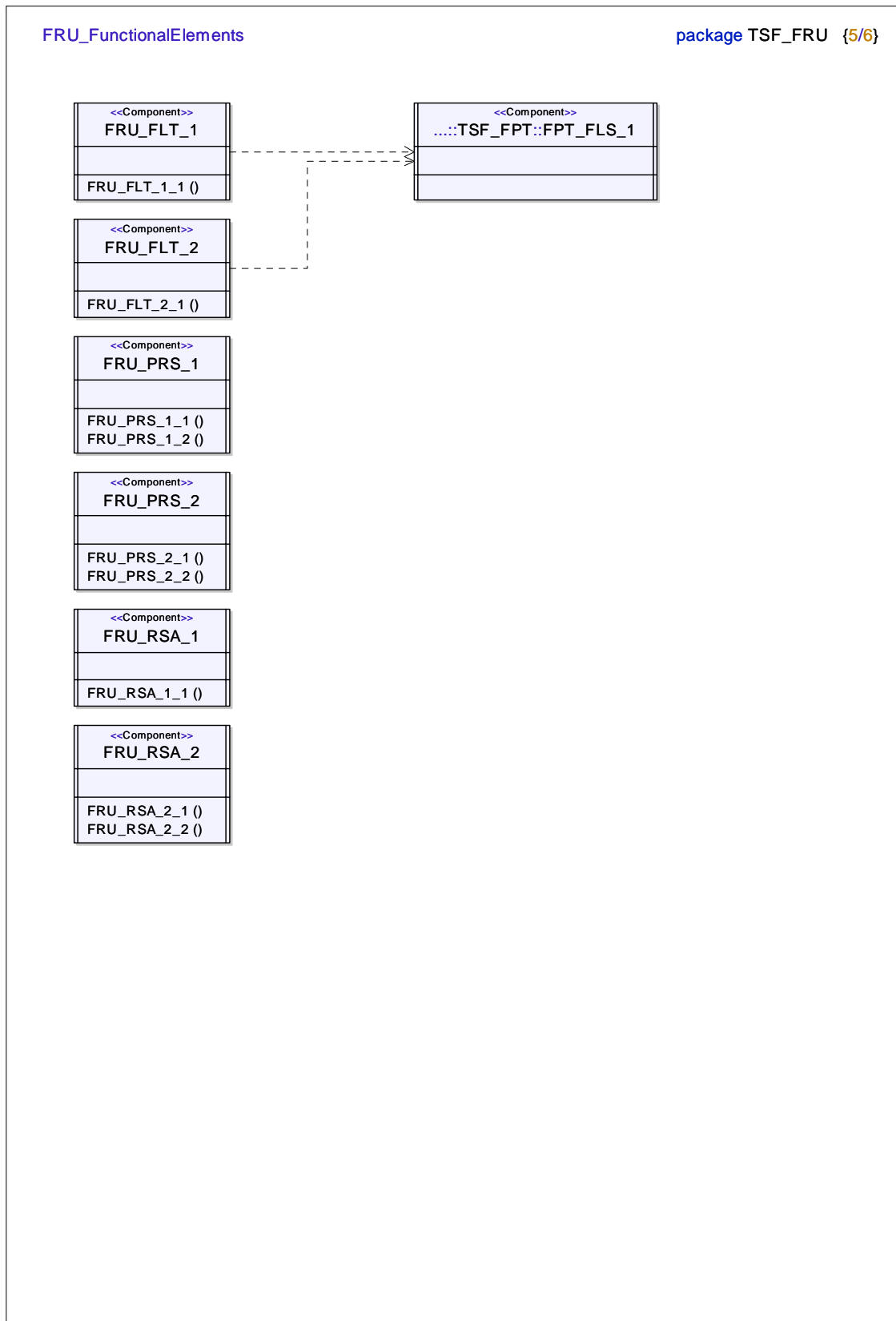
A.3.9 Package TSF_FRU











FRU_AuditEvents

package TSF_FRU {6/6}

Audit_FRU_FLT_1
auAnyFailure () auAllCapabDiscontinued ()

Audit_FRU_RSA_1
auRejAllocResrcLimits () auAllUseAtmptResrcLimits ()

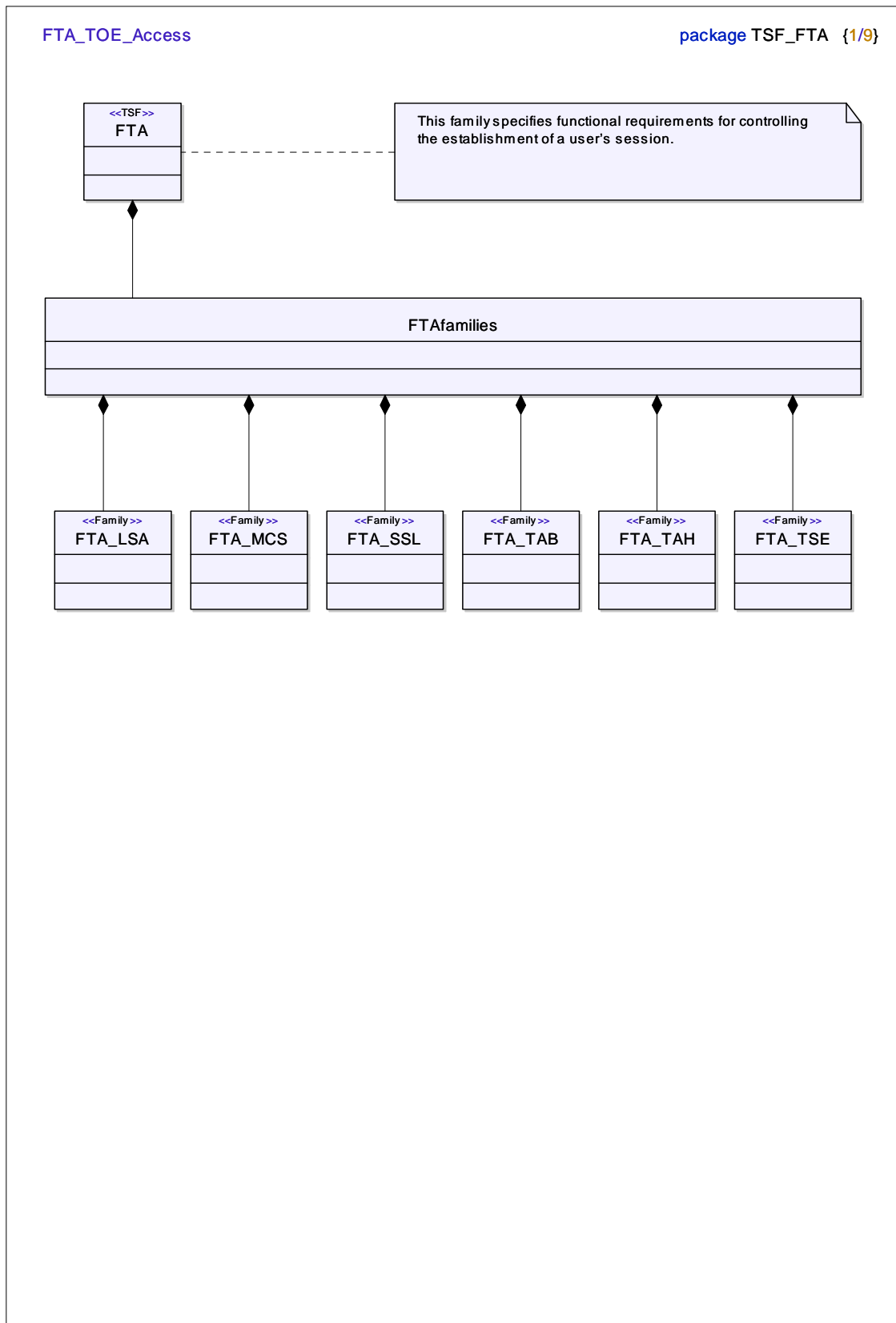
Audit_FRU_FLT_2
auAnyFailure ()

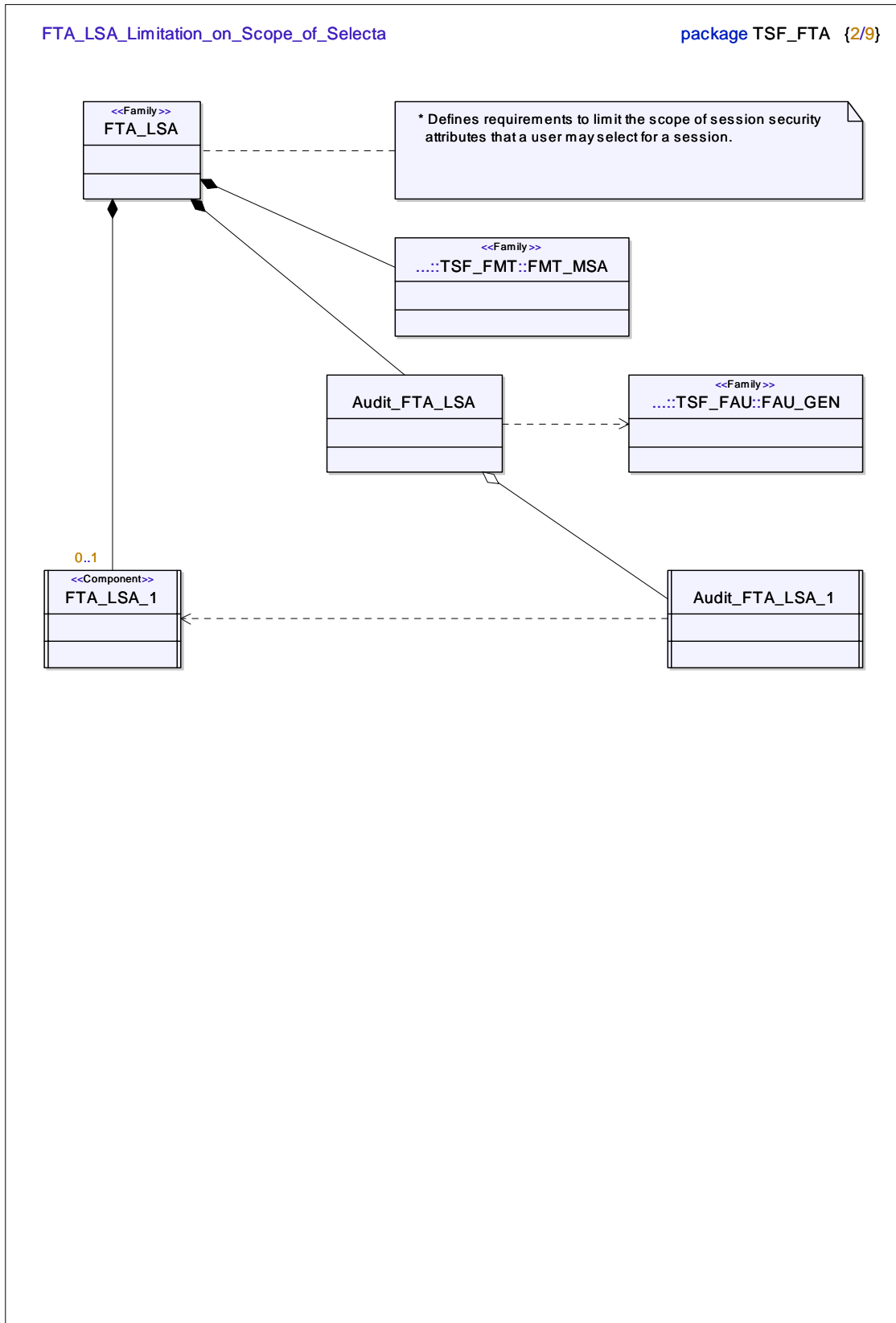
Audit_FRU_RSA_2
auRejAllocResrcLimits () auAllUseAtmptResrcLimits ()

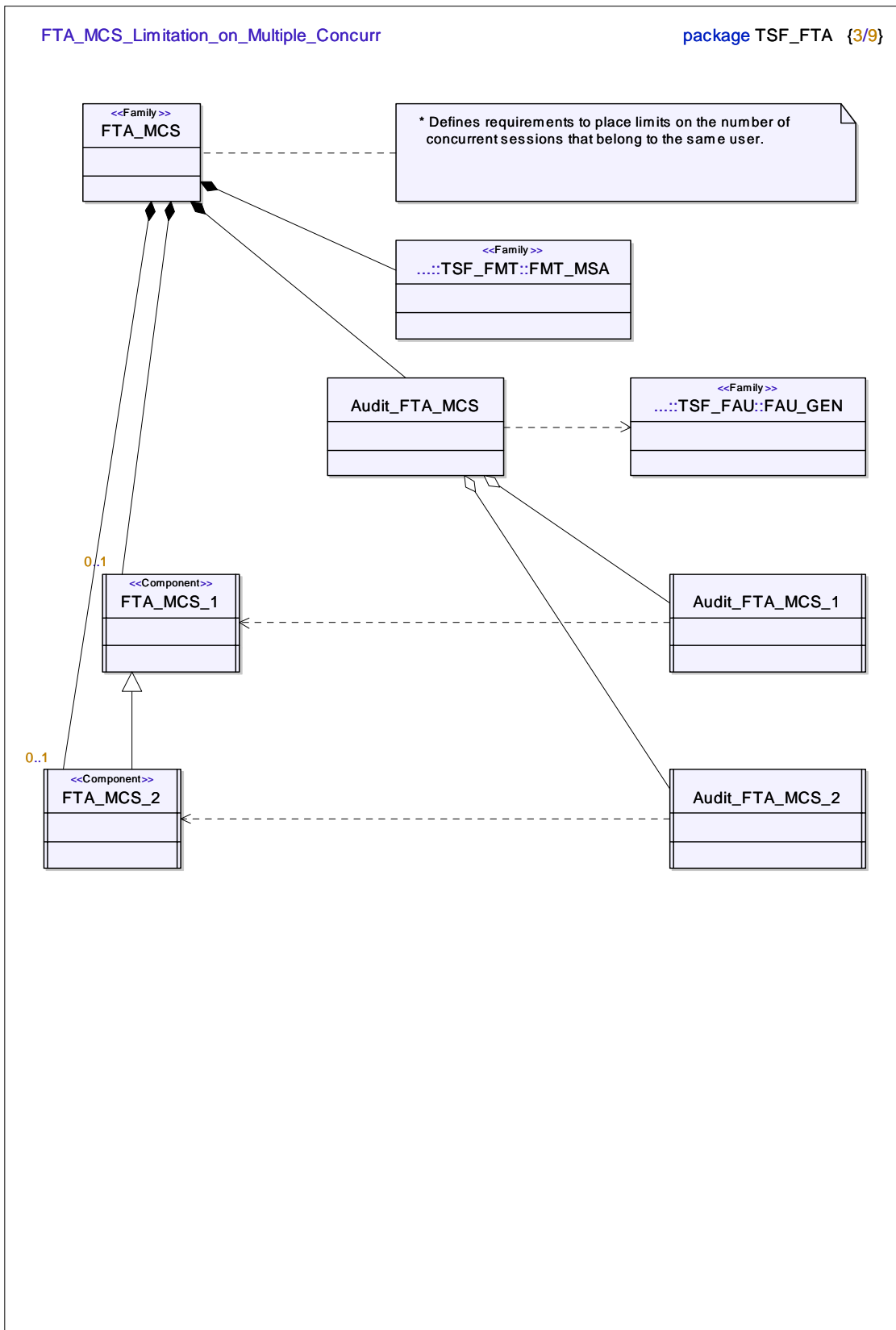
Audit_FRU_PRS_1
auOPRejDuePriority () auAllUseAtmptDuePriority ()

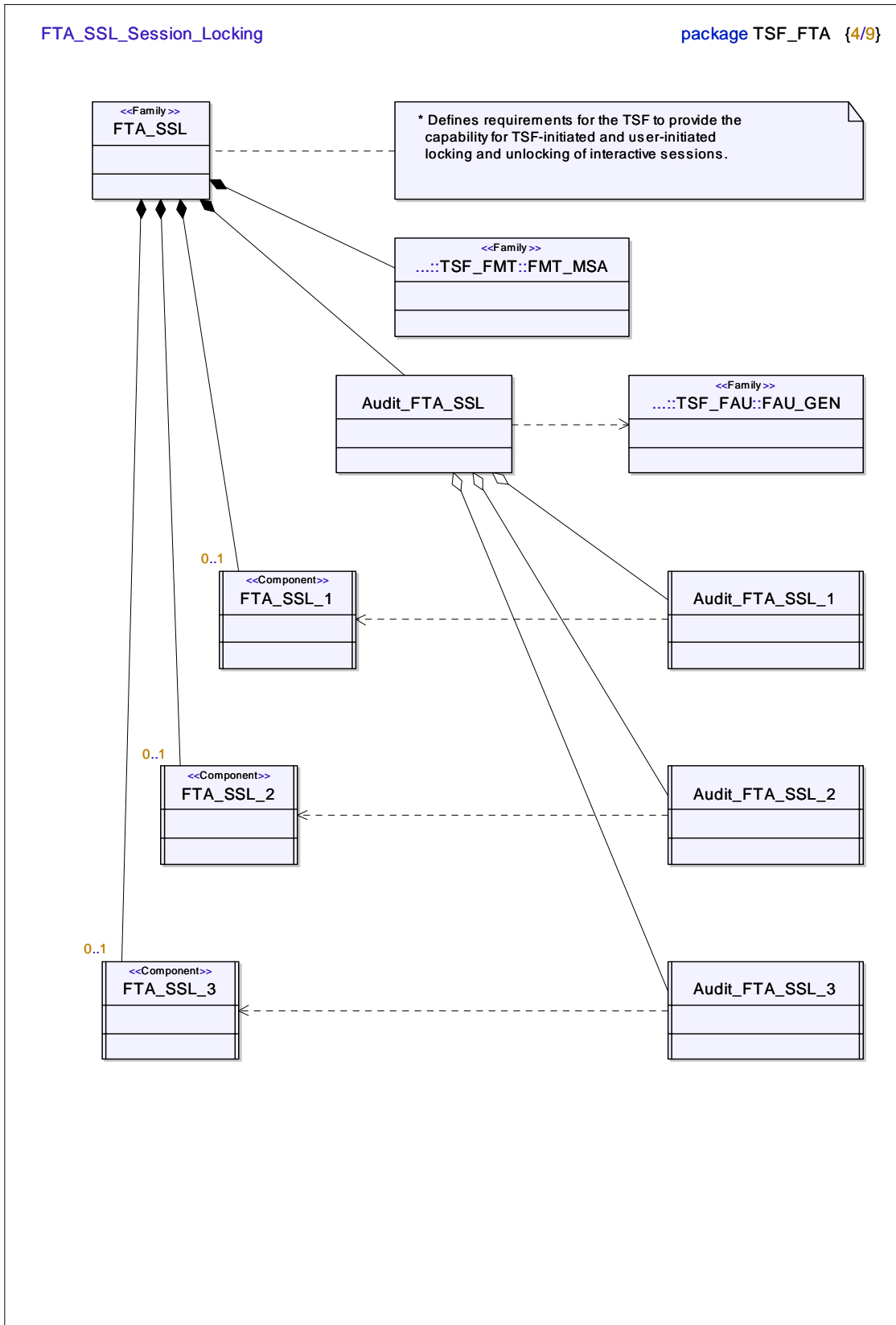
Audit_FRU_PRS_2
auOPRejDuePriority () auAllUseAtmptDuePriority ()

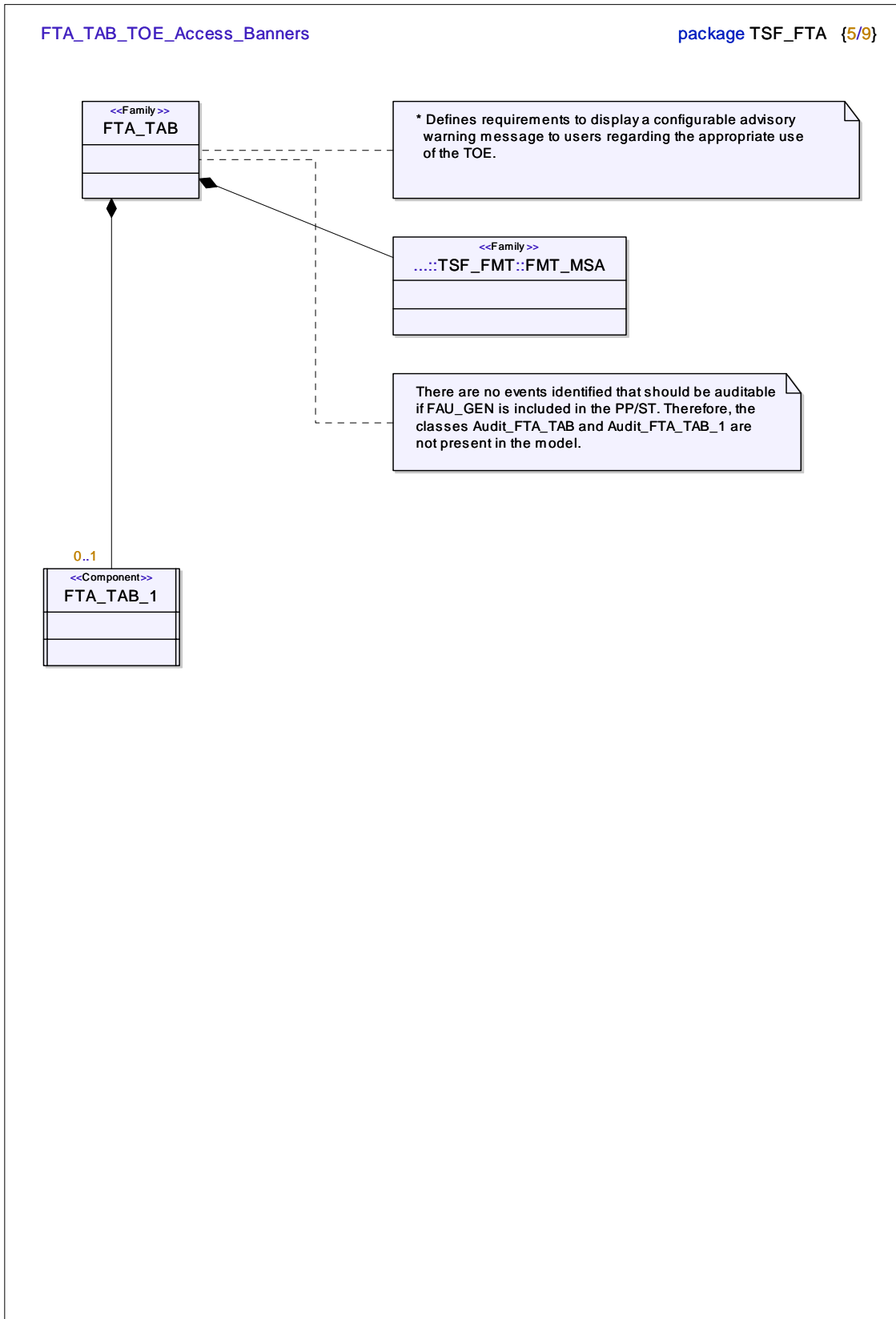
A.3.10 Package TSF_FTA

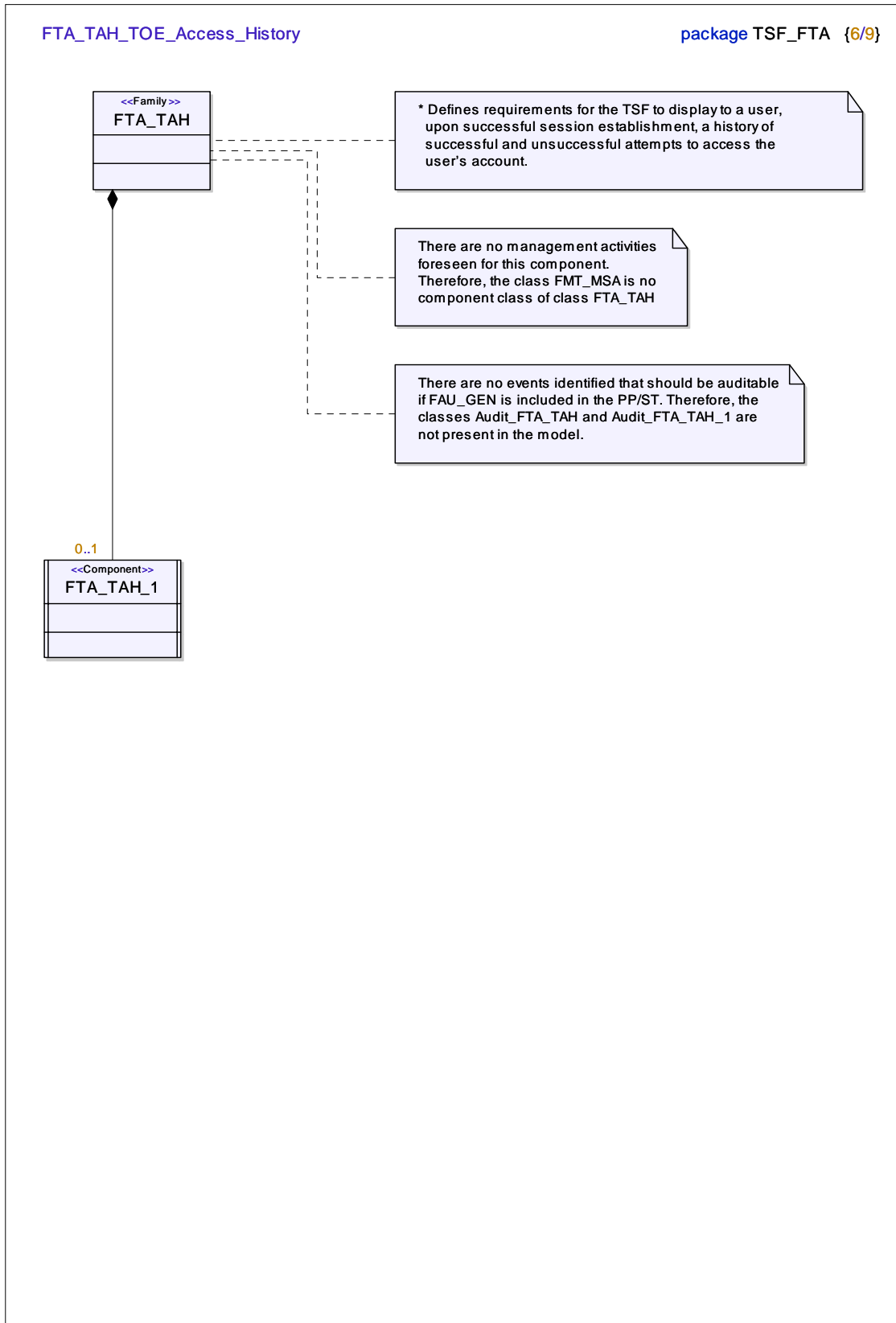


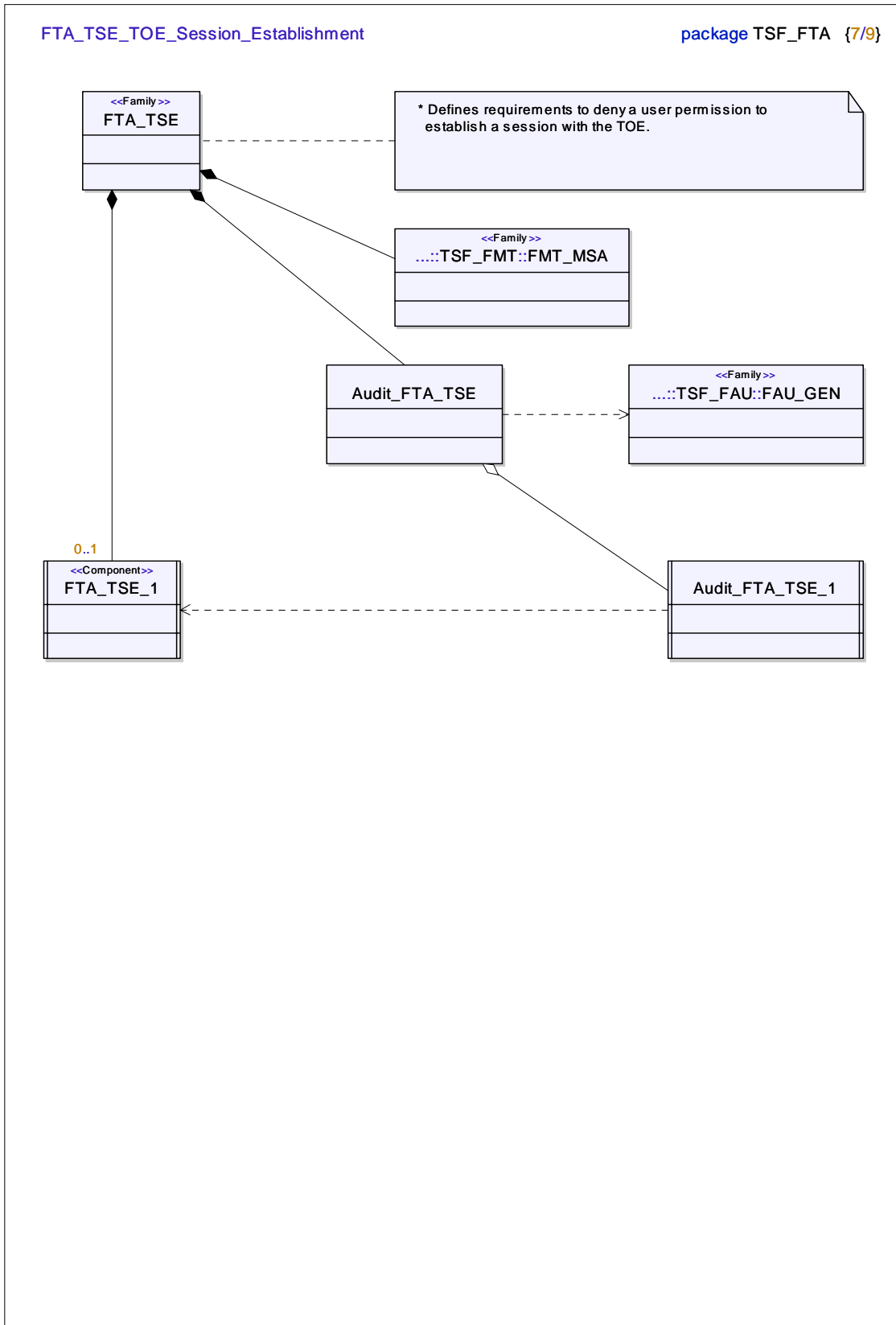


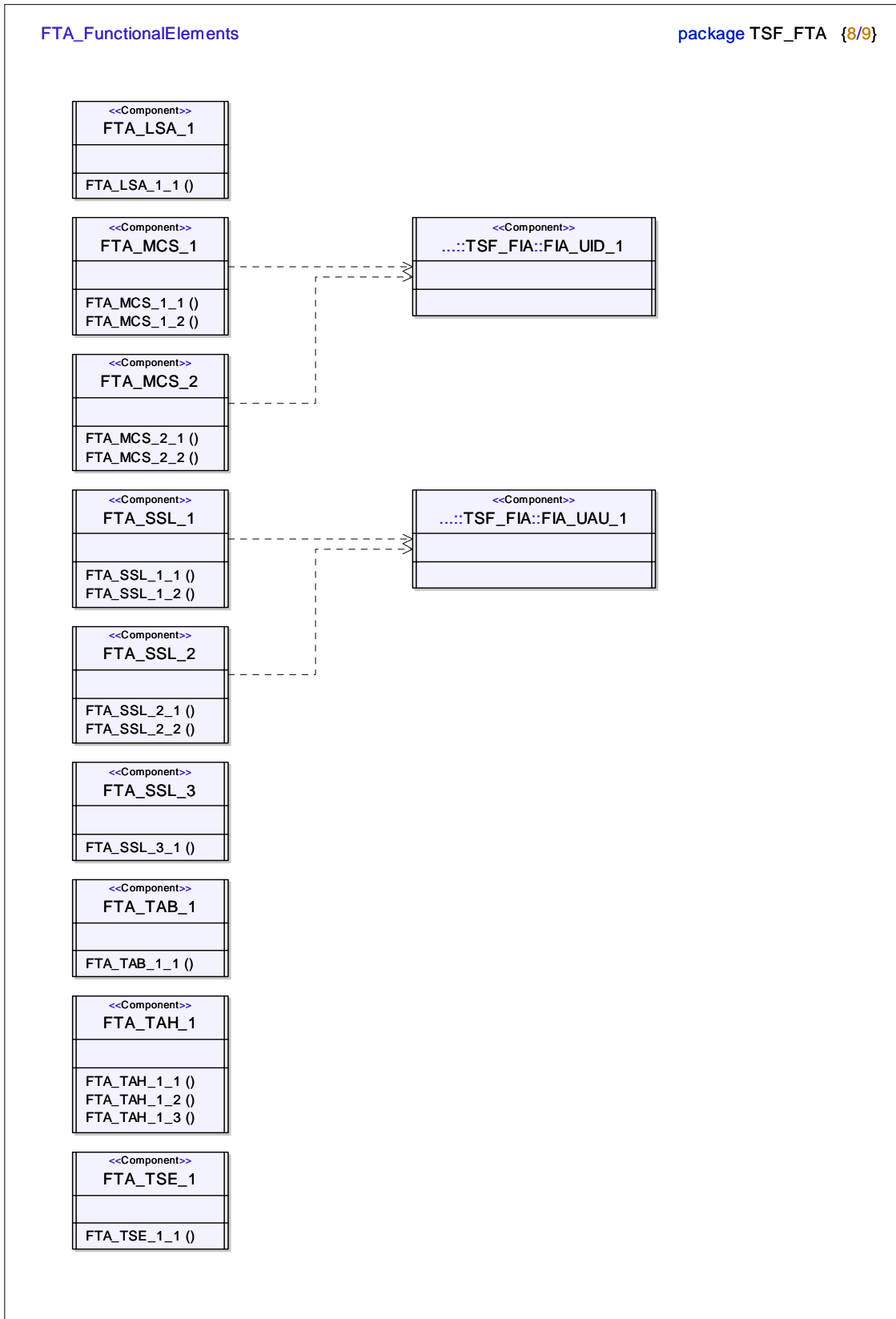












FTA_AuditEvents

package TSF_FTA {9/9}

Audit_FTA_LSA_1
auAllFailAtmpt2SessSecAttr ()
auAllAtmptSessSecAttr ()
auCaptValuesSessSecAttr ()

Audit_FTA_MCS_1
auTooManyNewSess ()
auNrCurrenUsrSessAttr ()

Audit_FTA_MCS_2
auTooManyNewSess ()
auNrCurrenUsrSessAttr ()

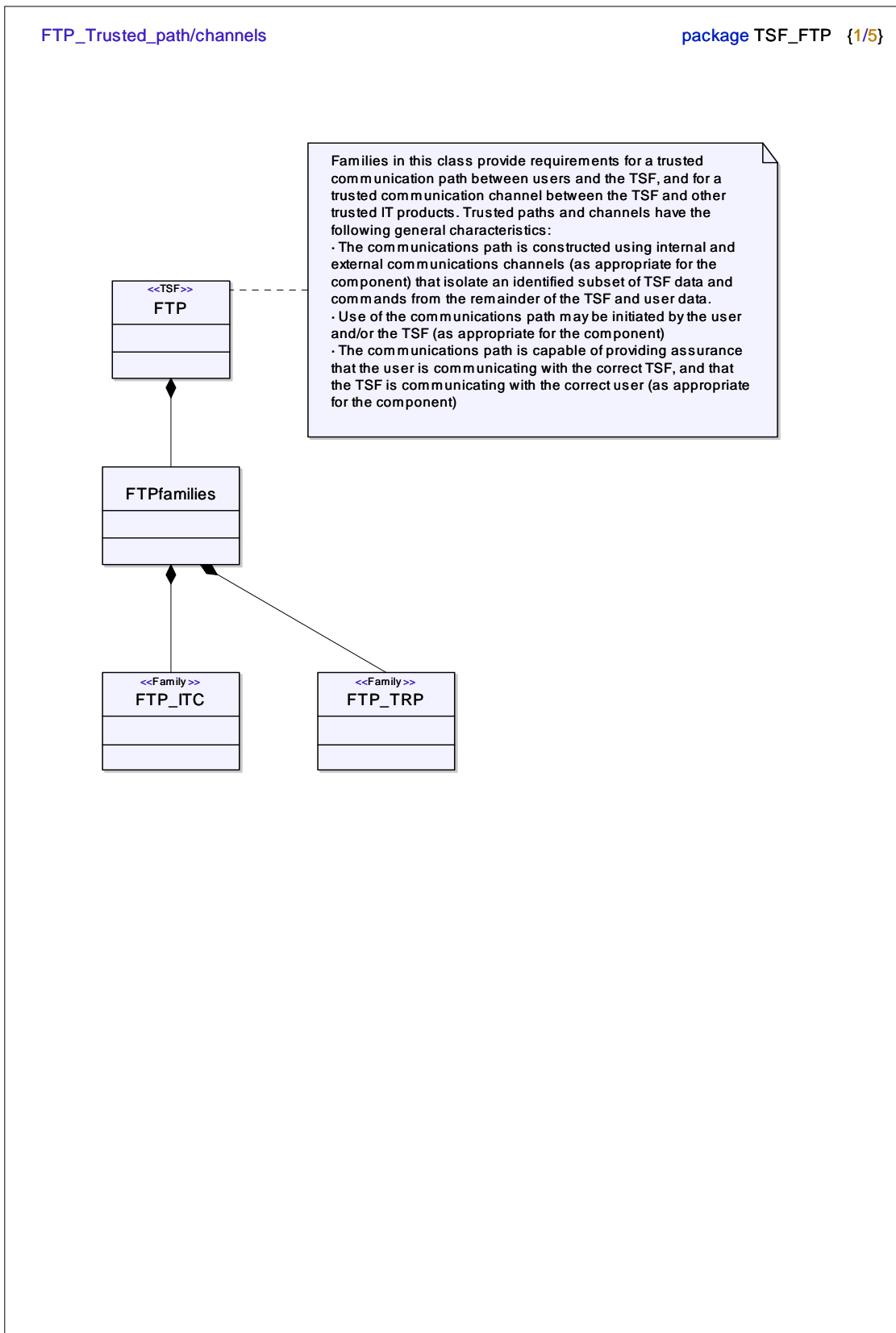
Audit_FTA_SSL_1
auLockIntractvSess ()
auUnlockIntractvSess ()
auAllAtmptUnlockSess ()

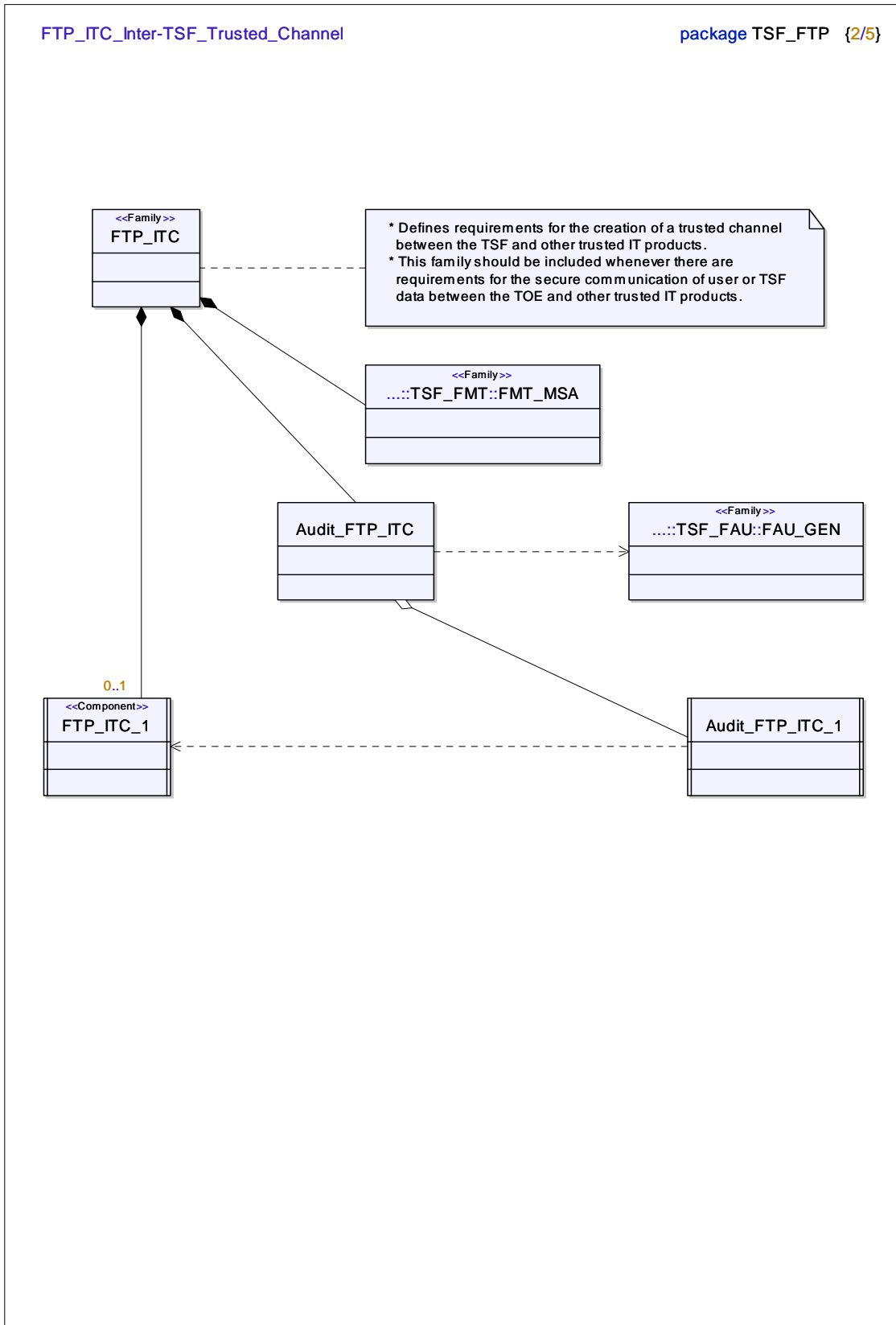
Audit_FTA_SSL_2
auLockIntractvSess ()
auUnlockIntractvSess ()
auAllAtmptUnlockSess ()

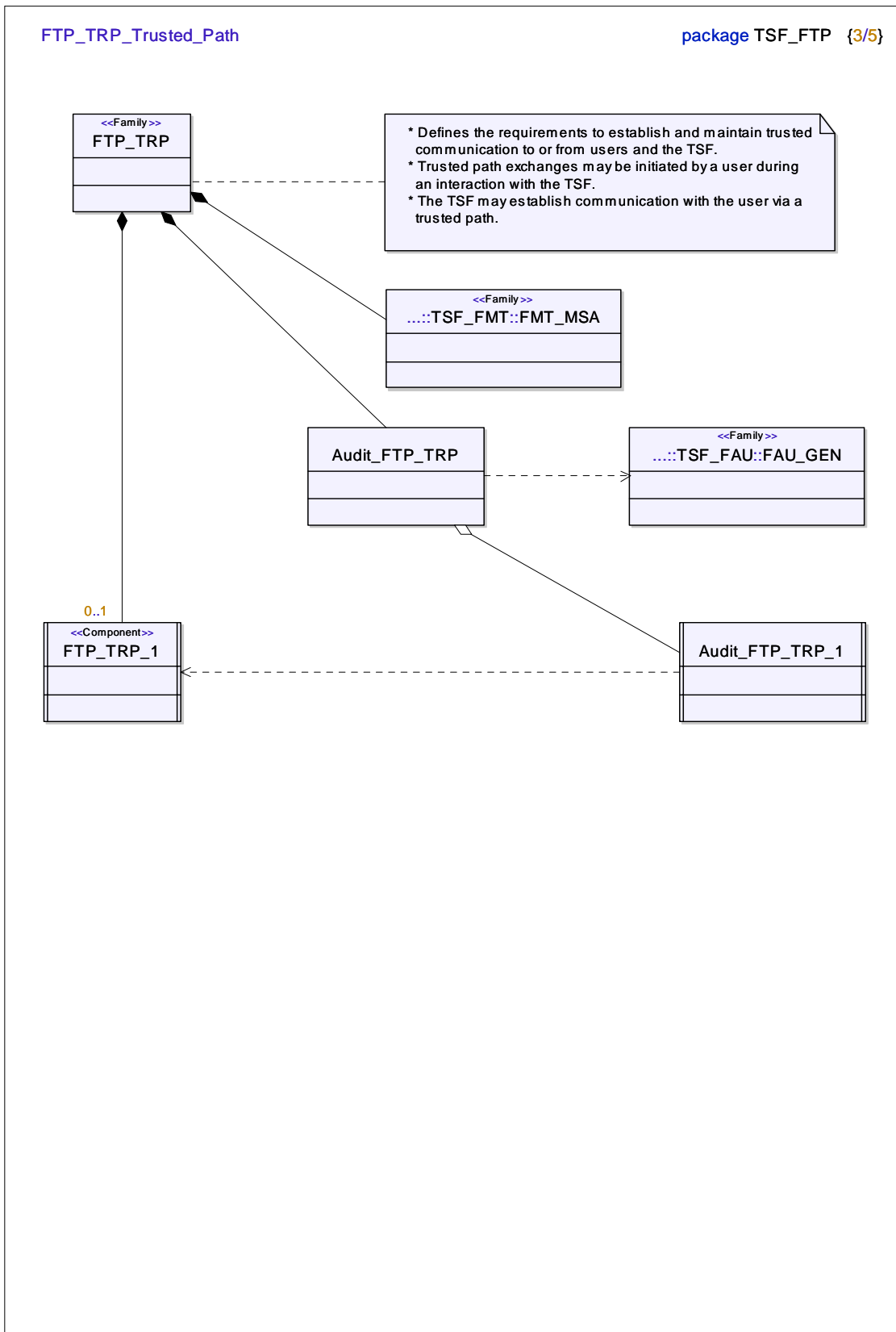
Audit_FTA_SSL_3
auTerminationIntractvSess ()

Audit_FTA_TSE_1
auDenialSessEstabl ()
auAllAtmptSess Establ ()
auCaptrAccessParam ()

A.3.11 Package TSF_FTP

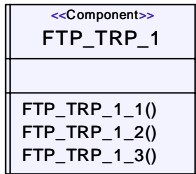
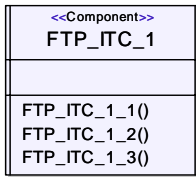






FTP_FunctionalElements

package TSF_FTP {4/5}



FTP_AuditEvents

package TSF_FTP {5/5}

Audit_FTP_ITC_1
auTrustedCHFail ()
auIDSrcDestCHFail ()
auAllTrustedCHUses ()
auIDSrcDestCHUses ()

Audit_FTP_TRP_1
auTrustedPathFail ()
auIDAssocPathFail ()
auAllTrustedPathUses ()
auIDAssocPathInvoc ()

History

Document history		
V1.1.1	May 2005	Publication