Business Authorization Identification and Labeling Scheme Version 1 (BAILS v.1.0)

Prepared by: TSCP ILH Team

Lead Author: Jean-Paul Buu-Sao, TSCP

Released to: TSCP Architecture Committee

Edition: 1.4

Published: October 22, 2012

Copyright © 2012 Transglobal Secure Collaboration Participation, Inc.

All rights reserved.

Terms and Conditions

Transglobal Secure Collaboration Participation, Inc. (TSCP) is a consortium comprising a number of commercial and government members (as further specified at http://www.tscp.org) (each a "TSCP Member"). This specification was developed and is being released under this open source license by TSCP.

Use of this specification is subject to the disclaimers and limitations described below. By using this specification you (the user) agree to and accept the following terms and conditions:

1. This specification may not be modified in any way. In particular, no rights are granted to alter, transform, create derivative works from, or otherwise modify this specification. Redistribution and use of this specification, without modification, is permitted provided that the following conditions are met:

- Redistributions of this specification must retain the above copyright notice, this list of conditions, and all terms and conditions contained herein.
- Redistributions in conjunction with any product or service must reproduce the above copyright notice, this list of conditions, and all terms and conditions contained herein in the documentation and/or other materials provided with the distribution of the product or service.
- TSCP's name may not be used to endorse or promote products or services derived from this specification without specific prior written permission.

2. The use of technology described in or implemented in accordance with this specification may be subject to regulatory controls under the laws and regulations of various jurisdictions. The user bears sole responsibility for the compliance of its products and/or services with any such laws and regulations and for obtaining any and all required authorizations, permits, or licenses for its products and/or services as a result of such laws or regulations.

3. THIS SPECIFICATION IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TSCP AND EACH TSCP MEMBER DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY, QUIET ENJOYMENT, ACCURACY, AND FITNESS FOR A PARTICULAR PURPOSE. NEITHER TSCP NOR ANY TSCP MEMBER WARRANTS (A) THAT THIS SPECIFICATION IS COMPLETE OR WITHOUT ERRORS, (B) THE SUITABILITY FOR USE IN ANY JURISDICTION OF ANY PRODUCT OR SERVICE WHOSE DESIGN IS BASED IN WHOLE OR IN PART ON THIS SPECIFICATION, OR (C) THE SUITABILITY OF ANY PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF TSCP OR ANY THIRD PARTY.

4. IN NO EVENT SHALL TSCP OR ANY TSCP MEMBER BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY CLAIM ARISING FROM OR RELATING TO THE USE OF THIS SPECIFICATION, INCLUDING, WITHOUT LIMITATION, A CLAIM THAT SUCH USE INFRINGES A THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS OR THAT IT FAILS TO COMPLY WITH APPLICABLE LAWS OR REGULATIONS. BY USE OF THIS SPECIFICATION, THE USER WAIVES ANY SUCH CLAIM AGAINST TSCP OR ANY TSCP MEMBER RELATING TO THE USE OF THIS SPECIFICATION. IN NO EVENT SHALL TSCP OR ANY TSCP MEMBER BE LIABLE FOR ANY DIRECT OR INDIRECT DAMAGES OF ANY KIND, INCLUDING CONSEQUENTIAL, INCIDENTAL, SPECIAL, PUNITIVE, OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR RELATED TO ANY USER OF THIS SPECIFICATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

5. TSCP reserves the right to modify or amend this specification at any time, with or without notice to the user, and in its sole discretion. The user is solely responsible for determining whether this specification has been superseded by a later version or a different specification.

6. These terms and conditions will be interpreted and governed by the laws of the State of Delaware without regard to its conflict of laws and rules. Any party asserting any claims related to this specification irrevocably consents to the personal jurisdiction of the U.S. District Court for the District of Delaware and to any state court located in such district of the State of Delaware and waives any objections to the venue of such court.

Document Contributors:

Name	Organization
Howard Mason	BAE Systems
Richard Skedd	BAE Systems
Tim Bird	The Boeing Company
Andrew Cowan	Boldon James
Patrick Patterson	EADS
Emilio Montolivo	Finmeccanica
Scott Fitch	Lockheed Martin Corporation
Trevor Freeman	Microsoft
Don Schmidt	Microsoft
Mark Burns	Northrop Grumman Corporation
Stephanne Charbonneau	Titus
Jean-Paul Buu-Sao	TSCP

Table of Contents

1. Introduction

1.1 Document Purpose

The purpose of the document is to specify metadata elements for information objects suitable for:

1) Identifying the protection policies applicable to the information object.
2) Characterizing the impact level associated with the information object (e.g., the damage that would occur should its contents be compromised).
3) Enabling the applications to produce visual marking required for procedural enforcement of the protection policies.

The above metadata may be used to support the enforcement of the applicable protection policies of the proper access control rules in a secure collaboration scenario.

1.2 Document Structure

This document is made of the following sections:

- Context: set out the context of use of metadata elements
- Logical view: specifies the core metadata elements in a way that is independent of technical constraints and representations (hence the term “logical”)
- Profile: defines how community of interests can customize the logical view to fit their need, by the mean of profiles
- Extensions: defines how organizations can add their own metadata elements, by the mean of extensions
- Implementations: defines the additional documents needed for implementation
- Security considerations: defines security mechanisms that implementations need to consider

The document is followed by appendices, which define:

- The profile defined for the TSCP community of interest
- An implementation of the profile for Microsoft ® Office Custom Properties (OCP) metadata format, and an associated illustrative metadata example
- A representation of the metadata in XML, and an application to the OOXML document format

2. Context

Information is exchanged between users and organizations that collaborate to pursue a business goal. Where sensitive information is involved, it is assumed that the parties will have agreed what information is sensitive and how such information will be identified and handled. Any recipient of a resource will rely upon the provider of the information to follow the agreed procedures to identify the sensitivity of the information.

This standard provides a means for such sensitivity information to be expressed and may be used between parties if interoperable systems are to be implemented. It provides a set of standard “fields” that can be used to hold sensitivity information. It does not attempt to define what the contents of these “fields” should be.

This approach is an improvement upon the only alternative that exists at the moment, which is for the provider to use an arbitrary means to express sensitivity that may not be useful to a recipient. It should be recognized that, while this standard has been developed with the intent that it would be applicable in any domain of activity, the experience and background of the developers is in the aerospace and defense industry, where sensitivity marking results from national security, export control and intellectual property policies.

3. Logical view

This section presents a logical view of the policy specification on information objects.

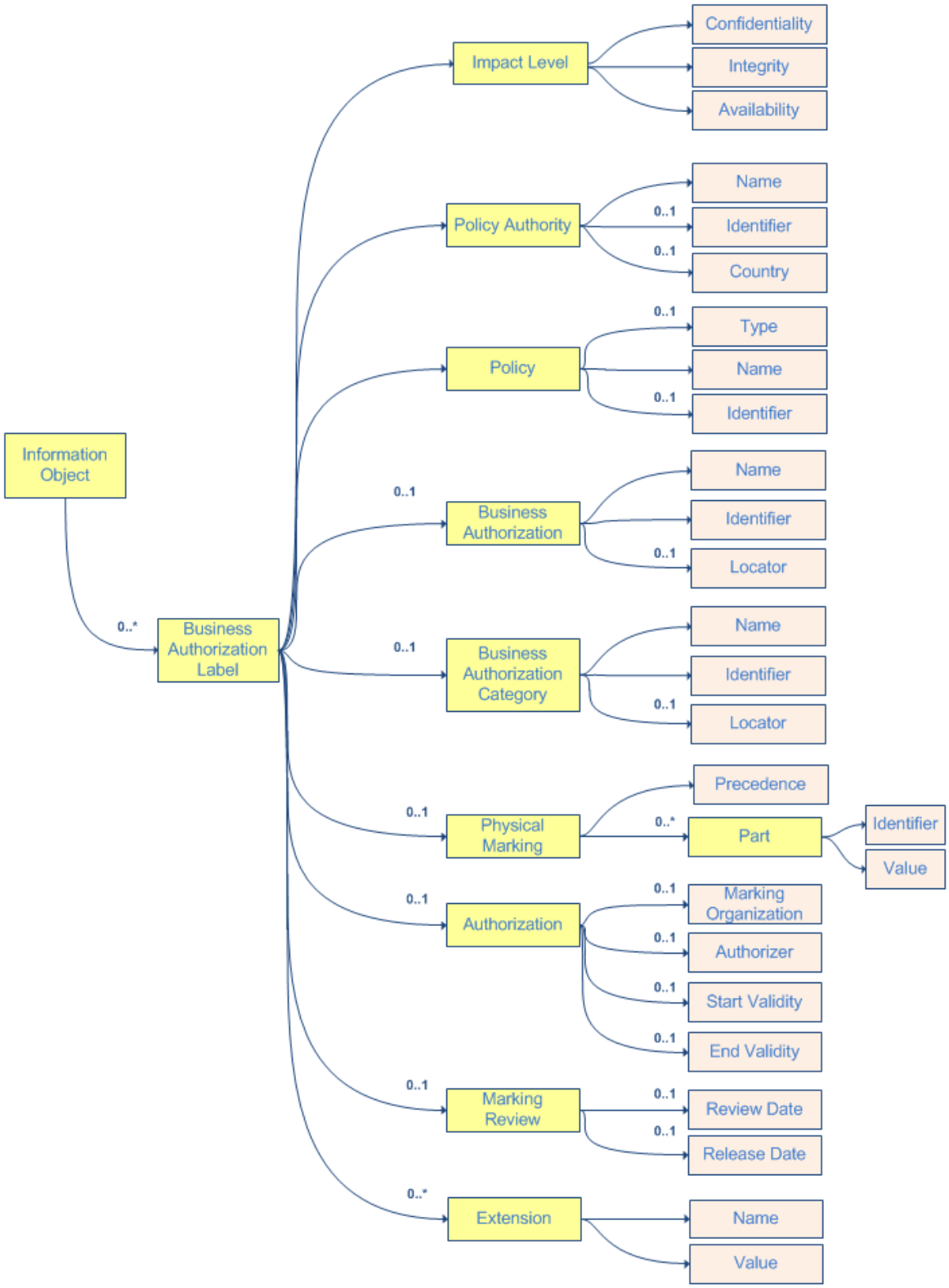

Table 1 below describes the purpose and contents of each component of the Business Authorization Labels metadata:

Table 1. Components of the Logical View

Component	Description
Information Object	An identifiable unit of digital information with a single owner, for example, a document, a database table, a database row, a digital image, a web page, a sequential file. An Information Object may represent an aggregation of other Information Objects.
Business Authorization Label	A set of metadata associated with an Information Object that identifies the following: • All the Business Authorizations that apply to the Information Object. And is composed of: • Visual indicators targeted to natural persons, so they can enforce the Business Authorization using human procedures • Systemic indicators targeted to applications and systems, so they can enforce the Business Authorization using automated systems
The rows below describe the components that constitute each Business Authorization Label	
Impact Level	The indication of the damage that would occur should the information object be compromised. The impact level is decomposed in terms of: • Confidentiality impact level; • Integrity impact level; • Availability impact level All three levels must be expressed within the same impact level scale
Policy Authority	The entity governing the protection policy under which the information object falls
Policy Authority - Name	The user-friendly name of the Policy Authority.
Policy Authority - Identifier	An identifier that uniquely designates the Policy Authority.
Policy Authority - Country	Indicates the country with which the policy authority is associated, expressed using an ISO 3166 country-name code whenever applicable.
Policy	This component identifies the protection policy under which the information object falls. This encompasses the governing policy authority and references to various policy artifacts.
Policy - Type	The type of policy. The possible values for the policy type are profile-specific.
Policy - Name	The user-friendly name that identifies the policy.

Component	Description
Policy - Identifier	An identifier that uniquely identifies the policy.
Business Authorization	A uniquely identifiable statement of requirements for the control of access to information established by a Policy Authority for a specific Policy.
Business Authorization - Name	The friendly-name that humans may use to identify the original, human-readable, business authorization artifacts. Applications may present this attribute to the user.
Business Authorization - Identifier	An identifier that uniquely designates the business authorization that systems can use to identify the original, system-readable, information protection rules.
Business Authorization - Locator	This attribute allows applications to locate the original policy artifacts. Applications may use this attribute to fetch human-readable policy artifact and present it to the user
Business Authorization Category	A uniquely identifiable construct that defines a subset of the requirements within a Business Authorization. The subset is distinguished by: • The set of rules that are used to determine if an Information Object is covered by the Business Authorization Category • The set of rules that are used to determine the privileges of a Principal regarding the Business Authorization Category
Business Authorization Category – Name	User-friendly name of the Business Authorization Category
Business Authorization Category - Identifier	An identifier that uniquely designates the business authorization category
Business Authorization Category – Locator	This attribute allows applications to locate the original artifacts about the business authorization category
Physical Markings	This component contains the label that must appear to human users, together with indications related to the application of these markings to the information object
Physical Markings – Precedence	A numerical value that determines the precedence of the visual marking of this Business Authorization Category over other Business Authorization Categories visual markings appearing on the same information object.
Physical Markings – Parts	The physical markings are broken up into multiple parts to allow applications to present individual parts at different locations and or with different presentation characteristics.
Physical Markings – Parts – Part – Identifier	The identifier of an individual part

Component	Description
Physical Markings – Parts – Part – Value	The string value of an individual part
Authorization	This component contains authorization data related to this Business Authorization Label
Authorization - Marking Organization	Identifier of the organization authorizing the physical marking.
Authorization - Authorizer	Identifier of the individual authorizing the physical marking.
Authorization - Start Validity Date	Start validity date of the marking, expressed using the extended ISO 8601 date format. Example: “2010-12-20”
Authorization - End Validity Date	End validity date of the marking, expressed using the extended ISO 8601 date format. Example: “2011-12-20”
Marking Review	This component contains review data related to this Business Authorization Label
Marking Review - Review Date	Date of confirmation of correct marking, expressed using the extended ISO 8601 date format Example: “2010-12-30”
Marking Review - Release Date	Date of release of the information object into a collaborative environment, expressed using the extended ISO 8601 date format Example: “2010-12-30”
Extension	An additional metadata attribute that organizations may add without having to declare it as part of the baseline profile. There may be multiple extensions per Business Authorization Label.
Extension - Name	Name of the added metadata attribute. Name collisions are avoided by qualifying the name with a namespace.
Extension - Value	Value of the added metadata attribute.

4. Profile

A profile of the Business Authorization Identification and Labeling Scheme is the specification of utilization, semantics and constraints imposed on the logical view presented above. Within a community of interest, organizations may define profiles that define, with respect to the logical view:

- The allowable number of Business Authorization Label elements.
- The allowable range of values of {Policy Authority Type}.
- The allowable range of names of {Policy Authority Name}.
- The semantics and naming conventions for Policy reference, locator and identifier.
- The semantics and naming conventions for Policy Category reference, locator and identifier.
- The allowable number of Object marking Parts.
- The manner in which current sensitivity markings will be expressed using the metadata structure.
- The extent to which optional metadata items will be used and the manner in which content will be expressed.

Organizations should also establish the guidance recommended in section 6 below. An example of an initial tailoring of this standard to produce a TSCP profile is provided in Appendix A.

Organizations should manage the definition and use of profiles to achieve their goal for interoperability with partners.

5. Extensions

Organizations are free to extend the Logical View stated in section 3 with additional components and data elements. Such extensions form a superset of the original logical view and must ensure backward compatibility with applications that are not aware of the extensions.

The typical business requirement involves two organizations, A and B, that need to include additional metadata to which they have bilaterally agreed. This requirement for dynamic extensions (i.e., extensions that do not need to be declared in advance to any central authority) is met by allowing organizations to make use of the multi-valued “Extension” attributes. Each “Extension” is characterized by an extension identifier and a value. To avoid potential naming collisions, the specification recommends using extension qualifiers defined by URIs qualified by namespaces.

Application developers must:

1. Be aware of the possibility of extensions.
2. Ensure that the application functions based on the intended profile.
3. Respect the extensions (e.g., when updating or transforming documents) so that they are preserved for the anticipating applications.

6. Implementation

To implement this metadata standard in information systems, organizations may also wish to provide the following documentation:

- Policy Implementation Guidance: Define a standard process by which data will be extracted from the policy and populated into metadata fields
- Label Encoding Guidance – Define a standard process by which data will be extracted from the policy and will be stored within the file type or system and its presentation and formatting for users

7. Security considerations

This specification provides information to enable sensitive content to be processed appropriately by information systems and their users. It will be important, particularly where the content has a high level of sensitivity, for implementers of this specification to implement mechanisms that ensure the validity and integrity of the Business Authorization Labels as well as the integrity of the binding between these Labels and the Information Object. These mechanisms are independent of the structure and content of the Labels described above.

Considerations that implementers should note include:

- Ensuring that the user is authorized to make a determination of the appropriate Labels.
- Supporting the user to apply Labels that are appropriate to the content of the resource.
- Ensuring that a complete set of Labels are applied and that their content is valid.
- Recording the identity and authority of the user with an appropriate level of assurance.
- Enabling controlled access to change Labels by authorized users.
- Ensuring the integrity of the Labels following their application by an authorized user.
- Establishing and maintaining a binding between the Information Object and the Labels.
- Understanding the need for binding between the Information Object and its content.
- Managing changes to content and the resultant impact on the Labels and their binding to the Information Object.
- Providing indications to users where the binding between the Labels and the Information Object has been compromised.

8. Appendix A: BAILS Profile for TSCP

The following provides an example of tailoring within the context of TSCP specifications.

Typographic convention: in the table below, text in gray represents the language that appears in the baseline specification. Text in black represents additions to the baseline specification, specific to the BAILS profile for TSCP.

Component	Description
Information Object	An identifiable unit of digital information with a single owner, for example, a document, a database table, a database row, a digital image, a web page, a sequential file. An Information Object may represent an aggregation of other Information Objects.
Business Authorization Label	A set of metadata associated with an Information Object that identifies the following: • All the Business Authorizations that apply to the Information Object. And is composed of: • Visual indicators targeted to natural persons, so they can enforce the Business Authorization using human procedures • Systemic indicators targeted to applications and systems, so they can enforce the Business Authorization using automated systems There must not be more than one Business Authorization Label of a given Policy Type, per Information Object.
The rows below describe the components that constitute each Business Authorization Label	
Impact Level	The indication of the damage that would occur should the information object be compromised. The impact level is decomposed in terms of: •Confidentiality impact level; •Integrity impact level; •Availability impact level All three levels must be expressed within the same impact level scale. This version of the specification recognizes two possible types of Impact Level: FIPS-199 and UK-Cabinet. Subsequent versions of the specification may add more types
Impact Level – Value	The indication of the damage that would occur should the information object be compromised. The value domains corresponding to each one of the types of Impact Level in the TSCP profile are defined

Component	Description
	as: • {Low, Moderate, High} for type of Impact Level = FIPS-199[1] • {0, 1, 2, 3}[2] for type of Impact Level = UK-Cabinet
Policy Authority	The entity governing the protection policy under which the information object falls.
Policy Authority - Name	The user-friendly name of the Policy Authority.
Policy Authority - Identifier	An identifier that uniquely designates the policy authority.
Policy Authority - Country	Indicates the country with which the policy authority is associated, expressed using an ISO 3166 country-name code whenever applicable. The country must not be specified for "Intellectual Property" policy type
Policy	This component identifies the protection policy under which the information object falls. This encompasses the governing policy authority and references to various the policy artifacts.
Policy - Type	The type of policy. The possible values for the policy type are profile specific The following policy types are defined: • Export Control • National Security • Intellectual Property
Policy - Name	The user-friendly name that identifies the policy.
Policy - Identifier	An identifier that uniquely identifies the policy.
Business Authorization	A uniquely identifiable statement of requirements for the control of access to information established by a Policy Authority for a specific Policy.
Business Authorization - Name	This optional attribute contains a reference that humans can use to identify the original human-readable business authorization artifacts. Applications may present this attribute to the user.
Business Authorization - Identifier	An identifier that uniquely designates the business authorization that systems can use to identify the original system-readable information protection rules.

[1] Per http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf, Section 3.

[2] The UK Cabinet defines scales 0 to 6. Only levels 0 to 3 are defined here, as the levels 4 to 6 are currently out of TSCP scope.

Component	Description
	This attribute contains a Unified Resource Name (URN)[3] that can be used to locate the original system-readable policy artifact.
Business Authorization - Locator	This attribute allows applications to locate the original policy artifacts. Applications may use this attribute to fetch human-readable policy artifact and present it to the user.
Business Authorization Category	This component identifies a set of information subject to a Business Authorization that shares the same characteristics and therefore marking/label.
Business Authorization Category – Name	User-friendly name of the Business Authorization Category.
Business Authorization Category - Identifier	An identifier that uniquely designates the business authorization category.
Business Authorization Category – OID	An identifier that uniquely designates the business authorization category, expressed as an OID[4]
Business Authorization Category – Locator	This attribute allows applications to locate the original artifacts about the business authorization category.
Physical Markings	This component contains the label that must appear to human users, together with indications related to the application of these markings to the information object.
Physical Markings – Precedence	A numerical value that determines the precedence of the visual marking of this Business Authorization Category over other Business Authorization Categories visual markings appearing on the same information object. The precedence is an integer value ranging from 1 to 10, inclusive, the value of 10 specifying the highest precedence.
Physical Markings – Parts	The physical markings are broken up into multiple parts to allow for applications to present individual parts at different locations and/ or with different presentation characteristics.
Physical Markings – Parts – Part – Identifier	The identifier of an individual part. This attribute contains a Unified Resource Name (URN)[5] that can be used to further characterize the part.

[3] URNs are a subset of URIs. Refer to http://www.w3.org/TR/uri-clarification/ for a clarification on URI, URL and URL

[4] OID: object identifier or OID is an identifier used to name an object. Structurally, an OID consists of a node in a hierarchically-assigned namespace, formally defined using the ITU-T's ASN.1 standard

[5] URNs are a subset of URIs. Refer to http://www.w3.org/TR/uri-clarification/ for a clarification on URI, URL and URL

Component	Description
	Applications can make use of this information to query for known identified part in order to render them appropriately. The current profile recognizes the following identifiers: **ui-name** The associated value represents a very brief (fewer than 20 characters) summary of the policy to use in UI, e.g., for users to select the policy from a drop down list. **ui-disclaimer** The associated value is a brief text typically located in a single place within the document, e.g., in a security control information table. **general-summary** The associated value is brief text typically located in a single place within the document, e.g., in a security control information table **general-warning-statement** The associated value contains a text typically located at the beginning of a document (e.g., on the cover page) that warns the end-user about the protection policy that must apply, and possibly the consequences if he or she does not comply. **general-distribution-statement** The associated value contains text typically located at the beginning of a document (e.g., on the cover page), that provides information on the distribution requirements of the document. **document-header** The associated value contains a brief text located at the top of each document's pages. **document-footer** The associated value contains a brief text located at the bottom of each document's pages. **email-first-line-of-text** The associated value contains a text located at the beginning of the email body. **email-last-line-of-text** The associated value contains a text located at the end of the email body. **email-subject-prefix** The associated value contains a brief text located at the

Component	Description
	beginning of the email subject. **email-subject-suffix** The associated value contains a brief text located at the end of the email subject .
Physical Markings – Parts – Part – Value	The string value of an individual part. The string length can vary from 0 to 1024 Unicode characters.
Authorization	This component contains authorization information related to this Business Authorization Label.
Authorization - Marking Organization	Identifier of the organization authorizing the physical marking.
Authorization - Authorizer	Identifier of the individual authorizing the physical marking.
Authorization - Start Validity Date	Start validity date of the marking, expressed using the extended ISO 8601 date format. Example: “2010-12-20”
Authorization - End Validity Date	End validity date of the marking, expressed using the extended ISO 8601 date format. Example: “2011-12-20”
Marking Review	This component contains review information related to this Business Authorization Label.
Marking Review - Review Date	Date of confirmation of correct marking, expressed using the extended ISO 8601 date format. Example: “2010-12-30”
Marking Review - Release Date	Date of release of the information object into a collaborative environment, expressed using the extended ISO 8601 date format. Example: “2010-12-30”
Extension	An additional metadata attribute that organizations may add without having to declare them as part of the baseline profile. There may be multiple extensions per Business Authorization Label. Although TSCP does not define any extension, organizations using this profile may define their own.
Extension - Name	Name of the added metadata attribute. Name collisions are avoided by qualifying the name with a namespace.
Extension - Value	Value of the added metadata attribute

9. Appendix B: Custom Properties implementation of BAILS Profile for TSCP

Some document formats implement metadata structured as a non-ordered list of attribute-value pairs. Provided below is a non-normative example of how Business Authorization Labels metadata can be expressed using non-ordered attribute-value pairs.

In the notation below:

- {type} designates the type of a policy. In BAILS 1.0, the recognized string values are: ExportControl, NationalSecurity and IntellectualProperty

The following metadata items may be used:

Mandatory metadata item	Description
urn:bails:{type}:PolicyAuthority:Name	Name of the policy authority
urn:bails:{type}:Policy:Name	Name of the policy
urn:bails:{type}:Impact:Scale	Scale of the impact level
urn:bails:{type}:Impact:Level:Confidentiality	Value of the confidentiality impact level
urn:bails:{type}:Impact:Level:Integrity	Value of the integrity impact level
urn:bails:{type}:Impact:Level:Availability	Value of the availability impact level

This allows the identification of the Policy Authority that governs the policy that is applicable to the resource, a cross-policy authority identification of overall sensitivity and a detailed representation of the set of security markings at present.

The BAILS metadata, for which an implementation based upon Office Custom Property (OCP) is provided here, are meant to be included in documents as Office field codes. In the case a given field code does not exist in the OCP, Office currently returns a string error, which is locale-dependent. Additionally, there is no support for detecting whether, in a locale-independent manner, a field code exists in the OCP. As a consequence of these constraints, default (known) values must always be specified for BAILS metadata. The known default value is always the empty string "" when the associated attribute is a visual marking; otherwise, it is the string "None."

The following additional metadata items may be used:

Optional metadata item	Description	Default value
urn:bails:{type}:PolicyAuthority:Identifier	Identifier of the policy authority	"None"
urn:bails:{type}:PolicyAuthority:Country	Country of the policy authority	"None"
urn:bails:{type}:Policy:Identifier	Identifier of the policy	"None"
urn:bails:{type}:BusinessAuthorization:Name	Name of the business authorization	"None"
urn:bails:{type}:BusinessAuthorization:Identifier	Identifier of the business authorization	"None"
urn:bails:{type}:BusinessAuthorization:Locator	Locator of the human readable artifact of the business authorization	"None"

Optional metadata item	Description	Default value
urn:bails:{type}:BusinessAuthorizationCategory:Name	Name of the business authorization category	“None”
urn:bails:{type}:BusinessAuthorizationCategory:Identifier	Identifier of the business authorization category	“None”
urn:bails:{type}:BusinessAuthorizationCategory:Identifier:OID	Identifier of the business authorization category, expressed as an OID	“None”
urn:bails:{type}:BusinessAuthorizationCategory:Locator	Locator of the human readable artifact of the business authorization category	“None”
urn:bails:{type}:Marking:Precedence	Integral value specifying the visual marking precedence	“None”
urn:bails:{type}:Marking:{identifier} identifier = ui_name identifier = ui_disclaimer identifier = general_summary identifier = general_warning_statement identifier = general_distribution_statement identifier = document_header	Physical marking part, with {identifier} designating the type of the marking. BAILS 1.1 recognizes the following identifiers: A very brief (less than 20 characters) summary of the policy to use in UI, e.g., for users to select the policy from a drop down list Text shown to the user (by an application e.g., SharePoint) before she can access information, and where the user (the potential recipient of the data) needs to acknowledge that she has read the disclaimer Brief text typically located in a single place within the document, e.g., in a security control information table Text typically located at the beginning of a document (e.g., on the cover page), that warns the end-user about the protection policy that must apply, and possibly the consequences if she does not comply with Text typically located at the beginning of a document (e.g., on the cover page), that provides information on the distribution requirements of the document Brief text located at the top of each document's pages	“”

Optional metadata item	Description	Default value
identifier = document_footer identifier = document_watermark identifier = email_first_line_of_text	Brief text located at the bottom of each document's pages Brief text formatted as a watermark on each document's page Text located at the beginning of the email body	
identifier = email_last_line_of_text identifier = email_subject_prefix identifier = email_subject_suffix	Text located at the end of the email body Brief text located at the beginning of the email subject Brief text located at the end of the email subject	
urn:bails:{type}:Authorization:MarkingOrganization	Name of the organization authorizing the physical marking	“None”
urn:bails:{type}:Authorization:Authorizer	Identifier of the individual authorizing the physical marking	“None”
urn:bails:{type}:Authorization:StartValidity	Start validity date of the physical marking	“None”
urn:bails:{type}:Authorization:EndValidity	End validity date of the physical marking	“None”
urn:bails:{type}:MarkingReview:ReviewDate	Date of confirmation of correct marking	“None”
urn:bails:{type}:MarkingReview:ReleaseDate	Date of release of the information object into a collaborative environment	“None”
urn:bails:{type}:Extension:{index}:Name	Name of added metadata attribute	“None”
urn:bails:{type}:Extension:{index}:Value	Value of added metadata attribute	“None”

Long attributes

Any attribute may be longer than the 255 character limit that Office allows for Custom Properties. In these cases, attributes are broken into as many parts of 255-character length as necessary to contain the entire long attribute. Attributes that are part of long, broken-up attributes have their names terminated by the string “:ext:n”, where n is the order of the chunk. The example below shows an Export Control warning statement that is split into four chunks:

urn:bails:ExportControl:Marking:general-warning-statement = Characters 1-255
urn:bails:ExportControl:Marking:general-warning-statement:ext:2 = Characters 256-511
urn:bails:ExportControl:Marking:general-warning-statement:ext:3 = Characters 512-767
urn:bails:ExportControl:Marking:general-warning-statement:ext:4 = Characters 768-1023

Locators

Business Authorization Locator and Business Authorization Category Locator are provided to allow identification of the appropriate area of a particular policy that applies. Business Authorization Identifier and Business Authorization Category Identifier provide the same information but in a manner that is system-processable.

Marking Authority and related fields are provided to identify who applied the current markings, when these markings should be reviewed.

10. Appendix C: Examples of implementation of the BAILS Profile for TSCP

Custom Properties implementation:

Attribute	Value
urn:bails:ExportControl:PolicyAuthority:Name	BIS
urn:bails:ExportControl:PolicyAuthority:Identifier	urn:us:doc:bis
urn:bails:ExportControl:PolicyAuthority:Country	US
urn:bails:ExportControl:Policy:Name	EAR
urn:bails:ExportControl:Policy:Identifier	urn:us:doc:bis:ear
urn:bails:ExportControl:Impact:Scale	FIPS-199
urn:bails:ExportControl:Impact:Level:Confidentiality	Moderate
urn:bails:ExportControl:Impact:Level:Integrity	Moderate
urn:bails:ExportControl:Impact:Level:Availability	Moderate
urn:bails:ExportControl:BusinessAuthorization:Name	EAR-EL.D456480
urn:bails:ExportControl:BusinessAuthorization:Identifier	urn:us:doc:bis:ear:el:d456480
urn:bails:ExportControl:BusinessAuthorization:Locator	None
urn:bails:ExportControl:BusinessAuthorizationCategory:Locator	None
urn:bails:ExportControl:Authorization:StartValidity	2011-03-11
urn:bails:ExportControl:Authorization:StopValidity	2013-03-31
urn:bails:ExportControl:BusinessAuthorizationCategory:Name	EAR-EL.D456480.1
urn:bails:ExportControl:BusinessAuthorizationCategory:Identifier	urn:us:doc:bis:ear:el:d456480.1
urn:bails:ExportControl:BusinessAuthorizationCategory:Identifier:OID	1.3.6.1.4.1.20000.100.1
urn:bails:ExportControl:MarkingPrecedence	1
urn:bails:ExportControl:Marking:general-summary	
urn:bails:ExportControl:Marking:general-warning-statement	Warning: Export controlled 2401 et.seq. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25. Dissemination to non-U.S. persons whether in the United States or abroad.
urn:bails:ExportControl:Marking:general-warning-statement:ext:2	
urn:bails:ExportControl:Marking:general-warning-statement:ext:3	
urn:bails:ExportControl:Marking:general-warning-statement:ext:4	
urn:bails:ExportControl:Marking:general-distribution-statement	This commodity, technology, or software was exported from the US in accordance with the Export Administration Regulations. Diversion contrary to US law is prohibited.
urn:bails:ExportControl:Marking:general-distribution-statement:ext:2	
urn:bails:ExportControl:Marking:general-distribution-statement:ext:3	
urn:bails:ExportControl:Marking:general-distribution-statement:ext:4	
urn:bails:ExportControl:Marking:document-footer	Export controlled – see sheet 1
urn:bails:ExportControl:Marking:document-header	
urn:bails:ExportControl:Marking:document-watermark	
urn:bails:ExportControl:Marking:email-first-line-of-text	EAR Export Controlled
urn:bails:ExportControl:Marking:email-last-line-of-text	

Attribute	Value
urn:bails:ExportControl:Marking:email-subject-prefix	EAR
urn:bails:ExportControl:Marking:email-subject-suffix	

11. Appendix D: XML implementation of BAILS Profile for TSCP

For purposes of example, a generic XML Schema that can be used to express the Business Authorization Labels proposed. This XML Schema uses constructs that express syntactic constraints of the logical view, in accordance with the example of tailored Meta-Data standard for TSCP presented in Appendix A.

TSCP will maintain the schema to use the most suitable formats for each considered class of resource, keeping in mind the goals of interoperability and the utilization of established standards.

```
<xs:schema xmlns="http://www.tscp.org/schemas/bails-v1" xmlns:bails="http://www.tscp.org/schemas/bails-v1"
xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:sstl="http://www.iso.org/schema/stl"
targetNamespace="http://www.tscp.org/schemas/bails-v1" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:import namespace="http://www.iso.org/schema/stl" schemaLocation="ISO3166CountryCode.xsd" />
    <xs:import namespace="http://www.iso.org/schema/stl" schemaLocation="ISO639LanguageCode.xsd" />
    <xs:element name="BusinessAuthorizationLabels">
        <xs:annotation />
        <xs:complexType>
            <xs:sequence minOccurs="0" maxOccurs="3">
                <xs:element ref="BusinessAuthorizationLabel" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="BusinessAuthorizationLabel">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="ImpactLevel" />
                <xs:element ref="PolicyAuthority" />
                <xs:element ref="Policy" />
                <xs:element ref="BusinessAuthorization" minOccurs="0" />
                <xs:element ref="BusinessAuthorizationCategory" minOccurs="0" />
                <xs:element ref="PhysicalMarkings" minOccurs="0" />
                <xs:element ref="Authorization" minOccurs="0" />
                <xs:element ref="MarkingReview" minOccurs="0" />
                <xs:element ref="Extensions" minOccurs="0" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="PolicyAuthority" type="PolicyAuthority" nillable="true" />
    <xs:complexType name="PolicyAuthority" abstract="true">
        <xs:sequence>
            <xs:element name="Name" type="xs:string" />
        </xs:sequence>
        <xs:attribute name="Identifier" type="xs:anyURI" use="required" />
    </xs:complexType>
    <xs:element name="CommercialPolicyAuthority" type="CommercialPolicyAuthority" nillable="true" />
    <xs:complexType name="CommercialPolicyAuthority" mixed="false">
        <xs:complexContent mixed="false">
            <xs:extension base="PolicyAuthority" />
        </xs:complexContent>
    </xs:complexType>
    <xs:element name="NationalPolicyAuthority" type="NationalPolicyAuthority" nillable="true" />
    <xs:complexType name="NationalPolicyAuthority" mixed="false">
        <xs:complexContent mixed="false">
            <xs:extension base="PolicyAuthority">
                <xs:sequence>
                    <xs:element name="Country" type="sstl:ISO3166CountryCode" />
                </xs:sequence>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
    <xs:element name="ExportPolicyAuthority" type="ExportPolicyAuthority" nillable="true" />
    <xs:complexType name="ExportPolicyAuthority" mixed="false">
        <xs:complexContent mixed="false">
            <xs:extension base="PolicyAuthority">
```

```
            <xs:sequence>
                <xs:element name="Country" type="sstl:ISO3166CountryCode" />
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:element name="Policy">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Type" type="xs:string" minOccurs="0" />
            <xs:element name="Name" type="xs:string" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="Identifier" type="xs:anyURI" use="required" />
    </xs:complexType>
</xs:element>
<xs:element name="BusinessAuthorization">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Name" type="xs:anyURI" minOccurs="0" />
            <xs:element name="Locator" type="xs:anyURI" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="Identifier" type="xs:anyURI" use="required" />
    </xs:complexType>
</xs:element>
<xs:element name="BusinessAuthorizationCategory">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Reference" type="xs:anyURI" minOccurs="0" />
            <xs:element name="Locator" type="xs:anyURI" minOccurs="0" />
        </xs:sequence>
        <xs:attribute name="Identifier" type="xs:anyURI" use="required" />
        <xs:attribute name="OID" type="xs:string" use="required" />
    </xs:complexType>
</xs:element>
<xs:element name="ImpactLevel" type="ImpactLevel" />
<xs:complexType name="ImpactLevel" abstract="true" />
<xs:element name="Undefined_ImpactLevel" type="Undefined_ImpactLevel" />
<xs:complexType name="Undefined_ImpactLevel" mixed="false">
    <xs:complexContent mixed="false">
        <xs:extension base="ImpactLevel" />
    </xs:complexContent>
</xs:complexType>
<xs:element name="FIPS_199_ImpactLevel" type="FIPS_199_ImpactLevel" />
<xs:complexType name="FIPS_199_ImpactLevel" mixed="false">
    <xs:complexContent mixed="false">
        <xs:extension base="ImpactLevel">
            <xs:sequence>
                <xs:element name="Value">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="Low" />
                            <xs:enumeration value="Moderate" />
                            <xs:enumeration value="High" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:element name="UK_Cabinet_ImpactLevel" type="UK_Cabinet_ImpactLevel" />
<xs:complexType name="UK_Cabinet_ImpactLevel" mixed="false">
    <xs:complexContent mixed="false">
        <xs:extension base="ImpactLevel">
            <xs:sequence>
                <xs:element name="Value">
```

```
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="0" />
                            <xs:enumeration value="1" />
                            <xs:enumeration value="2" />
                            <xs:enumeration value="3" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
            </xs:sequence>
        </xs:extension>
    </xs:complexContent>
</xs:complexType>
<xs:element name="Parts">
    <xs:complexType>
        <xs:sequence minOccurs="0" maxOccurs="4">
            <xs:element ref="Part" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="Organization">
    <xs:simpleType>
        <xs:restriction base="xs:string" />
    </xs:simpleType>
</xs:element>
<xs:element name="Name">
    <xs:simpleType>
        <xs:restriction base="xs:string" />
    </xs:simpleType>
</xs:element>
<xs:element name="Level" nillable="true">
    <xs:simpleType>
        <xs:restriction base="xs:byte">
            <xs:enumeration value="2" />
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="PhysicalMarkings">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="Parts" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="Authorization">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="MarkingOrganization" type="xs:string" minOccurs="0" />
            <xs:element name="Authorizer" type="xs:string" minOccurs="0" />
            <xs:element ref="Validity" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="Validity">
    <xs:complexType>
        <xs:sequence>
            <xs:element ref="StartDate" />
            <xs:element ref="EndDate" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="StartDate">
    <xs:simpleType>
        <xs:restriction base="xs:date" />
    </xs:simpleType>
</xs:element>
```

```
    <xs:element name="EndDate">
        <xs:simpleType>
            <xs:restriction base="xs:date" />
        </xs:simpleType>
    </xs:element>
    <xs:element name="Part">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Value" type="xs:string" />
                <xs:element ref="LocalizedParts" minOccurs="0" />
            </xs:sequence>
            <xs:attribute name="Identifier" type="xs:anyURI" use="required" />
        </xs:complexType>
    </xs:element>
    <xs:element name="LocalizedParts">
        <xs:complexType>
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
                <xs:element ref="LocalizedPart" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="LocalizedPart">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Language" type="sstl:ISO639LanguageCode" />
                <xs:element name="Value" type="xs:string" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="MarkingReview">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="ReviewDate" type="xs:date" minOccurs="0" />
                <xs:element name="ReleaseDate" type="xs:date" minOccurs="0" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Extension">
        <xs:complexType>
            <xs:simpleContent>
                <xs:extension base="xs:string">
                    <xs:attribute name="name" type="xs:anyURI" use="required" />
                </xs:extension>
            </xs:simpleContent>
        </xs:complexType>
    </xs:element>
    <xs:element name="Extensions">
        <xs:complexType>
            <xs:sequence minOccurs="0" maxOccurs="unbounded">
                <xs:element ref="Extension" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
</xs:schema>
```

12. Appendix E: Implementation example of the metadata standard using OOXML Custom XML Parts

The OOXML document format supports the integration of arbitrary business data within Microsoft® Office documents, via the mean of "Office™ Custom XML Parts"[6]. OOXML documents can contain any number of custom XML parts. Each custom XML Part has an Identifier (in the form of a GUID) and a schema namespace. The OOXML API allows enumerating the custom XML parts attached to a document, or locating any specific custom XML part by GUI or by schema namespace.

The implementation of the metadata standard using OOXML custom XML parts is straightforward and follows the following principles:

1. BAILS metadata, stored as custom XML part, is assigned a specific GUID (value to be defined). This GUID is unique in order to allow BAILS metadata to coexist with other business data in custom xml parts. An example of a GUID is: "263471E7-B7C8-11D2-BC44-006008BF0962"
2. BAILS metadata, stored as custom XML part, follows the XML Schema for BAILS, as proposed in the Appendix B of this document. It follows that its schema namespace is the schema namespace of the BAILS XML Schema, whose current proposed value is: "http://www.tscp.org/schemas/bails-v1." This value is subject to change before this specification is formally submitted.

Applications can create, update and delete BAILS metadata using the appropriate API (typically: OOXML API). It should be noted that:

1. The native functionality of document signing within Word 2007 and later versions does not sign custom XML parts. The integrity of the binding between the BAILS labels and the documents these labels refer to needs to be ensured by an external mechanism, which is out of scope for this document.
2. The BAILS metadata implemented as custom XML parts are associated with the document as a whole. This implementation proposal does not cope with document portion labeling.
3. Multiple versions of BAILS labels can coexist: all versions will share the same GUID, but will present different schema namespaces. In case of co-existence, it will be up to the applications to manage the appropriate compatibility between the labels of various versions.

[6] Office XML Custom Parts are defined in: http://msdn.microsoft.com/en-us/library/bb608618.aspx