AeroSpace and Defence
Industries Association of Europe

ASD STRATEGIC STANDARDISATION GROUP

TDP Message Header DEX Specification

Rev1.0, 05/10/2012

Ref: **ASD/TDPMHDEX/1.0**

Confidentiality level: **Public document**

Executive Summary

This document provides the definition of the TDP Message Header DEX, developed by the "TDP Message" working group sponsored by the ASD Strategic Standardisation Group (SSG).

The main Business Case motivating this TDP Message Header DEX specification is the secure files transfer/transportation of Technical Data Packages (TDPs) supported by a PLM Hub, such as BoostAerospace or PHUSION.

This specification is established as an ASD SSG Business DEX.

It is envisaged, in a second step, to propose this specification as an OASIS DEX.

This specification has been implemented and validated in two different platforms: BoostAerospace or PHUSION.

ASD SSG is seeking a wide dissemination and exploitation of this open specification, considering that this TDP exchange mechanism is universally required by the Industry and still requires standardisation.

List of Contributors

	Name	Organisation	Role / Title
Deliverable Leader	Nicolas Figay	EADS	
Contributing Author(s)	Jean Brangé	AFNET	
	Ramòn Somoza	Airbus Military	
	Alexandre Fournier	Boost Conseil	
		CASSIDIAN	
Internal Reviewer(s)	ASD SSG Members		
Process Auditor	Yves Baudier	EADS	ASD SSG Chair

Document History

Version	Date	Reason of change
0.1	09/02/2011	Document created
0.2	17/09/2011	Several sections added.
0.3	10/10/2011	inclusion of feedback from reviews performed by Carsten Zerbst and Yannick Fourastier
1.0	05/10/2012	Document updated to SSG format after approval by ASD SSG members.

Table of Contents

List of figures

List of acronyms / abbreviations used in this document

Acronym / abbreviation	Definition
AP203	Standard for the Exchange of Product model data (STEP - ISO 10303) - Application Protocol 203 "Configuration controlled 3D design of mechanical parts and assemblies"
AP214	Standard for the Exchange of Product model data (STEP - ISO 10303) Application Protocol 214 "Core data for automotive mechanical design processes"
AP239	Standard for the Exchange of Product model data (STEP - ISO 10303) Application Protocol 239 - Product Life Cycle Support (PLCS)
BoostAeroSpace	European Hub providing secure collaboration solutions and business process integration for Aerospace and Defense (A&D) industry. See www.boostaerospace.com
BRD	Business Requirement Definition??????????
CAD	Computer-Aided Design
CMS	Cryptographic Message Syntax (IETF standard)
DEX	Data Exchange Specification (PLCS terminology)
OASIS	Organization for the Advancement of Structured Information Standards. See www.oasis-open.org
PDM Schema	STEP PDM (Product Data Management) Schema
PHUSION	EADS interchange hub (from EADS PHC project)
PKCS	Public-Key Cryptography Standards
PLCS	Product Life-Cycle Support
PLM	Product Life-cycle Management
SSG	ASD Strategic Standardisation Group, see www.asd-ssg.org
SSRS	SQL Server Reporting Services
TDP	Technical Data Package
TSCP	Transglobal Secure Collaboration Program. See
TSCP ILH	Transglobal Secure Collaboration Program – Information Labeling and Handling
XML	

1 Introduction

1.1 Purpose of the document

This document describes the ASD **Technical Data Package (TDP) Message Header DEX Specification**.

It includes recommendations on the way to populate TDP Message Header files when dealing with secure files transfer/transportation supported by a PLM Hub, such as BoostAeroSpace or PHUSION, which is the main Business Case motivating the TDP Message Header DEX Specification.

1.2 Content of the document

The document includes:

- Description of the information handled by the TDP Message Header DEX Specification (Chapter 2), including:
  - Envelop and message
  - Associated date and time
  - Encryption key
  - Signature of the TDP
  - Sender and Receivers as identified persons in organization
  - Files and related information
  - Security classification, export control and banned countries
  - Context of the exchange
- Description of the Data Schema used (Chapter 3)
- Description of the mapping of the TDP Message Header information on the Data Schema (Chapter 4)
- Reference to a set of annexes providing technical models to be used for implementation.

2 Information handled by the TDP Message Header

The information contained in the TDP Message Header is the following:

2.1 Envelop and Message

When creating a TDP message header, first a message is created, with an identifier and content, and then an envelope is created for the sending, for which transportation information is provided.

2.2 Associated date and time

This is the date of sending of the message.

2.3 Encryption Key

This is the key used to encrypt the files within the Technical Data Package. Note that the TDP Message Header itself is not encrypted. Encryption process allows the TDP content to be read only by targeted receivers, as the encryption key is encrypted itself in a way it can be decrypted only by the intended recipients.

2.4 Signature of the TDP

To ensure that no one changed the TDP Message Header during transfer, a signature could be used. In such a case, it should be contained in the header. The signature is created using the private key of the sender and is attached to the envelope.

2.5 Sender and Receivers as identified persons in organization

The TDP Message Header contains identification of the sender and the receivers, who are persons inside organizations. It means that, if a person belongs to several companies, this will correspond to several persons in organizations. Let's notice that for each person in organization, a certificate is used in order to be able to authenticate the person as an employee of the collaborating organization.

Note: ability to send TDP to a given role is also a possibility, even if not supported by current processes within current HUB pilot implementation due to security constraints.

2.6 Files and related information

The content of a TDP is a set of files which have to be transferred from an organization to another organization(s). This includes documents and CAD models, plus a "Product metadata" file, based on such or such application protocol, and which is used by PDM Systems or CAD systems as metadata .

In Aerospace PLM hubs such as BootAeroSpace or PHUSION, a common subpart of AP203 and AP214 (PDMSchema) is used, based on AIM and Part21. One particular file declared in the TDP Message Header should be indicated as the 'masterfile', which will be the file from which the entire set of data could be accessed. It corresponds to the "Product metadata" file.

2.7 Security classification, export control and banned countries

It should be possible to indicate security classification of the content of the TDP, in order to avoid communicating some classified information where some regulation needs to be applied. The security classification depends on the business context.

In addition, it should be possible to indicate export control restriction when needed, as well as a list of allowed or denied countries consistently with the regulation.

Note: such restriction or authorization could be as well linked to the used classification - which can be used in order to decide who can or cannot be a receiver. So usage of export control tag related to such or such country remains an open discussion if willing to find the more appropriate and easy way to implement. Those properties should be considered consistently with the TSCP ILH1, for information labelling and handling.

Some default security information should be defined for the TDP content, with ability to add a particular security label on some files.

Example: compliance with SSRS and BRD requirements for sensitive data to be security tagged and filtered with associated relevant actions.

2.8 Context of the exchange

In order to route properly the TDP, some contextual information can be added, such as Program, Work package or Configuration.

Contextual information may be extended according needs, but it is then related to some specific needs.

Extending contextual information is usually made by assigning textual properties, attached to the envelope or to the message. It is recommended not to add information which is dedicated to any other need than transfer and secured transportation. The naming of the property should be based on existing standards adopted by the concerned community. Mechanism related to textual property assignment is for example used for security information. In this example, naming of properties is based on CMS / PKCS #7#, which is a security standard adopted by security officers in most of the Aeronautic and Defense companies for secure messaging.

The TDP message specifications doesn't enforce usage of such or such algorithm or security standard, but provide a standardized way to security related data inside the TDP message header using the TDP message header schema.

Let's note that contextual information is dedicated only to the transfer. It must not be used by target systems such as PDM systems or CAD Systems. It means that this information should be replicated in the "Product metadata" file, dedicated to these systems. It ensures the separation between secured TDP files transfer and Product Data interchange. Such replication also occurs for files, which are both described in TDP message header in order to validate the secured transfer, and in Product metadata, in order to describe how these files are related to documents and Product structure(s).

2.9 Data Schema

The schema was initially defined a subset of the AP239 information model, as:

- AP239 was the only Application Protocol including message and envelop modules
- It was envisaged to define a TDP Message Header DEX inside the OASIS PLCS scope, which provides for each DEX a schema and information model which is a subset of AP239, of use for the Business Processes supported by the DEX.

In the reverse, it should be clear the TDP Message Header is not AP239, and that its usage doesn't have to comply with any recommended practice related to AP239 or PLCS DEXs. TDP message header standardization project is the one to provide the recommendation for the usage of this schema. Formalized textually, it will eventually be formalized as a DEX, or ASD SSG DEX, or OASIS PLCS DEX. It will depend on the required efforts and on the robustness of the OASIS PLCS DEXLIB .

In addition, some complex mechanisms such as external classifications based on Reference Data libraries are avoided, as it is not accurate when comparing required efforts and benefits.

The schema is formalized first in EXPRESS, and then in XML (the Part 28 default configuration – as for PLCS). This is motivated by the fact that the exchanged are implemented using XML and not Part 21. It is based on the Application Reference Model and not on the Application Integrated Model.

The schema is versioned, as it may evolve within the time.

The current version is 1.0. Reference is provided in annex.

3 Mapping

3.1 Introduction

The mapping consists in describing how the TDP message information is formalized using the schema by mean of diagrams and tables.

3.2 Envelop and Message

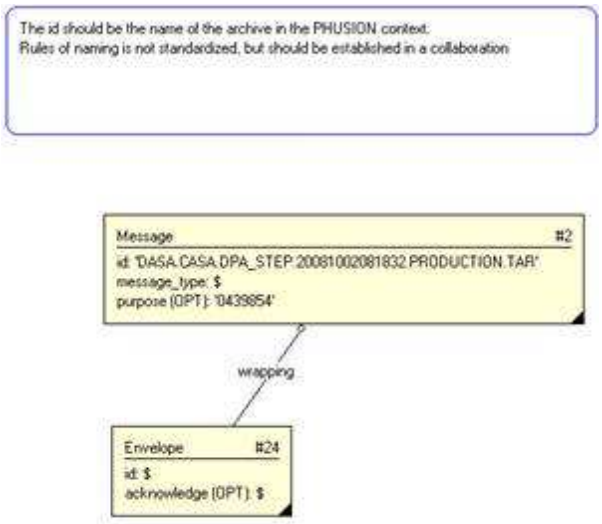

Figure 1: Envelop and Message

Message	
id	It is required information. It should be the name of the archive file containing the Technical Data Package
message_type	This is a mandatory file, with as value a set of predefined values which have been defined by the collaboration context.
Purpose	It is an optional attribute, which can be used in order to indicate the purpose of the message. It could be used by the hubs in order to indicate motivation of the sending, for people and not for applications. It is consequently not subject to automation.
Envelope	
Id	It is required attribute.
Acknowledge	This field could be used as a mechanism in order to provide feedback concerning success or not for different steps in the process of secured transfer of the TDP. Such notification can also be taken into account by other mechanisms and technologies. If used, the different value of the acknowledgment should be agreed by the partners involved in a same program and using the same

	hubs.

3.3 Associated date and time

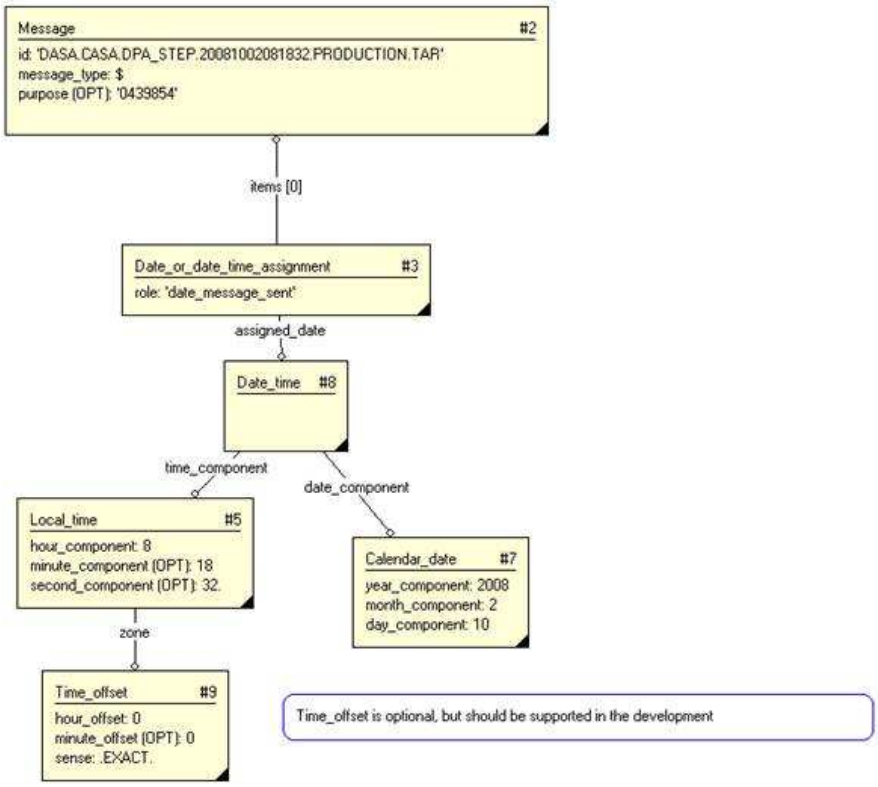

Figure 2: Associated date and time

Precise data of sending is required, including offset, as collaboration can be made with multiple sites distributed in numerous countries.

This way of indicating dates is the recommended one.

Note: some alternative way could be used, using standardized way to represent date and time in XML. It is currently not included in recommended practice, but it is a matter of evolution in the future.

Date_or_date_time_assignement	
Role	It indicated the kind of data or date time that is assigned. The sending date must be provided, and in this case, the role value must be “date_message_sent”. For other kind of time or date time information which could be used, partners have to agree on the value to use for the role of each date.
Date_time	

Local_time	
Hour_component	Mandatory
Minute_component	Mandatory
Second_component	Mandatory
Calendar_date	
Year_component	Mandatory
Month_component	Mandatory
Day_component	Mandatory
Time_offset	
Hour_offset	Mandatory
Minute_offset	Mandatory
sense	Mandotory

3.4 Encryption Key

Usually, all the files in the Technical Data Package are digested and encrypted in order to respond to security requirements.

The same encryption algorithm and the same encryption key are used for each file of the TDP, except the TDP message header which is not encrypted.

Encryption algorithm and encryption key are to be provided as assigned textual property, with as name of the properties names which are those of the elected security standards in the community.

In the particular case of Aerospace and Defense in Europe, the standard of reference for digesting and encryption is CMS / PKCS #7#, and may evolve to usage of W3_DisiSig / SOAP-ENC. It is implemented on Hubs such as BoostAerospace or EADS PHUSION.

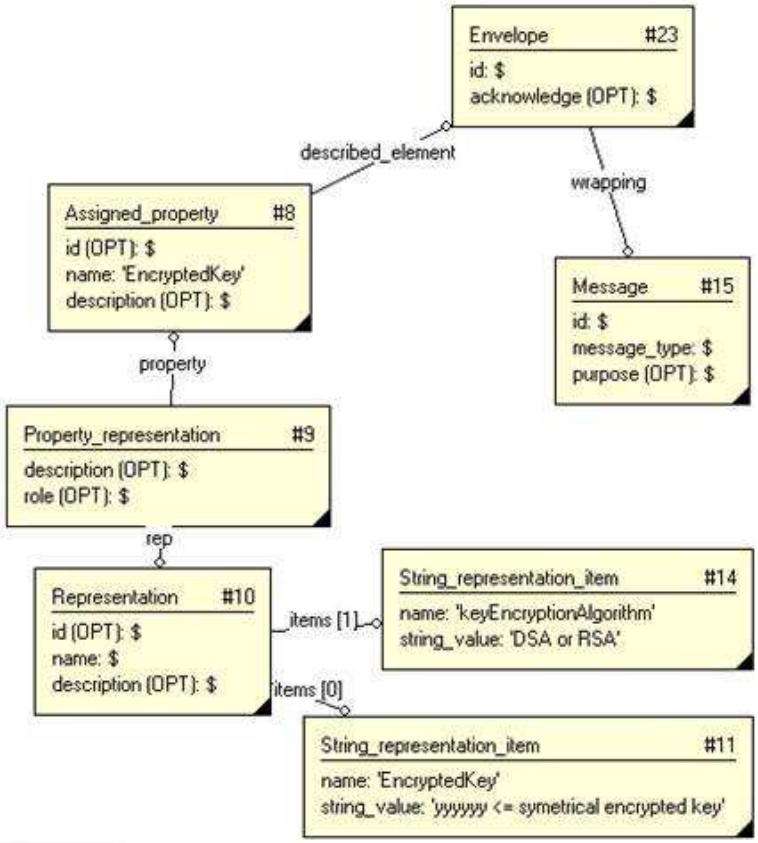

Figure 3: Encryption key

Assigned_property	
Role	Mandaroty filed, with as value “EncryptedKey”
Id	Optional field
Description	Optional field
Property_representation	
Id	Optional field
Acknowledge	Optional field
Representation	
Id	Optional field
Name	Optional field
Description	Optional field
String_representation_item for key Encryption Algorithm	
Name	Mandatory field. When CMS / PKCS#7# is the security standard to apply, the value must be “keyEncryptionAlgorithm”. If W3C_DisiSig / SOAP-ENC adopted, it could be other relevant names.
String_value	Mandatory field.

	When CMS / PKCS#7# is the security standard to apply, the value must be the symmetrical encrypted key string as defined by PKCS#7#. For example, it can be AES or Blowfish algorithm. If W3C_DisiSig / SOAP-ENC adopted, it could be other relevant values.
String_representation_item for encrypted key	
Name	Mandatory field. When CMS / PKCS#7# is the security standard to apply, the value must be "EncryptedKey". If W3C_DisiSig / SOAP-ENC adopted, it could be other relevant names.
String value	Mandatory field. When PKCS#7# is the security standard to apply, the value contains the key used for the symmetrical encryption of the associated archive. The symmetrical key is contained encrypted as CMS / PKCS #7# value and encoded as Base64.

Complementary information could be needed when using other security standards for encryption. In this case, the representation of the encryption key could be defined by adding other String_representation_item with a couple (name, string_value) indicating the name of required properties, extracted from the related standard, and its value.

Open Question: should we give a predefined name for property representation and representation which give more information on the adopted security policy for encryption?

3.5 Signature of the TDP

When the security implies signature of the TDP message, the signature must be attached to the message as a textual property.

In the following example, we consider that CMS / #PKCS7# is used, and described how it should be mapped to the TDP Message schema. In the future, other example could be given with W3C-Disig SOAP-ENC.

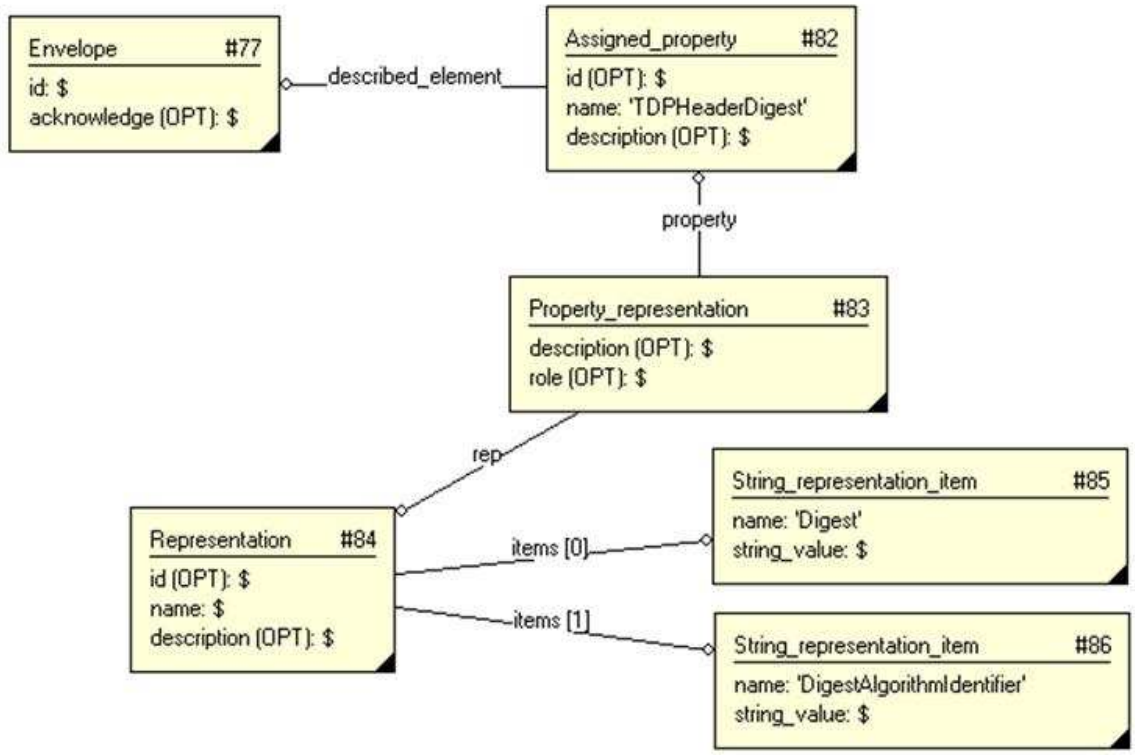

Figure 4: Signature of the TDP

Assigned_property	
id	Optional – Not taken into account
name	The value shall be “TDPHeaderDigest” when using CMS /#PKCS7#.
description	Optional
described_element	Mandatory : a link to the envelop of the TDP message
Property_representation	
description	Optional
role	Optional
property	Mandatory: a link to the assigned property

rep	Mandatory: a link to the representation
Representation	
id	Optional – not taken into account
name	Optional – not taken into account
description	Optional – not taken into account
Items	Mandatory: links to the digest and to the digest algorithm identifier string representation items
String_representation_item (Digest algorithm)	
name	Mandatory. If using CMS / #PKCS7 #, the name should be 'DigestAlgorithmIdentifier'. If using W3C-DisiG SOAP-ENC, the name should be an appropriate name for this standard.
string_value	Mandatory. It contains the identifier for the used signature algorithm, e.g. 'SHA1withDS'
String_representation_item (digest)	
name	Mandatory. If using CMS/ PKCS #7#, the name should be 'Digest. If using W3C-DisiG SOAP-ENC, the name should be an appropriate name for this standard.
string_value	Mandatory. It contains the signature. If CMS / #PKCS 7 # is used, it contains the Base64 and URL encoded signature.

3.6 Sender and Receivers as identified persons in organizations

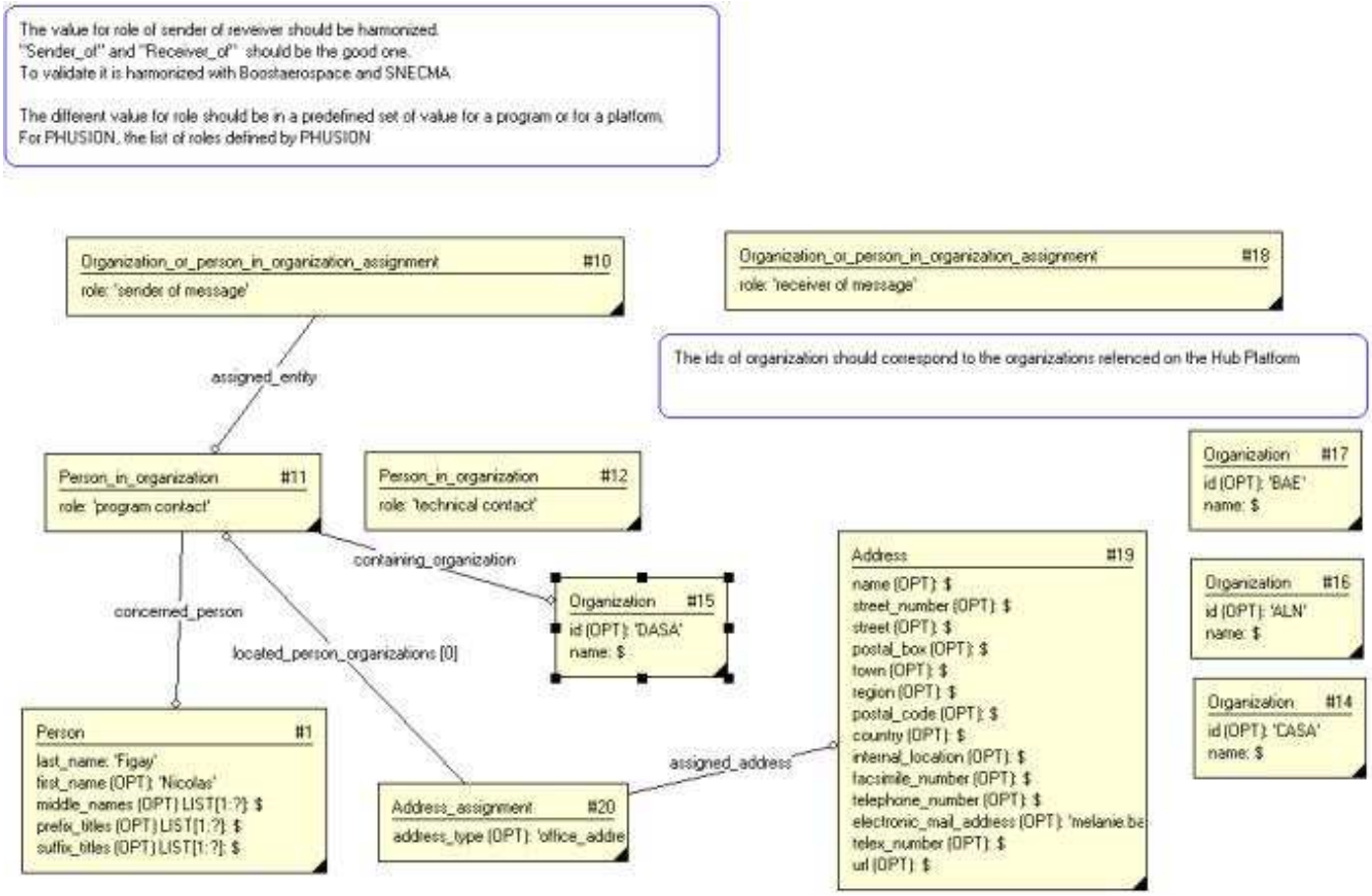

Figure 5: People and Organization

Organization_or_person_in_organization for the sender of the TDP	
Role	Mandatory field, with as value “Sender_of”
Organization_or_person_in_organization for a receiver of the TDP	
Role	Mandatory field, with as value “Receiver_of”
Person_in_organization	
Role	Mandatory field. This should provide the name or the code of the role of the sender. TDP message recommendation does not imply a set of predefined value. It is up to a Program or to a set of Program using a given hub to enforce a set of predefined values, that could be dedicated to people or to automate.
Person	
last_name	Mandatory field. It contains last (family) name of the person. If no distinguished input on first and last name is available, contains the concatenated value.

first_name	Mandatory field. It contains the first (Christian) name of the person. If no distinguished input on first and last name is available, it contains the concatenated value.
Middle_names	Optional
Prefer_titles	Optional
Suffic_titles	Optional
Address_assignment for address(es). Required if several addresses exist. Note that security policy may enforce usage of a single address, the one within the organization, in order to be aligned with certificate usage policies for authentication of the persons within organization.	
Address_type	Optional
Address – the address to provide will depend on the context, i.e. used system for the secured transfer and transportation. In particular, when notification is based on email, the Electronic_email_address is mandatory (case for EADS PHUSION or for BAS). For the other field, it will be based on practices agreed between the partners and on the authentication policies and processes. For example, federation of identity standards allows authentication without providing detailed information on the persons and their address.	
Name	Optional
Street_number	Optional
Street	Optional
Postal_box	Optional
Town	Optional
Region	Optional
Postal_code	Optional
Country	Optional
Internal_location	Optional
Facsimile_number	Optional
Telephone_number	Optional
Electronic_mail_adress	Optional
Telex_number	Optional
url	Optional

3.7 Certificates of the persons in organization

In order to ensure that the TDP is sent or received by authenticated persons in organizations, a certificate is to be provided and associated to person_in_organization.

Referring the practices in Aerospace and Defense, CMS / PKCS #7# is a standard of reference, and indicated that certificate should be provide through “Certificate” property. Certificate usually used are X509 certificates. The way to proceed will depend on security policies. It may evolve to usage of W3C_DisiSig / SOAP-ENC.

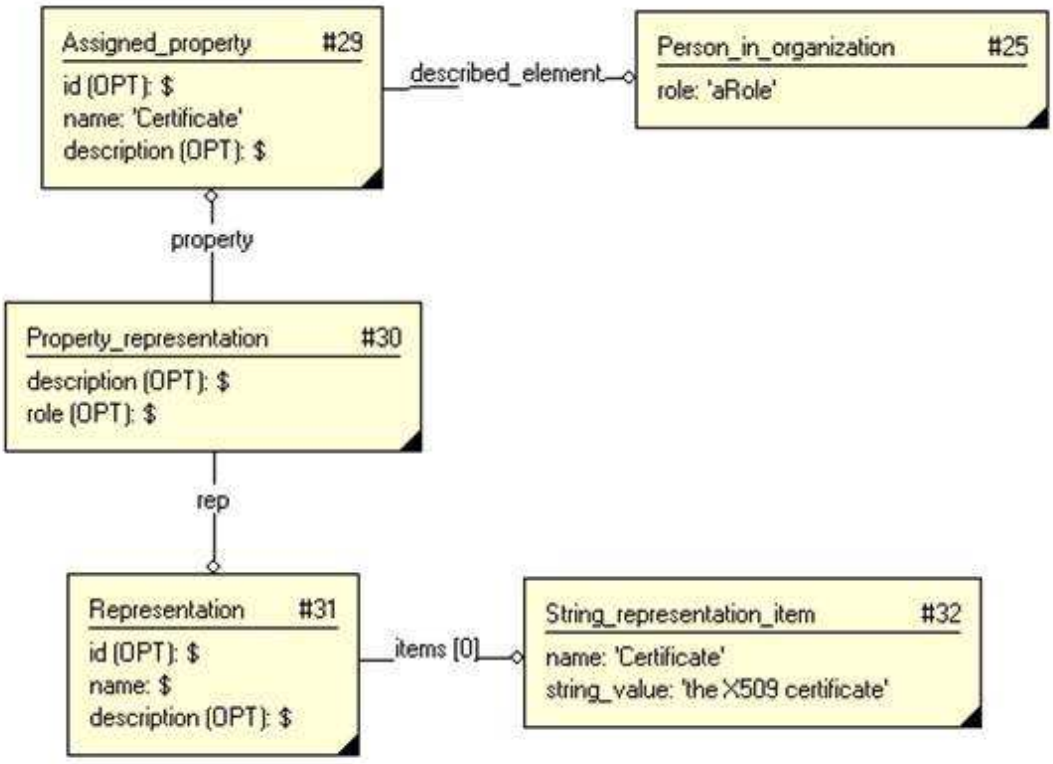

Figure 6: Certificate

Assigned_property	
Name	Mandatory field. If CMS / PKCS #7# is to be applied, the value must be “Certificate”. If W3C_DisiSig / SOAP-ENC is to be used, other relevant name is to be used.
Id	Optional field
Description	Optional field
Representation	
Id	Optional field
Name	Optional field

Description	Optional field
Property_representation	
Id	Optional field
acknowledge	Optional field
String_representation_item for certificate	
Name	Mandatory field. If CMS / PKCS#7# is the security standard to apply, the value must be “Certificate”. If W3C_DisiSig / SOAP-ENC is to be used, other relevant name is to be used.
String value	Mandatory field. If CMS / PKCS#7# is the security standard to apply, the value must be a X509 certificate as Base64 encoded value

Open question: any need to provide or agree on predefine values for names and descriptions of the representation and property_representation? Or eventually have we to provide a recommendation in order not to do so?

3.8 Files and related information

The content of the TPD is a set of files, which has to be securely transferred and transported a secured way from a sender in one organization to a set of receivers in one or several organizations.

In particular, it implies to be able to check that during this transfer, the files were neither corrupted nor accessed by an unauthorized tier or by the automated transfer means.

For these reasons, a set of information is required in order to describe the files in the TDP and to ensure their integrity.

It includes first their name and size.

According the adopted security policy, it should also include digesting information.

Within Aerospace and Defense Industry, currently CMS / PKCS #7# encrypted digest is required per file within PLM hubs context, and it may evolve to W3_DisiSig / SOAP-ENC.

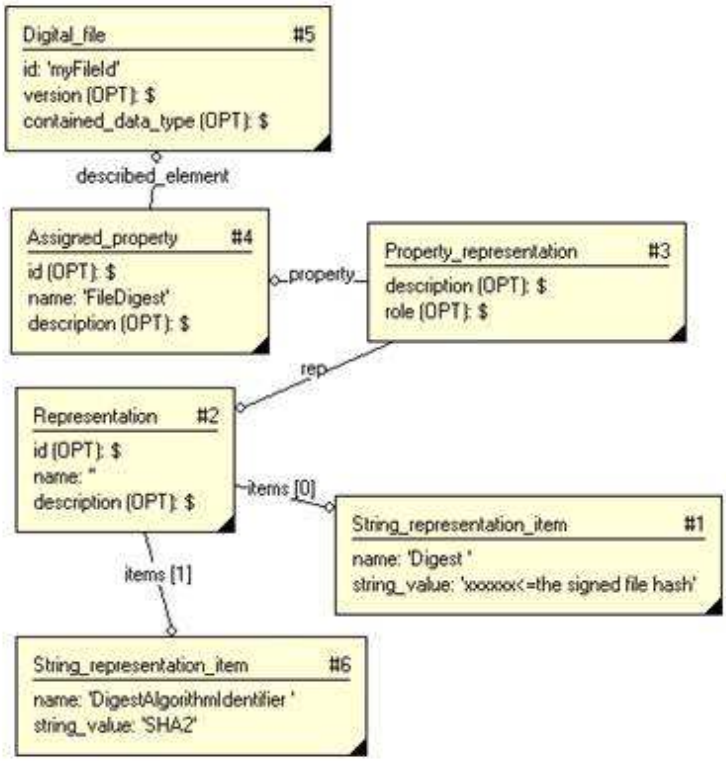

Figure 7: File description

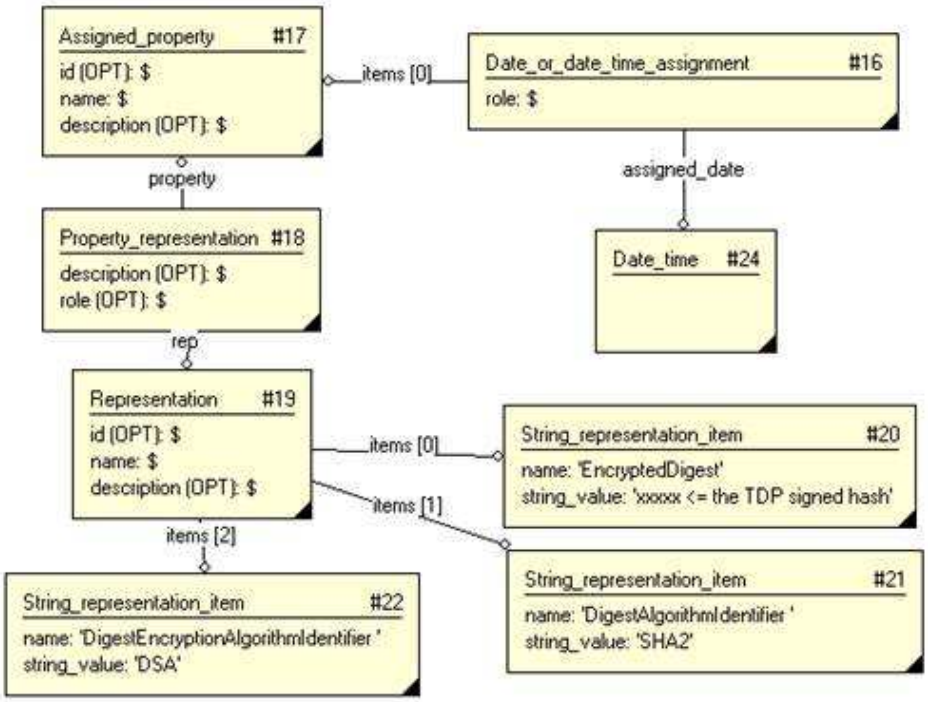

Figure 8: Encryption

When exchanging TDP and product structures, the Product metadata file is a particular file which is to be open first. The recommended practice is to indicate this file in the TDP message header by typing it as “masterfile” content item.

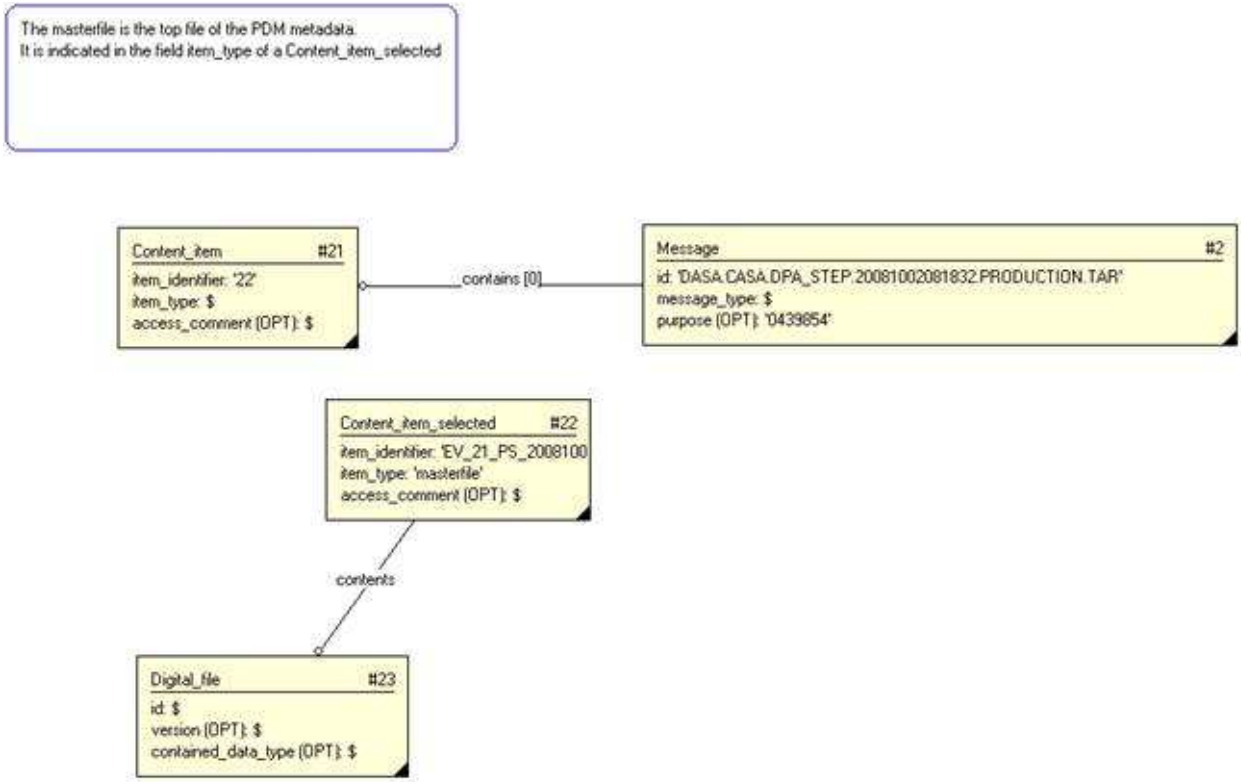

Figure 9: Masterfile

3.9 Security classification, export control and banned countries

For security classification and export control, the entities to choose in the schema are those related to security classification.

Export control is considered as a particular security classification.

Security classification to use will be specific to a given security context, and consequently the value of the classes (External_class.name) and the name of the classification (External_class.name) are not specified within this recommendation.

One classification to use identified, they should be formalized the way that is described in this section.

The assignment of the classification can be assigned to the message when willing to define the default values for all the files of the Technical Data Package. In this case, it could be indicated that the security classification is the default one (Security_classification.description=”DEFAULT”).

Each file (digital_file) can also be categorized by using security_classification_assignment, pointing on the file (digital_document) in place of the message.

It will then be provided a category that is different than the default one.

Note: it is not yet clarified if each file should be categorized systematically or if the default classification should be used and attached to the message. The last solution should be easier, reducing the amount of data.

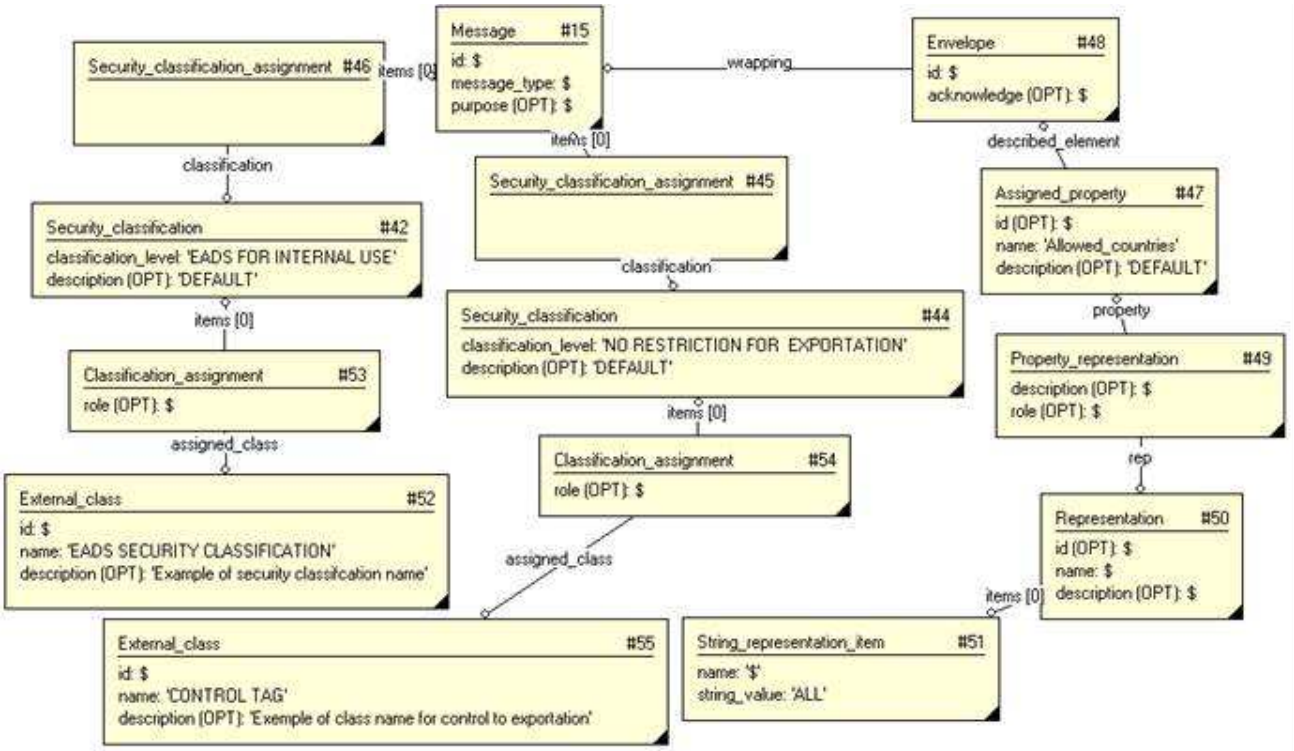

Figure 10: Security Classification

The mechanism allowing defining the allowed countries or restricted countries is the usage of a textual property assignment to envelop containing the message (default for the content of the TDP) or property assignment to each individual file for which specific rules exist. The values for allowed or denied countries (String_representation_item.string_value) will contain predefined set of values that are to be defined within the business context.

It should be “ALL” if all countries are concerned or “NONE if no country is concerned.

The string value should contain the code values of the countries concerned, separated by a comma. The codification to use is not defined in this specification, but for operational exchange, it should be defined by the partners exchanging Technical Data Packages.

In order to identify if what is considered is respectively allowed countries, or denied countries, the value of assigned_property.name will be respectively “Allowed_countries” and “Denied_countries”.

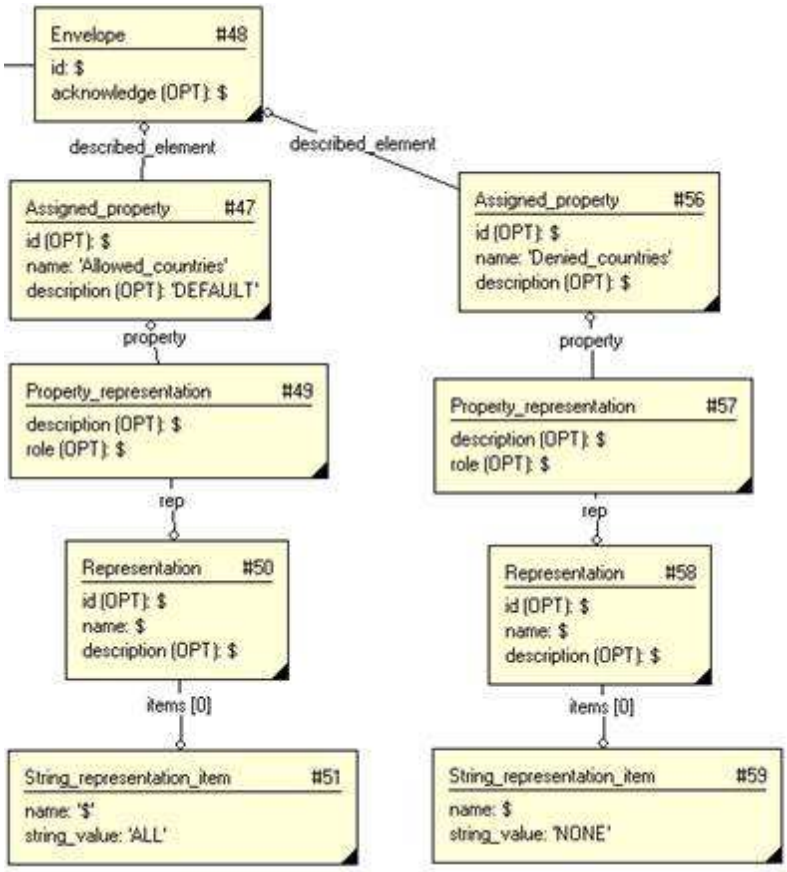

Figure 11: Allowed and denied Countries

When security is attached directly to file, it will be done as described in the following picture.

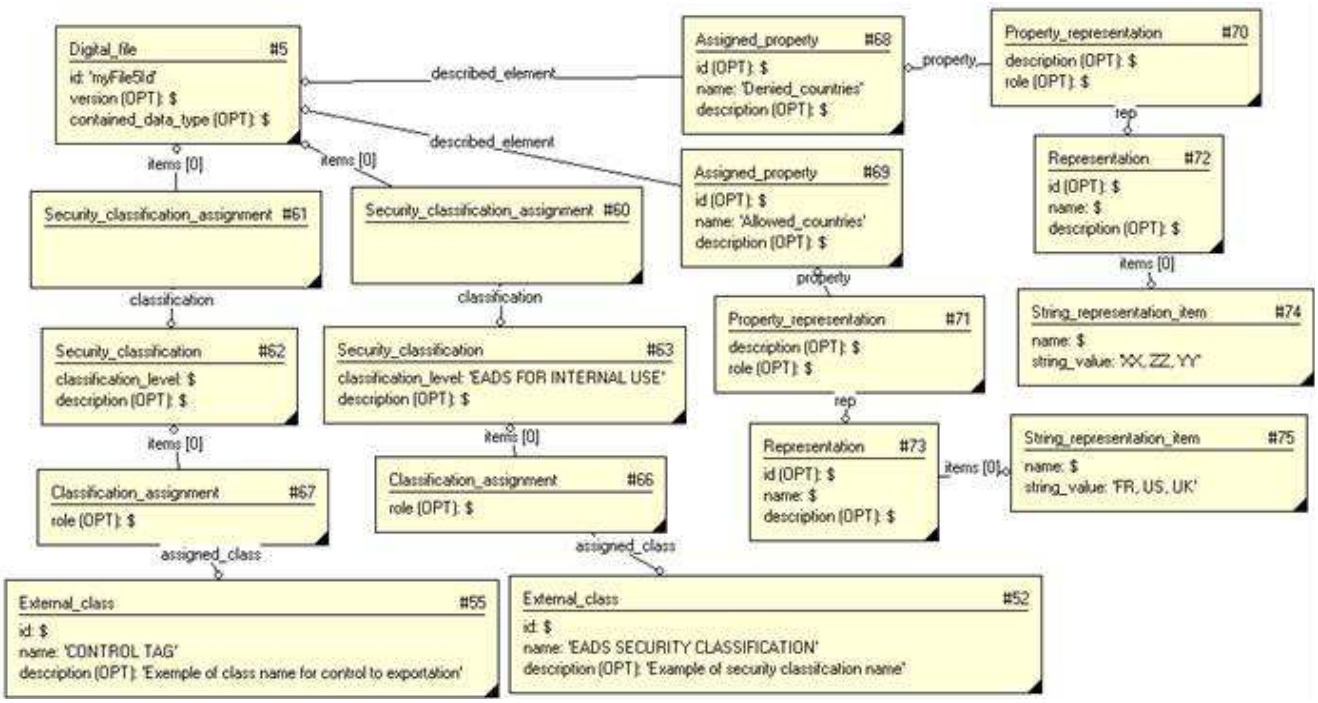

Figure 12: Security Classification

Note: the detailed tables of entities and attributes are to be written there, knowing that all attributes not used will be optional, and all those for which a value is provided are mandatory. The diagrams provide example of values that should be defined by business context codifications, except for "Denied_countries" and "Allowed_countries" and the value "ALL" and "NONE". It could be reconsidered if some relevant security standards already propose a standardized name. In this case, those values will be change to comply with it.

3.10 Context of the exchange

Within industrial context, when dealing with multiple programs, partners and applications, implementing secured TDP transfer and transportation could differ according the program or the partner to which a work package is attributed. Heterogeneity may can from different security constraints (e.g. for a military program in a given country) or operational transfer and PLM capabilities. For this reason, adding contextual information in the TDP header may be relevant, in particular for parameterization of the automated processes performed by a PLM Hub or for the services provided by a PLM Hub and associated collaborative platform.

It was identified during industrial pilots implementing TDP message header specifications that information such as Work package or Program is usually needed.

So the recommendations are to include such information a standardized way when required.

It is also recommended not to use the TDP message header in order to provide any contextual information related to Product data import or export, which is usually not to be done by a PLM Hub, but depend on sending and receiving applications.

Notes

When talking about collaboration context, it is related by the scope in which usage rules are defined. It could be an industrial program, a project, and the users of a given PLM Hub or a given Industry (e.g. Aerospace & Defense in Europe through the ASD SSG community). The target is to harmonize and align the usage rules in order to ensure interoperability and coherency between the different environments supporting TDP secured interchange.

This will concerned the set of predefined values for some of the attributes used for automation: those related to identification, related to authentication, related to notification, related to encryption, related to addresses and related to traceability (dates, status, etc).

It should also include context of the transfer related to definition of the concerned program, projects or work package, as soon such information is needed for routing of information. Once again, such information are not dedicated to CAD or PDM systems, as the place to provide information is the Product metadata file.

4 Annexes

1. EXPRESS Schema

   TDP_Message_Header_EXPRESS_V1.exp

2. XML Schema

   TDP_Message_Header_XML_V1.xsd

   Plus referenced schemas: cnf.xsd, doc.xsd and ex.xsd