ACS Marking Definition Version 3.0 - STIX™ Version 2.1. Part 1: STIX Core Concepts

Working Draft 02

30 September 2019

​Integrated Cyber Defense Working Group (ICDWG)

​Editors:

ICDWG - Access Control Specification Sub-Working Group

Additional artifacts:

This prose specification is one component of a Work Product that also includes:

* Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0
* Intelligence Community Authorized Classification and Control Markings, Register and Manual (Version 5.1)

Related work:

This specification replaces or supersedes:

* *N/A*

Abstract:

Initially developed to support information sharing by the Enhance Shared Situational Awareness (ESSA) initiative across the Federal Cyber Centers, the Information Sharing Architecture (ISA) Access Control Specification (ACS) document specifies a common set of elements for tagging information and related common attributes that indicate characteristics of a person or system that allow automated decisions to be made regarding information sharing. This document defines an approach to express ACS using Structured Threat Information Expression (STIXTM) language via the use of a marking definition.

## 7.2​ Data Markings

Data markings represent restrictions, permissions, and other guidance for how data can be used and shared. For example, data may be shared with the restriction that it must not be re-shared, or that it must be encrypted at rest. In STIX, data markings are specified using the marking-definition object. These definitions are applied to complete STIX Objects using object markings and to individual properties of STIX Objects via granular markings.

Multiple markings can be added to the same object, including both object and granular markings. Some types of marking definitions or trust groups have rules about which markings override other markings or which markings can be additive to other markings. This specification does not define rules for how multiple markings applied to the same object or property should be interpreted.

Granular data markings are also used to mark individual fields on an object with which language their text content is in. For example, granular markings can be used to indicate that while the rest of the object is in English, the **description** field is in Japanese. This mechanism does not use the marking-definition object to represent language, rather a separate **lang** field that can also be applied via granular markings.

### ​7.2.1​ Marking Definition

**Type Name:** marking-definition

The marking-definition object represents a specific marking. Data markings typically represent handling or sharing requirements for data and are applied in the **object\_marking\_refs** and **granular\_markings** properties on STIX Objects, which reference a list of IDs for marking-definition objects.

Two marking definition types are defined in this specification: TLP, to capture TLP markings, and Statement, to capture text marking statements. In addition, it is expected that the FIRST Information Exchange Policy (IEP) will be included in a future version once a machine-usable specification for it has been defined.

Unlike other STIX Objects, Marking Definition objects cannot be versioned because it would allow for indirect changes to the markings on a STIX Object. For example, if a Statement marking is changed from "Reuse Allowed" to "Reuse Prohibited", all STIX Objects marked with that Statement marking would effectively have an updated marking without being updated themselves. Instead, a new Statement marking with the new text should be created and the marked objects updated to point to the new marking.

The JSON MTI serialization uses the JSON Object type [[RFC8259](#pleh5znnqume)] when representing marking-definition.

#### ​7.2.1.1​ Properties

|  |  |  |
| --- | --- | --- |
| **Required Common Properties** | | |
| **type**, **spec\_version**, **id**, **created** | | |
| **Optional Common Properties** | | |
| **created\_by\_ref**, **external\_references**, **object\_marking\_refs**, **granular\_markings** | | |
| **Not Applicable Common Properties** | | |
| **modified**, **revoked**, **labels**, **confidence**, **lang**, **defanged**, **extensions** | | |
| **Marking Definition Specific Properties** | | |
| **name**, **definition\_type**, **definition** | | |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The **type** property identifies the type of object. The value of this property **MUST** be marking-definition. |
| **name** (optional) | string | A name used to identify the Marking Definition. |
| **definition\_type** (required) | open-vocab | The **definition\_type** property identifies the type of Marking Definition. The value of the **definition\_type** property **SHOULD** be one of the types defined in the subsections below: statement or tlp (see sections [7.2.1.3](#_3ru8r05saera) and [7.2.1.4](#_yd3ar14ekwrs)) |
| **definition** (required) | <marking object> | The **definition** property contains the marking object itself (e.g., the TLP marking as defined in section [7.2.1.4](#_yd3ar14ekwrs), the Statement marking as defined in section [7.2.1.3](#_3ru8r05saera), or some other marking definition defined elsewhere). |

#### ​7.2.1.2​ Relationships

There are no relationships explicitly defined between the Marking Definition object and other STIX Objects, other than the embedded relationships listed below. These embedded relationships are listed by property name along with their corresponding target.

|  |  |
| --- | --- |
| **Embedded Relationships** | |
| **created\_by\_ref** | identity |
| **object\_marking\_refs** | marking-definition |

​

#### ​7.2.1.3​ Statement Marking Object Type

The Statement marking type defines the representation of a textual marking statement (e.g., copyright, terms of use, etc.) in a definition. The value of the **definition\_type** property **MUST** be statement when using this marking type. Statement markings are generally not machine-readable, and this specification does not define any behavior or actions based on their values.

Content may be marked with multiple statements of use. In other words, the same content can be marked both with a statement saying "Copyright 2019" and a statement saying, "Terms of use are ..." and both statements apply.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **statement** (required) | string | A Statement (e.g., copyright, terms of use) applied to the content marked by this marking definition. |

**Examples**

{

"type": "marking-definition",

"spec\_version": "2.1",

"id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",

"created": "2016-08-01T00:00:00.000Z",

"definition\_type": "statement",

"definition": {

"statement": "Copyright 2019, Example Corp"

}

}

#### ​7.2.1.4​ TLP Marking Object Type

The TLP marking type defines how you would represent a Traffic Light Protocol (TLP) marking in a definition property. The value of the **definition\_type** property **MUST** be tlp when using this marking type.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **tlp** (required) | string | The TLP level [[TLP](#2rvyub9rtmpf)] of the content marked by this marking definition, as defined in this section. |

The following standard marking definitions **MUST** be used to reference or represent TLP markings. Other instances of tlp-marking **MUST NOT** be used or created (the only instances of TLP marking definitions permitted are those defined here).

|  |  |
| --- | --- |
| white | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--613f2e26-407d-48c7-9eca-b8e91df99dc9",  "created": "2017-01-20T00:00:00.000Z",  "definition\_type": "tlp",  "name": "TLP:WHITE",  "definition": {  "tlp": "white"  }  } |
| green | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da",  "created": "2017-01-20T00:00:00.000Z",  "definition\_type": "tlp",  "name": "TLP:GREEN",  "definition": {  "tlp": "green"  }  } |
| amber | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--f88d31f6-486f-44da-b317-01333bde0b82",  "created": "2017-01-20T00:00:00.000Z",  "definition\_type": "tlp",  "name": "TLP:AMBER",  "definition": {  "tlp": "amber"  }  } |
| red | {  "type": "marking-definition",  "spec\_version": "2.1",  "id": "marking-definition--5e57c739-391a-4eb3-b6be-7d15ca92d5ed",  "created": "2017-01-20T00:00:00.000Z",  "definition\_type": "tlp",  "name": "TLP:RED",  "definition": {  "tlp": "red"  }  } |

### ​7.2.1.5 Access Control Specification (ACS) Marking Object Type

The Access Control Specification (ACS) marking type defines the object types required to implement automated access control systems based on the relevant policies governing sharing between participants. The value of the **definition\_type** property **MUST** be **x-isa-acs-3-0**

when using this marking type.

Information sharing across a Federal Cybersecurity Information Sharing Community requires a capability to protect and allow access to information in accordance with applicable information sharing agreements, policies, and laws. This marking definition is the result of collaboration among this community.

Please refer to "Information Sharing Architecture (ISA) Access Control Specification (ACS) Version 3.0" [ref] for more information on creating ACS data marking definitions.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **sep\_version** (required) | integer | This required property indicated the specification version of the serialization being used.  The value of this property **MUST** be 1 for ACS data marking objects defined according to this specification. |
| **identifier** (required) | string | This required property holds a single unique identifier associated with the resource. This value can be used for tracking data provenance, executing data retraction, and enforcing auditing requirements. The Resource Identifier will use a format that includes a prefix and an RFC4122 suffix. The prefix used will include the ISA common prefix (GUIDE prefix). The ISA has been assigned a GUIDE7 (Globally Unique Identifier for Everything) prefix of 19001 for production and 999191 for test use. It is recommended that RFC 4122 Version 4 UUIDs be used for the suffix; however, other versions are permitted. |
| **name (optional)** | string | This property provides a "handle" to identify and describe this marking definition.  Note that the **name** property in no way defines the data marking. It is simply provided as a convenience for users. |
| **create\_date\_time** (required) | timestamp | This required property provides the creation date and time of the associated resource as identified by the Identifier. This value supports a number of functions including enforcing data retention policies and auditing requirements. |
| **responsible\_entity\_custodian** (required) | open-vocab | This property represents the data producer that is responsible for providing the associated resource to be shared. It is represented as an organization value. This value is necessary for auditing and enforcing data retention and provenance policies.  Allowable values, listed in Appendix A: List of Organizations of **[ref], MUST** be used.  The set of allowable values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **responsible\_entity\_originator**  (optional) | open-vocab | This optional property represents the originating organization for the associated resource. If not present, then the origin of the information is unspecified. It is represented as an organization value. An appropriate value from the organizations in Appendix A: List of Organizations of **[ref] SHOULD** be used. However, additional values may be created to specify the originator.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification.  Certain Originators may require anonymity to protect their identity. This is common when dealing with a cybersecurity threat or incident where the originator is an entity in the Private Sector. Cover terms (e.g., USENERGY01) assigned to an entity should be carried through anytime the resource is shared. |
| **authority\_reference**  (optional) | string | This property captures the legal authority under which the content was created, not the limitation on sharing the content. This property is used for auditing and records management, not for access control decisions. In some cases, the Authority Reference is needed by ESSA Participants to be included in the Control Policy Group as well as the Resource Accounting Group.  It **MUST** be of the of the format *urn(:\w+)+.* |
| **policy\_reference** (required) | string | This property provides the means of indicating a particular policy related to the sharing of the resource.  Multiple URNs can be included, separated by a space, but one of the following **MUST** be included:   * urn:isa:policy:acs:ns:v3.0?privdefault=permit&amp;sharedefault=permit * urn:isa:policy:acs:ns:v3.0?privdefault=permit&amp;sharedefault=deny * urn:isa:policy:acs:ns:v3.0?privdefault=deny&amp;sharedefault=permit * urn:isa:policy:acs:ns:v3.0?privdefault=deny&amp;sharedefault=deny   Each value **MUST** be of the format *urn(:\w+)+.* |
| **original\_classification**  (optional) | x-isa-acs-original-classification-type | This property provides details for generating a classification authority block for presentation of a classified resource to an operator.  Either the Original Classification or the Derivative Classification **MUST** be provided for classified resources, as appropriate.  Details regarding the basic encoding specification detail for Original Classification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community **[ref]**. |
| **derivative\_classification**  (optional) | x-isa-acs-derivative-classification-type | This property provides details for generating a classification authority block for presentation of a classified resource to an operator.  Either the Original Classification or the Derivative Classification **MUST** be provided for classified resources, as appropriate.  Details regarding the basic encoding specification detail for Original Classification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community **[ref]**. |
| **declassification**  (optional) | x-isa-acs-declassification-type | This property provides the declassification instructions associated with an original or derived classification for generating a classification authority block for presentation of a classified resource to an operator.  Details regarding the basic encoding specification detail for Declassification are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community **[ref]**. |
| **resource\_disposition** (optional) | x-isa-acs-resource\_disposition-type | This property can be used to provide a fixed date and time at which an action is to be taken on the associated resource, such as destruction. Retention can be enforced through the use of this property or through the use of policies.  This property allows for specifying ad hoc (i.e., not policy based) retention limitation requests from information creators such as private industry.  Details regarding the basic encoding specification detail for Resource Disposition are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community [ref]. |
| **public\_release**  (optional) | x-isa-acs-public-release-type | This property is used to provide the release authority and date for resources that have been through a formal public release determination process or note that the resource has not been publicly released.  Details regarding the basic encoding specification detail for Public Release are included in the Smart Data – Enterprise Data Header (EDH) Implementation Profile for the Cyber Community **[ref]**. |
| **access\_privilege** (optional) | list of type x-isa-acs-access-privilege-type | This property provides a means of limiting or permitting specific actions once access control decisions have been made. |
| **further\_sharing** (optional) | list of type x-isa-acs-access-privilege-type | This property provides a means of limiting or permitting further sharing once original access control decisions have been made. |
| **control\_set**  (required) | x-isa-acs-control-set-type | The **control\_set** property is the group of data tags that are used to inform automated access control decisions. |

#### 7.2.1.5.1 ACS Original Classification Object Type

**Type Name:** x-isa-acs-original-classification-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **classified\_by** (required) | string | This property contains the name of person with the original classification authority who made a classification determination. |
| **classified\_on** (optional) | timestamp | This property contains the date an original classification determination was made. |
| **classification\_reason** (optional) | string | This property contains the rationale for an original classification determination. |
| **compilation\_reason**  (optional) | string | This property contains the rationale for assigning a higher classification level than a simple roll-up of its portions would indicate. |

#### 7.2.1.5.2 ACS Derivative Classification Object Type

**Type Name:** x-isa-acs-derivative-classification-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **classified\_by** (required) | string | This property contains the name of person with the original[[1]](#footnote-1) classification authority who made a classification determination. |
| **classified\_on** (optional) | timestamp | This property contains the date an original classification determination was made. |
| **derived\_from** (required) | string | This property contains the citation of the original classification guidance used for a derivative classification. |

#### 7.2.1.5.3 ACS Declassification Object Type

**Type Name:** x-isa-acs-declassification-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **declass\_exemption** (optional) | string | This property contains the basis for a resource not being subject to standard automatic declassification processes. |
| **declass\_period** (optional) | integer | This property contains the duration of time in years for calculating from a create date or classification date when a resource will be automatically declassified if not exempt. |
| **declass\_date** (optional) | timestamp | This property contains the date upon which a resource will be automatically declassified if not exempt. |
| **declass\_event** (optional) | string | This property contains the future occurrence upon which a resource will be automatically declassified if not exempt. |

#### 7.2.1.5.4 ACS Resource Disposition Object Type

**Type Name:** x-isa-acs-resource-disposition-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **disposition\_date** (required) | timestamp | This property contains the date upon which the declared disposition process is to be initiated. |
| **disposition\_process** (required) | string | This property contains the  allowed disposition process to be performed (e.g., destruction). |

#### 7.2.1.5.5 ACS Public Release Object Type

**Type Name:** x-isa-acs-public-release-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **released\_by** (optional) | string | This property contains the authority that authorized the public release. |
| **released\_on** (optional) | timestamp | This property contains the date of public release. |

#### 7.2.1.5.6 ACS Access Privilege Object Type

**Type Name:** x-isa-acs-access-privilege-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **privilege\_action**  (required) | open-vocab | This property indicates the action that may be taken when the access privilege is allowed.  This is an open vocabulary and values **SHOULD** come from x-isa-privilege-action-ov vocabulary. |
| **privilege\_scope** (required) | x-isa-acs-privilege-scope-type | This property indicates the scope of the access privilege. |
| **rule\_effect** (required) | x-isa-acs-rule-effect-enum | This property indicates if actions are permitted or denied.  The values of this property **MUST** come from the x-isa-acs-rule-effect -enum enumeration. |

#### 7.2.1.5.6 ACS Privilege Scope Object Type

**Type Name:** x-isa-acs-privilege-scope-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **permitted\_nationalities**  (optional) | list of type string | The **permitted\_nationalities**  (CTRY) property identifies the limitation on the distribution of the resource based on nationality.  Allowable values are listed in Geopolitical Entities, Names, and Codes (GENC) Standard Edition 1[[2]](#footnote-2) **MUST** be used. |
| **permitted\_organizations** (optional) | list of type open-vocab | The **permitted\_organizations** (ORG) property identifies the limitation on the distribution of the resource based on organization.  Allowable values listed in Appendix A: List of Organizations of **[ref] MUST** be used.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **shareabiity** (optional) | list of type x-isa-acs-shar-enum | The **shareability** (SHAR) property is used to identify the shareability of a resource that may be released based on the determination of an originator in accordance with established disclosure procedures.  The values of this property **MUST** come from the x-isa-acs-shar-enum enumeration. |
| **entity** (optional) | list of type x-isa-acs-entity-enum | The **entity** (ENTITY) property is used to identify the entities to which information may be released based on the determination of an originator.  The values of this property **MUST** come from the x-isa-acs-entity-enum enumeration. |

#### 7.2.1.5.7 ACS Further Sharing Object Type

**Type Name:** x-isa-acs-further-sharing-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **sharing\_scope** (required) | list of type open- vocab | This property indicates the scope of the further sharing. The organizations in Appendix A: List of Organizations of **[ref] SHOULD** be used. The values, FOREIGNGOV or SECTOR **MAY** also be used.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **rule\_effect** (required) | x-isa-rule-effect-enum | This property indicates if further sharing is permitted or denied. |

#### 7.2.1.5.8 ACS Control Set Object Type

**Type Name:** x-isa-acs-control-set-type

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **classification**  (required) | x-isa-acs-classification-enum | This property contains information specifying the classification level.  The Classification value contains the classification of the data based on the Executive Order 13526, Classified National Security Information [ref] and the Information Security Manual (ISM) [ref] marking system. Unclassified information will include a classification marking.  The value of this property **MUST** come from the x-isa-acs-classification-enum enumeration. |
| **sci\_controls** (optional) | list of type open-vocab | The appropriate values for the sensitive compartmented information (SCI) property are listed in MDM SCI Control List [ref].  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **logical\_authority\_category** (optional) | list of type open-vocab | The **logical\_authority\_category** (LAC) property represent classes of authority upon which data can be generated or acquired and that can be used to apply mandatory special access control and handling policies.  The allowable values are listed in the NSA’s Master Data Registry [ref].  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |
| **formal\_determination** (optional) | list of type x-isa-acs-fd-enum | The **formal\_determination** (FD) property is used to Indicate other formal determinations beyond classification that have been applied to a resource.  The values of this property **MUST** come from the x-isa-acs-fd-enum enumeration. |
| **caveat** (optional) | list of type x-isa-acs-cvt-enum | The **caveat** (CVT) property is used to indicate a specific control.  The values of this property **MUST** come from the x-isa-acs-cvt-enum enumeration. |
| **sensitivity** (optional) | list of type x-isa-acs-sens-enum | The **sensitivity** (SENS) property is used to specify an inherent sensitivity about the data that requires specific restrictions in access or handling.  The values of this property **MUST** come from the x-isa-acs-sens-enum enumeration. |
| **shareability** (optional) | list of type x-isa-acs-shar-enum | The **shareability** (SHAR) property is used to identify the shareability of a resource that may be released based on the determination of an originator in accordance with established disclosure procedures.  The values of this property **MUST** come from the x-isa-acs-shar-enum enumeration. |
| **entity** (optional) | list of type x-isa-acs-entity-enum | The **entity** (ENTITY) property is used to identify the entities to which information may be released based on the determination of an originator.  The values of this property **MUST** come from the x-isa-acs-entity-enum enumeration. |
| **permitted\_nationalities**  (optional) | list of type string | The **permitted\_nationalities**  (CTRY) property identifies the limitation on the distribution of the resource based on nationality.  Allowable values are listed in Geopolitical Entities, Names, and Codes (GENC) Standard Edition 1[[3]](#footnote-3) **MUST** be used. |
| **permitted\_organizations** (optional) | list of type open-vocab | The **permitted\_organizations** (ORG) property identifies the limitation on the distribution of the resource based on organization.  Allowable values listed in Appendix A: List of Organizations of **[ref] MUST** be used.  The set of possible values can be thought of as an open vocabulary, but it is not explicitly defined in this specification. |

#### 7.2.1.5.9 ACS Privilege Action Open Vocabulary

**Type Name**: x-isa-privilege-action-ov

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| DSPLY | The action of displaying, either in a hard copy document or a visual presentation of the resource. DSPLY should be used to permit display when there is generally a global deny for all actions. |
| IDSRC | The action of identifying the source of the resource further than the entity receiving the resource. When set to deny, attributes or elements in the resource that identify the source and custodian must be removed or replaced prior to additional actions being taken. This restriction applies not only to the elements in the header of the resource but may also apply to elements within the body of the document being shared. The use of IDSRC does not authorize any changes to markings on the resource. For example, the removal of the source information will not change the classification of the resource. |
| TENOT | The action of notifying a targeted entity of a cybersecurity incident based on the resource. |
| NETDEF | The action of taking network defense actions including detection and mitigation, remediation, and local analysis and signature development, based on the resource. |
| LEGAL | The action of using the resource in legal proceedings. |
| INTEL | The action of conducting additional intelligence analysis based on the resource. |
| TEARLINE | The action of removing and taking further action on components of a resource based on their component markings. To be tear-lineable indicates that marked components of a document may be removed and treated as individually marked components. When set to deny, even though there may be components with fewer restrictions than the overall document, they may not be removed. |
| OPACTION | The action of conducting cyber-based operations applied to adversary capabilities based on the resource. |
| REQUEST | The action of requesting a waiver to an access privilege restriction. When set to deny, the originator will not consider specific requests to take actions based on the resource. |
| ANONYMOUSACCESS | The action of allowing anonymous access to the resource. This action is included to support the restrictions placed on the indicators shared with the US government from the DHS Automated Indicator Sharing (AIS) program. |
| CISAUSES | The cybersecurity purposes allowed in the Cybersecurity Information Sharing Act of 2015 [ref] |

#### 7.2.1.5.10 ACS Rule Effect Enumeration

**Type Name**: x-isa-acs-rule-effect-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| permit | The specified action, privilege, etc is permitted |
| deny | The specified action, privilege, etc is denied |

#### 7.2.1.5.11 ACS Classification Enumeration

**Type Name**: x-isa-acs-classification-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| U | Unclassified |
| C | Confidential |
| S | Secret |
| TS | Top Secret |

#### 7.2.1.5.12 ACS Formal Determination Enumeration

**Type Name**: x-isa-acs-fd-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| AIS | The resource is appropriate for AIS (Automated Indicator Sharing) |
| FOUO | The resource is appropriate For Official Use Only. |
| NF | Indicates that the resource is releasable to U.S. citizens and not releasable to foreign nationals without the permission of the originator. |
| PII-NECESSARY-TO-UNDERSTAND-THREAT | Personally identifiable information (PII) necessary to understand the context of the resource is present. |
| PII-NOT-PRESENT | Personally identifiable Information (PII) is *not* present. |
| PUBREL | Approved for Public Release |

#### 7.2.1.5.13 ACS Caveat Enumeration

**Type Name**: x-isa-acs-cvt-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| FISA | The FISA caveat marking denotes the presence of Foreign Intelligence Surveillance Act (FISA) (Reference 18) or FISA-derived information in the document. This is an informational marking only to highlight such information. Recipients of resources with the FISA control marking are responsible for ensuring that the resource is protected in conformance with the legal requirements of the FISA for limitations on use and warning displays. |
| POSSIBLEPII | The POSSIBLEPII caveat marking indicates to the recipient that the resource may contain Personally Identifiable Information (PII). Recipients are responsible for ensuring that the resource is protected according to their agencies policies related to PII. |
| CISAPROPRIETARY | The CISAPROPRIETARY caveat marking indicates that the resource must observe appropriate restrictions as requested by the originator in accordance with the Cybersecurity Information Sharing Act of 2015 [ref] |

#### 7.2.1.5.14 ACS Sensitivity Enumeration

**Type Name**: x-isa-acs-sens-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| NTOC\_DHS\_ECYBER\_SVC\_SHARE.NSA.NSA | Enhanced Cybersecurity Services |
| PCII | Protected Critical Infrastructure Information |
| LES | Law Enforcement Sensitive Information |
| INT | Intelligence Information |
| PII | Personally Identifiable Information |
| PR | Cybersecurity Targeted Entity Information |
| TEI | Commercial Proprietary Information |

#### 7.2.1.5.15 ACS Shareability Enumeration

**Type Name**: x-isa-acs-shar-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| NCC | National Cyber Centers |
| EM | Emergency Management |
| LE | Law Enforcement |
| IC | Intelligence Community |

#### 7.2.1.5.16 ACS Entity Enumeration

**Type Name**: x-isa-acs-entity-enum

|  |  |
| --- | --- |
| **Vocabulary Value** | **Description** |
| MII | Military service member |
| GOV | U.S. federal government civilian employee |
| CTR | Contractor |
| SVR | Server |
| SVC | Service, Widget, Application, Software, etc |
| DEV | End-point device |
| NET | Network device |

#### 7.2.1.5.17 Examples

Notice these examples of the ACS marking definitions appear as part of a marking-definition STIX object type.

{ "type": "marking-definition",  
 "id": "marking-definition--f4d1771b-d6a6-4eb1-9768-9686efeeb89a",  
 "created": "2018-10-01T00:00:00Z",  
 "definition\_type": "x-isa-acs-3-0",   
 "definition": {  
 "sep\_version": "1",

"identifier": "isa:guide.19001.ACS3-bc9034f8-c732-5328-b9df-d9d72aae480b",

"name": "banner\_marking",  
 "create\_date\_time": "2016-06-27T14:10:26.723Z",  
 "responsible\_entity\_custodian": "USA.NSA",  
 "responsible\_entity\_originator": "USA.NSA",  
 "authority\_reference": "urn:isa:authority:CFR2013\_32\_2\_236",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=deny&amp;sharedefault=deny",  
 "original\_classification": {  
 "classified\_by": "Available-On-Request",  
 "classified\_on": "2017-01-10T00:00:00Z",  
 "classification\_reason ": "Example",  
 "compilation\_reason": "Orig-Doc"  
 },  
 "derivative\_classification": {  
 "classified\_by": "Available-On-Request",  
 "classified\_on": "2018-02-20T00:00:00Z",  
 "derived\_from": "Orig-Doc"  
 },  
 "declassification": {  
 "declass\_period": "32",  
 "declass\_date": "2020-02-20T00:00:00Z",  
 "declass\_event": "Per Exec Order blah-blah-blah"  
 },

"access\_privilege": [

{

"privilege\_action": "CISAUSES",

"rule\_effect": "permit"

},

{

"privilege\_action": "ANONYMOUSACCESS",

"rule\_effect": "deny"

}

],  
 "public\_release": {  
 "releasable\_to\_public ": "false"  
 },  
 "control\_set": {  
 "classification": "TS",

"sci\_controls": ["SI"],

"logical\_authority\_category": ["LAC12345"],

"formal\_determination": ["AIS"],

"sensitivity": ["NTOC\_DHS\_ECYBER\_SVC\_SHARE.NSA.NSA"],

"permitted\_nationalities": ["USA", "AUS", "CAN", "GBR", "NZL"],  
 "permitted\_organizations": ["USA.NSA", "USA.DHS"]N  
 }  
 }  
}

{  
 "type": "marking-definition",  
 "id": "marking-definition--11b6042f-7b98-4b97-a168-bec4c025dda9",  
 "created": "2018-10-01T00:00:00Z",  
 "definition\_type": "x-isa-acs-3-0”,   
 "definition": {  
 "sep\_version": "1",

"identifier": "isa:guide.19001.ACS3-bc9034f8-c732-5328-b9df-d9d72aae4ccc",

"name": "some\_unclassified\_marking",   
 "create\_date\_time": "2016-06-27T14:10:26.723Z",  
 "responsible\_entity\_custodian": "USA.NSA",  
 "responsible\_entity\_originator": "USA.NSA",   
 "authority\_reference": "urn:isa:authority:CFR2013\_32\_2\_236",

"policy\_reference": "urn:isa:policy:acs:ns:v3.0?privdefault=denyt&amp;sharedefault=deny",

"access\_privilege": [

{

"privilege\_action": "CISAUSES",

"rule\_effect": "permit"

},

{

"privilege\_action": "ANONYMOUSACCESS",

"rule\_effect": "permit"

}

],  
 "control\_set": {  
 "classification": "U",

"formal\_determination": ["FOUO", "AIS"],  
 "permitted\_organizations": ["USA.NSA", "USA.DHS"]  
 },  
 }  
}​

### 7.2.2 Object Markings

Object Markings apply data markings to an entire STIX Object and all of its contents. Object Markings are specified as embedded relationships in the **object\_marking\_refs** property, which is an optional list of IDs for Marking Definition objects. The referenced markings apply to that STIX Object or Marking Definition and all of its contents. Changes to the **object\_marking\_refs** property (and therefore the markings applied to the object) are treated the same as changes to any other properties on the object and follow the same rules for versioning.

​

**Examples**

This example marks the Indicator and all its properties with the Marking Definition referenced by the ID.

{

"type": "indicator",

"spec\_version": "2.1",

"id": "indicator--b346b4b3-f4b7-4235-b659-f985f65f0009",

...

"object\_marking\_refs": ["marking-definition--34098fce-860f-48ae-8e50-ebd3cc5e41da"],

...

}

### ​7.2.3 Granular Markings

Whereas object markings apply to an entire STIX Object or Marking Definition and all its properties, granular markings allow both data markings and language markings to be applied to individual portions of STIX Objects and Marking Definitions. Granular markings are specified in the **granular\_markings** property, which is a list of granular-marking instances. Each of those instances contains a list of selectors to indicate what is marked and either a reference to the marking-definition object to be applied or a language code to be applied. Granular markings can be used, for example, to indicate that the **name** property of an indicator should be handled as TLP:GREEN, the **description** property as TLP:AMBER, and the **pattern** property as TLP:RED.

The **granular\_markings** property can also be used for language markings. To support applying both data markings and language markings to an object, the granular-marking type has a choice of two properties in addition to the selector: the **lang** property is used to apply language markings, and the **marking\_ref** property is used to apply data markings. Because each granular marking instance applies to either a language or a marking, one and only one of these properties **MUST** be present on each instance of a granular marking.

#### ​7.2.3.1​ Granular Marking Type

The granular-marking type defines how the marking-definition object referenced by the **marking\_ref** property or a language specified by the **lang** property applies to a set of content identified by the list of selectors in the **selectors** property.

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **lang** (optional) | string | The **lang** property identifies the language of the text identified by this marking. The value of the **lang** property, if present, **MUST** be an [[RFC5646](#kix.5jvc7h6u3pms)] language code.  If the **marking\_ref** property is not present, this property **MUST** be present. If the **marking\_ref** property is present, this property **MUST NOT** be present. |
| **marking\_ref** (optional) | identifier | The **marking\_ref** property specifies the ID of the marking-definition object that describes the marking.  If the **lang** property is not present, this property **MUST** be present. If the **lang** property is present, this property **MUST NOT** be present. |
| **selectors**  (required) | list of type string | The **selectors** property specifies a list of selectors for content contained within the STIX Object in which this property appears. Selectors **MUST** conform to the syntax defined below.  The marking-definition referenced in the **marking\_ref** property is applied to the content selected by the selectors in this list.  The [[RFC5646](#kix.5jvc7h6u3pms)] language code specified by the **lang** property is applied to the content selected by the selectors in this list. |

​**Selector Syntax**

Selectors contained in the **selectors** list are strings that consist of multiple components that **MUST** be separated by the . character. Each component **MUST** be one of:

* A property name or dictionary key, e.g., description, or;
* A zero-based list index, specified as a non-negative integer in square brackets, e.g., [4]

Selectors denote path traversals: the root of each selector is the STIX Object that the **granular\_markings** property appears in. Starting from that root, for each component in the selector, properties and list items are traversed. When the complete list has been traversed, the value of the content is considered selected.

Selectors **MUST** refer to properties or list items that are actually present on the marked object.

As an example, consider the following STIX Object:

{

"id": "vulnerability--ee916c28-c7a4-4d0d-ad56-a8d357f89fef",

"spec\_version": "2.1",

"created": "2016-02-14T00:00:00.000Z",

"modified": "2016-02-14T00:00:00.000Z",

"type": "vulnerability",

"name": "CVE-2014-0160",

"description": "The (1) TLS...",

"external\_references": [{

"source\_name": "cve",

"external\_id": "CVE-2014-0160"

}],

"labels": ["heartbleed", "has-logo"]

}

Valid selectors:

* description selects the **description** property ("The (1) TLS...").
* external\_references.[0].source\_name selects the **source\_name** property of the first value of the **external\_references** list ("cve").
* labels.[0] selects the first item contained within the **labels** list ("heartbleed").
* labels selects the list contained in the **labels** property. Due to the recursive nature of the selector, that includes all items in the list (["heartbleed", "has-logo"]).
* external\_references selects the list contained in the **external\_references** property. Due to the recursive nature of the selector, that includes all list items and all properties of those list items.

Invalid selectors:

* pattern and external\_references.[3] are invalid selectors because they refer to content not present in that object.
* description.[0] is an invalid selector because the description property is a string and not a list.
* labels.name is an invalid selector because labels property is a list and not an object.

This syntax is inspired by JSONPath [[Goessner 2007](#qvelyeswt61d)] and is in fact a strict subset of allowable JSONPath expressions (with the exception that the '$' to indicate the root is implicit). Care should be taken when passing selectors to JSONPath evaluators to ensure that the root of the query is the individual STIX Object. It is expected, however, that selectors can be easily evaluated in programming languages that implement list and key/value mapping types (dictionaries, hashmaps, etc.) without resorting to an external library.

**Examples**

This example marks the **description** and **labels** properties with the marking-definition referenced in the **granular\_markings** property however the **name** property uses the object marking.

{

...

"granular\_markings": [

{

"marking\_ref": "marking-definition--089a6ecb-cc15-43cc-9494-767639779123",

"selectors": ["description", "labels"]

}

],

"object\_marking\_ref": "marking-definition--79e2fa14-02c6-40d7-aa4b-ebf281dd78ef"

"description": "Some description",

"name": "Some name",

"labels": ["first", "second"]

}

​​This example marks the default language for this object as English (in this case, the **name** property) and the **description** as German.

{  
 "type": "campaign",

"spec\_version": "2.1",  
 "id": "campaign--12a111f0-b824-4baf-a224-83b80237a094",

"lang": "en",  
 "created": "2017-02-08T21:31:22.007Z",  
 "modified": "2017-02-08T21:31:22.007Z",  
 "name": "Bank Attack",  
 "description": "Weitere Informationen über Banküberfall",

"granular\_markings": [

{

"selectors": ["description"],

"lang": "de"

}

]  
}

# ​**8​ STIX™ Bundle Object**

**Type Name:** bundle

A Bundle is a collection of arbitrary STIX Objects grouped together in a single container. A Bundle does not have any semantic meaning and the objects contained within the Bundle are not considered related by virtue of being in the same Bundle.

A STIX Bundle Object is not a STIX Object but makes use of the **type** and **id** Common Properties. A Bundle is transient, and implementations **SHOULD NOT** assume that other implementations will treat it as a persistent object or keep any custom properties found on the bundle itself.

The JSON MTI serialization uses the JSON Object type [[RFC8259](#mmt4e4p953r5)] when representing bundle.

## ​8.1​ Properties

|  |  |  |
| --- | --- | --- |
| **Property Name** | **Type** | **Description** |
| **type** (required) | string | The **type** property identifies the type of object. The value of this property **MUST** be bundle. |
| **id** (required) | identifier | An identifier for this Bundle. The **id** property for the Bundle is designed to help tools that may need it for processing, but tools are not required to store or track it. Tools that consume STIX should not rely on the ability to refer to bundles by ID. |
| **x\_usa\_gov\_banner\_marking\_ref (optional)** | identifier | When used in conjunction with ACS data markings, this contains the id of the most restrictive data marking definition of the bundle.  This is a customized property on bundle (see section [8.1​](#_​8.1​_Custom_Properties)) to support handling restrictions in multi-security fabric sharing. |
| **objects** (optional) | list of type *<STIX Object>* | Specifies a set of one or more STIX Objects. Objects in this list **MUST** be a STIX Object. |

## ​8.2​ Relationships

STIX Bundle Object is not a STIX Object and **MUST NOT** have any relationships to or from it.

​

**Examples**

{

"type": "bundle",

"id": "bundle--5d0092c5-5f74-4287-9642-33f4c354e56d",

"objects": [

{

"type": "indicator",

"spec\_version": "2.1",

"id": "indicator--8e2e2d2b-17d4-4cbf-938f-98ee46b3cd3f",

"created\_by\_ref": "identity--f431f809-377b-45e0-aa1c-6a4751cae5ff",

"created": "2016-04-29T14:09:00.000Z",

"modified": "2016-04-29T14:09:00.000Z",

"object\_marking\_refs": ["marking-definition--089a6ecb-cc15-43cc-9494-767639779123"],

"name": "Poison Ivy Malware",

"description": "This file is part of Poison Ivy",

"pattern": "[file:hashes.'SHA-256' = 'aec070645fe53ee3b3763059376134f058cc337247c978add178b6ccdfb0019f']"

}

]

}

# ​**11​ Customizing STIX™**

There are three primary means to customize STIX: Custom Properties, Custom Objects and Custom Extensions. Custom Properties provide a mechanism and requirements for adding properties not defined by this specification to existing STIX Objects. Custom Objects, on the other hand, provides a mechanism and requirements to create custom STIX Objects (objects not defined by this specification). Custom Extensions provide a mechanism and requirements for the specification of extensions not defined by this specification on SCOs.

A consumer that receives STIX content containing Custom Properties, Objects or Extensions it does not understand **MAY** refuse to process the content or **MAY** ignore those properties or objects and continue processing the content.

Producers of STIX content that contain Custom Properties, Objects or Extensions should recognize that consumers may not understand them and may ignore them. Producers should define any Custom Properties, Objects and Extensions they use, along with any rules for processing them, and make these definitions and rules accessible to any potential consumers. This specification does not specify a process for doing this.

Custom Properties **SHOULD** be used for cases where it is necessary to add one or more simple additional properties (i.e. key/value pairs) on an SCO. On the other hand, Custom Extensions **SHOULD** be used for cases where it is necessary to describe more complex additional properties (i.e., those with potentially multiple levels of hierarchy). As an example, a vendor-specific property that expresses some custom threat score for a File object should be added directly to the SCO as a custom property, whereas a set of properties that represent metadata around a new file system to the File object should be done as a custom extension.

## ​11.1​ Custom Properties

There will be cases where certain information exchanges can be improved by adding properties to STIX Objects that are neither specified nor reserved in this specification; these properties are called **Custom Properties**. This section provides guidance and requirements for how producers can use Custom Properties and how consumers should interpret them in order to extend STIX in an interoperable manner.

### ​11.1.1​ Requirements

* A STIX Object **MAY** have any number of Custom Properties.
* Custom Property names **MUST** be in ASCII and **MUST** only contain the characters a–z (lowercase ASCII), 0–9, and underscore (\_).
* Custom Property names **SHOULD** start with “x\_” followed by a source unique identifier (such as a domain name with dots replaced by underscores), an underscore and then the name. For example, **x\_example\_com\_customfield**.
* Custom Property names **MUST** have a minimum length of 3 ASCII characters.
* Custom Property names **MUST** be no longer than 250 ASCII characters in length.
* Custom Property names that do not start with “x\_” may be used in a future version of the specification for a different meaning. If compatibility with future versions of this specification is required, the “x\_” prefix **MUST** be used.
* Custom Properties **SHOULD** only be used when there are no existing properties defined by the STIX specification that fulfils that need.
* For Custom Properties that use the hex type, the property name **MUST** end with '\_hex'.
* For Custom Properties that use the binary type, the property name **MUST** end with '\_bin'.

**Examples**

{

...,

"x\_acme\_org\_risk\_score": 10,

"x\_acme\_org\_scoring": {

"impact": "high",

"probability": "low"

},

...

}

## ​11.2​ Custom Objects

There will be cases where certain information exchanges can be improved by adding objects that are not specified nor reserved in this specification; these objects are called **Custom Objects**. This section provides guidance and requirements for how producers can use Custom Objects and how consumers should interpret them in order to extend STIX in an interoperable manner.

### ​11.2.1​ Requirements

* Producers **MAY** include any number of Custom Objects in STIX content.
* Custom Objects **MUST** support the Common Properties as defined in section [3.2](#_xzbicbtscatx).
  + Common property names **MUST NOT** be reused to represent the custom properties in the object.
* A Custom Object **MUST** have one or more properties.
* The name of a property of a Custom Object **MUST** be in ASCII and **MUST** only contain the characters a–z (lowercase ASCII), 0–9, and underscore (\_). The "x\_" prefix as described in section 11.1.1 **MAY** be used.
* The name of a property of a Custom Object **MUST** have a minimum length of 3 ASCII characters.
* The name of a property of a Custom Object **MUST** be no longer than 250 ASCII characters in length.
* The **type** property in a Custom Object **MUST** be in ASCII and **MUST** only contain the characters a–z (lowercase ASCII), 0–9, and hyphen (-).
* The **type** property **MUST NOT** contain a hyphen (-) character immediately following another hyphen (-) character.
* Custom Object names **MUST** have a minimum length of 3 ASCII characters.
* Custom Object names **MUST** be no longer than 250 ASCII characters in length.
* The value of the **type** property in a Custom Object **SHOULD** start with “x-” followed by a source unique identifier (like a domain name with dots replaced by hyphens), a hyphen and then the name. For example, x-example-com-customobject.
* A Custom Object whose name is not prefixed with “x-” may be used in a future version of the specification with a different meaning. Therefore, if compatibility with future versions of this specification is required, the “x-” prefix **MUST** be used.
* The value of the **id** property in a Custom Object **MUST** use the same format as the identifier type, namely, [object-type]--[UUID].
* Custom Objects **SHOULD** only be used when there is no existing STIX Object defined by the STIX specification that fulfils that need.

**Examples**

{

"type": "bundle",

"id": "bundle--f37aa79d-f5f5-4af7-874b-734d32c08c10",

"objects": [

{

"type": "x-example-com-customobject",

"id": "x-example-com-customobject--4527e5de-8572-446a-a57a-706f15467461",

"created": "2016-08-01T00:00:00.000Z",

"modified": "2016-08-01T00:00:00.000Z",

"some\_custom\_stuff": 14,

"other\_custom\_stuff": "hello"

}

]

}​

## ​11.3​ Custom Object Extensions

In addition to the Predefined Cyber Observable Object extensions, STIX supports user-defined custom extensions for STIX Cyber-observable Objects (SCO). As with Predefined Object Extensions, custom extension data **MUST** be conveyed under the extensions property. Note, custom extensions can only be used with SCOs.

### ​11.3.1​ Requirements

* A SCO **MAY** have any number of Custom Extensions.
* Custom Extension names **MUST** be in ASCII and are limited to characters a-z (lowercase ASCII), 0-9, and hyphen (-).
* Custom Extension names **SHOULD** start with “x-” followed by a source unique identifier (like a domain name), a hyphen and then the name. For example: x-example-com-customextension.
* Custom Extension names **MUST** have a minimum length of 3 ASCII characters.
* Custom Extension names **MUST** be no longer than 250 ASCII characters in length.
* Custom Extension names that are not prefixed with “x-” may be used in a future version of the specification for a different meaning. If compatibility with future versions of this specification is required, the “x-” prefix **MUST** be used.
* Custom Extensions **SHOULD** only be used when there is no existing extension defined by the STIX 2.1 specification that fulfills that need.
* A Custom Extension **MUST** have one or more properties.

**Examples**

*Custom File object extension*

{

"type": "file",

"hashes": {

"SHA-256": "effb46bba03f6c8aea5c653f9cf984f170dcdd3bbbe2ff6843c3e5da0e698766"

},

"extensions": {

"x-example-com-foo": {

"foo\_val": "foo",

"bar\_val": "bar"

}

}

}

# ​**Appendix E. Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Editor** | **Changes Made** |
| 01 | 2018-10-23 | Gregory Cheatham  Terri Hayes  Toni Haynes  Ivan Kirillov  Timothy Lachapelle  Mark Munoz  Rich Piazza  Scott Pinkerton  David Schuler  Craig Schweinhart  Kathy Simunich  Marlon Taylor  David Thomas | Initial Version |
| 02 | 2019-09-30 | Gregory Cheatham  Terri Hayes  Toni Haynes  Ivan Kirillov  Timothy Lachapelle  Mark Munoz  Rich Piazza  Scott Pinkerton  David Schuler  Craig Schweinhart  Kathy Simunich  Marlon Taylor  David Thomas | Redesign x-isa-acs-control-set-type. |

1. "original" in this definition is taken directly from [ref]. This is assumed to be a typo in that document, and the classified\_by property should contain the name of the person who created the derivative classification. [↑](#footnote-ref-1)
2. <https://api.nsgreg.nga.mil/geo-political/ISO3166-1/3/VI-12> [↑](#footnote-ref-2)
3. <https://api.nsgreg.nga.mil/geo-political/ISO3166-1/3/VI-12> [↑](#footnote-ref-3)