**Security and Privacy**

The current draft Energy Interoperation Common Transactive Services (CTS) document has the following guidance from OASIS on this topic:

Appendix B. Security and Privacy Considerations Note:

OASIS strongly recommends that Technical Committees consider issues that might affect safety, security, privacy, and/or data protection in implementations of their work products and document these for implementers and adopters. For some purposes, you may find it required, e.g., if you apply for IANA registration. While it may not be immediately obvious how your work product might make systems vulnerable to attack, most work products, because they involve communications between systems, message formats, or system settings, open potential channels for exploit. For example, IETF [RFC3552] lists “eavesdropping, replay, message insertion, deletion, modification, and man-in-the-middle” as well as potential denial of service attacks as threats that must be considered and, if appropriate, addressed in IETF RFCs. In addition to considering and describing foreseeable risks, this section should include guidance on how implementers and adopters can protect against these risks. We encourage editors and TC members concerned with this subject to read Guidelines for Writing RFC Text on Security Considerations, IETF [[RFC3552](https://www.bing.com/search?q=rfc+3552&cvid=3e6281644c394a44a6d312bfe4ad451e&aqs=edge.0.0.4333j0j1&pglt=43&FORM=ANNTA1&PC=LCTS)], for more information.

 A review of relevant OASIS TC documents to be considered:

* 1. OData (Open Data Protocol) – Chapter 12
	2. STIX (Structured Threat Information Expression) – Appendix D (IANA)
	3. CACAO (Security Playbooks) – Appendix B (IANA in Appendix C)
	4. XACML (eXtensible Access Control Markup Language) – Chapter 8
	5. Privacy Management Reference Model
	6. COEL (Classification of Everyday Life)

**OData** provides the following Section 12 for Security Considerations. There is no mention of privacy. It is not large but may be a helpful model.

**12    [Security Considerations](http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html%22%20%5Cl%20%22sec_SecurityConsiderations)**

This section is provided as a service to the application developers, information providers, and users of OData version 4.0 giving some references to starting points for securing OData services as specified.

OData is a REST-full multi-format service that depends on other services and thus inherits both sides of the coin, security enhancements and concerns alike from the latter.

For HTTP relevant security implications please cf. the relevant sections of [**[RFC7231]**](http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html#HTTPSemantic) (9. Security Considerations) and for the HTTP PATCH method [**[RFC5789]**](http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html#RFC5789) (5. Security Considerations) as starting points.

**12.1 [Authentication](http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html%22%20%5Cl%20%22sec_Authentication)**

OData Services requiring authentication SHOULD consider supporting basic authentication as defined in [**[RFC7617]**](http://docs.oasis-open.org/odata/odata/v4.01/odata-v4.01-part1-protocol.html#RFC7617) over HTTPS for the highest level of interoperability with generic clients. They MAY support other authentication methods.

+++++++++++++++++++

**STIX** - "Security considerations" and "Privacy considerations" are parts of the IANA Considerations (Appendix D) - mostly references to other documents. - <https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#_6aygoa1w5oc6>

Appendix D. IANA Considerations

This appendix contains the required information to register the STIX media type with IANA. While some of the information here is only for IANA, implementers of STIX should pay close attention to the security considerations and privacy considerations outlined in this appendix.

This document defines the "application/stix+json" media type

Media type name:  application

Media subtype name:  stix+json

Required parameters:  None

Optional parameters:  version

This parameter is used to designate the specification version of STIX that is being used during HTTP content negotiation. Example: "application/stix+json;version=2.1". The parameter value is of the form 'n.m', where n is the major version and m the minor version, both unsigned integer values.

Encoding considerations:  binary

Encoding considerations are identical to those specified for the "application/json" media type. See [[RFC8259](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#kix.7mjpf76rih72)].

Security considerations:

Security considerations relating to the generation and consumption of STIX messages are similar to application/json and are discussed in section 12 of [[RFC8259](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#kix.7mjpf76rih72)].

Unicode is used to represent text such as descriptions in the format. The considerations documented by Unicode Technical Report #36: Unicode Security Considerations [[UnicodeTR#36](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#6xn37k7emy22)] should be taken into account.

The STIX standard does not itself specify a transport mechanism for STIX documents. It is expected that TAXII is often used (which uses TLS via HTTPS). As there is no transport mechanism specified, it is up to the users of this to use an appropriately secured transport method. For example, TLS, JSON Web Encryption [[RFC7516](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#kix.a1a6no3ns9zm)] and/or JSON Web Signature [[RFC7515](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#kix.uvrynvap3wz)] can provide such mechanisms.

Documents of "application/stix+json" are STIX based Cyber Threat Intelligence (CTI) documents. The documents may contain active or executable content as well as URLs, IP addresses, and domain names that are known or suspected to be malicious. Systems should thus take appropriate precautions before decoding any of this content, either for persistent storage or execution purposes. Such precautions may include measures such as de-fanging, sandboxing, or other measures. The samples included in STIX documents are reference samples only, and there is no provision or expectation in the specification that they will be loaded and/or executed. There are provisions in the specification to encrypt these samples so that even if a tool decodes the data, a further active step must be done before the payload will be "live". It is highly recommended that all active code be armored in this manner.

STIX specifies the use of hashing and encryption mechanisms for some data types. A cryptography expert should be consulted when choosing which hashing or encryption algorithms to use to ensure that they do not have any security issues.

STIX provides a graph-based data model. As such, STIX implementations should implement protections against graph queries that can potentially consume a significant amount of resources and prevent the implementation from functioning in a normal way.

This specification also describes "STIX Patterning", a mechanism to describe and evaluate a search/match for data observed on systems and networks. Patterning is a grammar itself and includes PCRE regular expressions. Care should be taken when parsing and evaluating the grammar (particularly when evaluating PCRE from unknown or untrusted sources) as they can potentially consume a significant amount of resources.

Privacy considerations:

These considerations are, in part, derived from Section 10 of the Resource-Oriented Lightweight Information Exchange [[RFC8322](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#3aveyvn8n6s4)].

Documents may include highly confidential, personal (PII), and/or classified information. There are methods in the standard for marking elements of the document such that the consumer knows of these limitations. These markings may not always be used. For example, an out-of-band agreement may cover and restrict sharing. Just because a document is not marked as containing information that should not be shared does not mean that a document is free for sharing. It may be the case that a legal agreement has been entered into between the parties sharing documents, and that each party understands and follows their obligations under that agreement as well as any applicable laws or regulations.

Adoption of the information-sharing approach described in this document will enable users to more easily perform correlations across separate, and potentially unrelated, cybersecurity information providers. A client may succeed in assembling a data set that would not have been permitted within the context of the authorization policies of either provider when considered individually. Thus, providers may face a risk of an attacker obtaining an access that constitutes an undetected separation of duties (SOD) violation. It is important to note that this risk is not unique to this specification, and a similar potential for abuse exists with any other cybersecurity information-sharing protocol.

Interoperability considerations:

The STIX specification specifies the format of conforming messages and the interpretation thereof. In addition, the OASIS Cyber Threat Intelligence (CTI) Technical Committee has defined interoperability tests to ensure conforming products and solutions can exchange STIX documents.

Published specification:

STIX Version 2.1 OASIS Committee Specification 01

http://docs.oasis-open.org/cti/stix/v2.1/cs01/stix-v2.1-cs01.html

Cited in the "OASIS Standards" document:

https://www.oasis-open.org/standards#oasiscommiteespecs, from

https://www.oasis-open.org/standards#stix2.1

Applications which use this media:

Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence (CTI) such as Threat Actors, Campaigns, Intrusion Sets, Attack Patterns, Indicators of Compromise, etc. STIX enables organizations to share CTI with one another in a consistent and machine-readable manner, allowing security communities to better understand what computer-based attacks they are most likely to see and to anticipate and/or respond to those attacks faster and more effectively. STIX is designed to improve many different capabilities, such as collaborative threat analysis, automated threat exchange, automated detection and response, and more.

Fragment identifier considerations:  None

Restrictions on usage:  None

Additional information:

1. Deprecated alias names for this type: application/vnd.oasis.stix+json

2. Magic number(s): n/a [[RFC8259](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#kix.7mjpf76rih72)]

3. File extension(s): stix

4. Macintosh file type code: TEXT [[RFC8259](https://docs.oasis-open.org/cti/stix/v2.1/cs02/stix-v2.1-cs02.html#kix.7mjpf76rih72)]

5. Object Identifiers: None

Person and email to contact for further information:  Chet Ensign (chet.ensign@oasis-open.org)

Intended usage:  COMMON

Author:

OASIS Cyber Threat Intelligence (CTI) Technical Committee;

URI reference: http://www.oasis-open.org/committees/cti/.

Change controller:  OASIS

Provisional registration:  No

++++++++++++++++++++++++++++++++++++++++++

**CACAO** - Security Playbooks - pretty good example
- <https://docs.oasis-open.org/cacao/security-playbooks/v1.0/csd03/security-playbooks-v1.0-csd03.html#_6aygoa1w5oc6>

Appendix B. Security and Privacy Considerations

The following two sections are copied verbatim into the IANA Considerations Appendix.

B.1 Security Considerations

Security considerations relating to the generation and consumption of CACAO messages are similar to application/json and are discussed in section 12 of [RFC8259].

Unicode is used to represent text such as descriptions in the format. The considerations documented by Unicode Technical Report #36: Unicode Security Considerations [UnicodeTR#36] should be taken into account.

The CACAO standard does not itself specify a transport mechanism for CACAO documents. As there is no transport mechanism specified, it is up to the users of this specification to use an appropriately secured transport method, for example TLS.

Documents of "application/cacao+json" are CACAO based Cybersecurity Playbook documents. The documents may contain active or executable content as well as URLs, IP addresses, and domain names that are known or suspected to be malicious. Systems should thus take appropriate precautions before decoding any of this content, either for persistent storage or execution purposes. Such precautions may include measures such as de-fanging, sandboxing, or other measures. The samples included in CACAO documents are reference samples only, and there is no provision or expectation in the specification that they will be loaded and/or executed. There are provisions in the specification to encrypt these samples so that even if a tool decodes the data, a further active step must be done before the payload will be "live". It is highly recommended that all active code be armored in this manner.

CACAO specifies the use of hashing and encryption mechanisms for some data types. A cryptography expert should be consulted when choosing which hashing or encryption algorithms to use to ensure that they do not have any security issues.

CACAO specifies the use of digital signature technology that is based on concepts from JWS [RFC7515], JWK [RFC7517], and relies on JCS [RFC8785]. In addition to the security considerations defined in section 10 of JWS, section 9 of JWK, and section 5 of JCS, implementers should carefully consider and verify any digital certificate that is delivered via the CACAO Playbook itself to ensure that it is coming from the identity that it claims to come from.

CACAO provides a graph-based data model. As such, CACAO implementations should implement protections against graph queries that can potentially consume a significant amount of resources and prevent the implementation from functioning in a normal way.

B.2 Privacy Considerations

These considerations are, in part, derived from section 10 of the Resource-Oriented Lightweight Information Exchange [RFC8322].

Documents may include highly confidential, personally identifiable (PII), and classified information. There are methods in the standard for marking elements of the document such that the consumer knows of these limitations. These markings may not always be used. For example, an out-of-band agreement may cover and restrict sharing. Just because a document is not marked as containing information that should not be shared does not mean that a document is free for sharing. It may be the case that a legal agreement has been entered into between the parties sharing documents, and that each party understands and follows their obligations under that agreement as well as any applicable laws or regulations.

Further, a client may succeed in assembling a data set that would not have been permitted within the context of the authorization policies of either provider when considered individually. Thus, providers may face a risk of an attacker obtaining an access that constitutes an undetected separation of duties (SOD) violation. It is important to note that this risk is not unique to this specification, and a similar potential for abuse exists with any other cybersecurity information-sharing protocol.

+++++++++++++++++++++++++++++++++++++

**XACML** - Related and Nested Entities Profile, decent discussion, considers various parts of the security environment and effects on several aspects of the specification.
- <https://docs.oasis-open.org/xacml/xacml-3.0-related-entities/v1.0/cs02/xacml-3.0-related-entities-v1.0-cs02.html#_Toc54187782>

8      Security Considerations

***Entities*** may contain sensitive information that must be protected from unauthorized disclosure. A policy writer interacting with a policy administration point (PAP) would not normally see any ***entities*** known to the PIP or PEP, but there are ways a policy writer could manipulate policies in order to discover the values of ***entity*** attributes.

The most direct method is to use attribute assignment expressions in obligations and advice **[XACML3]**. Attribute assignment expressions provide a means to return information from the request context to the PEP. This attack requires the existence of an obligation or advice that presents the extracted attribute values in a form that is accessible to the policy writer. For example, an obligation that can be co-opted to send an email to the policy writer, display an on-screen message in an application that the policy writer uses or print a message in a log file that the policy writer can read. The policy writer adds such an obligation or advice to a policy that is under the writer’s control. The policy writer can then cause the targeted information to be extracted by instigating an access attempt for which the policy is applicable, or by just waiting until such an access attempt occurs in the course of normal operations.

A more indirect method of exposing ***entity*** attributes is to change a target or condition in a policy under the control of the policy writer so that an authorization decision is dependent on the value of an ***entity*** attribute the policy writer is attempting to discover. Using relational functions (type‑less‑than, type‑equal and type‑greater‑than) and a binary search, the policy writer can home in on the actual value of the ***entity*** attribute by iteratively editing the condition and observing the effect on the authorization decision.

These methods are available using only the core capabilities of XACML, however, the attribute-designator function defined in this profile allows access to ***entities*** that might not otherwise be accessible through the request context.

If a policy writer is a highly privileged user with access to the ***entity*** data stores underlying the PIP and PEP, then the fact that the policy writer can obtain information about ***entities*** by other means is not an issue. However, there are two ways a less-privileged user can inject a malicious policy.

The <XACMLAuthzDecisionQuery> element **[SAML]** allows an XACML client to include additional policies to be used by the PDP in evaluating the authorization request. A malicious client (or a client that has been compromised by a malicious user) could provide a policy that is designed to discover ***entity*** attributes.

The Administration and Delegation Profile **[ADMIN]** defines a mechanism for the delegation of policy administration. A delegate can create arbitrary policies, but the applicability of those policies is limited in scope by administrative policies created by trusted policy writers. However, the procedure for establishing the authority of a delegate’s policy does not take into consideration the obligations and advice in the policy. There is no verification of the obligations and advice and therefore no restriction on the attribute assignment expressions the delegate uses. The procedure also does not restrict which functions or attributes the delegate can use in a policy. The delegate could create a policy that is applicable within the delegated scope, but is designed to discover ***entity***attributes.

To protect ***entity*** attributes from unauthorized disclosure, implementers might consider the following strategies:

* Disallow policies and policy sets in <XACMLAuthzDecisionQuery> elements.
* Only accept policies and policy sets in <XACMLAuthzDecisionQuery> elements provided by authenticated, trusted clients.
* Disallow the attribute-designator function in policies and policy sets provided in <XACMLAuthzDecisionQuery> elements. Note that this still leaves the contents of the predefined ***entities*** such as the access subject and resource open to discovery.
* Apply access controls to the ***entity***attributes accessed by policies and policy sets in <XACMLAuthzDecisionQuery> elements, or otherwise limit the ***entities*** and ***entity*** attributes that these policies and policy sets can access.

With respect to delegation, implementers might consider the following mitigation strategies:

* Disable or not implement the capabilities of the Administration and Delegation Profile.
* Disallow the attribute-designator function in policies and policy sets written by delegates. Note that this still leaves the contents of the predefined ***entities*** open to discovery.
* Have the PAP limit the ***entity*** attributes that delegates can reference in their policies.
* Apply access controls to the ***entity***attributes accessed by delegate’s policies and policy sets during reduction **[ADMIN]** by the PDP.

A malicious policy writer could use ***quantified expressions*** to deliberately create policies that perform excessive computation resulting in a reduction of service or denial of service for applications using the PDP. ***Quantified expressions*** should be considered in whatever methods are used to mitigate denial of service attacks.

+++++++++++++++++++++++++++++++++++++++++++

**PMRM -** Privacy Management Reference Model

[Quick Start Guide for Data Protection to Support Regulatory Compliance Version 9.0 (oasis-open.org)](https://docs.oasis-open.org/pmrm/PMRM-guide/v9.0/cnd01/PMRM-guide-v9.0-cnd01.html)

See Step 3 of the quick start process guide

|  |  |
| --- | --- |
| ***Step 3:*** **List the Privacy Policy Conformance Criteria you are aware of – internal privacy and security policies -- regulatory mandates applicable to the Use Case -- existing privacy statements – existing controls** (PMRM Task; #3)  |  ·         Collect commitments and privacy controls already made by your organization in the form of any existing privacy and security policies and public privacy statements.·         Include any inherited privacy commitments and controls from other organizations and exported privacy commitments and controls that you require other organizations to implement.·         Highlight the commitments and controls that seem applicable to this Use Case.·         State whether your initial review indicates that this Use Case is/is not/or may be governed by the GDPR and/or other laws and regulations.·         If *yes or may be*, note the particular regulations and related references material.  If *no,*state why not or what you have done to find out.·         Identify any known risks associated with these privacy controls (PMRM Task  #19) |

Also see steps 2, 4 and 5 referencing privacy

++++++++++++++++++++++++++++++++++++++++++++

**COEL –** Classification of Everyday Living

[Classification of Everyday Living Version 1.0 (oasis-open.org)](https://docs.oasis-open.org/coel/COEL/v1.0/os/COEL-v1.0-os.html)

**6      Security**

**6.1 General Technical Principles**

**6.1.1 Internet**

SSL/TLS **[RFC5246]**SHALL be used for all internet communications within the Architecture. This creates an encrypted channel for the data (Behavioural Atoms, Report Data, Segment Data and Pseudonymous Keys) and prevents a third party from reading it in transit. It means that servers like the IDA, Data Engine and any Service Provider and Operator systems MUST use SSL/TLS certificates.

**6.1.2 Pseudonymous Keys**

IDA generated Pseudonymous Keys SHALL be used as the userids for the roles and actors in the Architecture. These are devoid of DIPI and unique across the Architecture. Pseudonymous Keys used as ConsumerIDs need to be handled securely and carefully since they could be mis-used to pollute the Atom collection in a Data Engine, or to retrieve data about a Consumer if a Service Provider's credentials are divulged.

**6.1.3 Userids and passwords**

Different userids MAY be used and different passwords SHALL be used for each service layer (e.g. for Operator with Identity Authority, Operator with Data Engine). These SHALL be encrypted when stored. Separate credentials SHOULD be used to access the Management Interface (MMI) and Query Interface (PQI), reducing the likelihood of getting access to both and retrieving Atoms for all of a Service Provider’s Consumers.

Where the Operator is a separate entity from the Service Provider, it SHOULD use BasicAuth, as a minimum, to request/return reports from its Service Provider. These reports SHALL be pseudonymised and contain no DIPI.

**11 Privacy-by-Design Implementations (non-normative)**

**11.1 Introduction**

This section describes how the normative elements of the COEL Specification can be configured to achieve a privacy-by-design implementation within an Ecosystem managed by a single IDA. It sets out principles of operation, controls the roles that actors can perform and gives detailed requirements of the responsibilities of actors.

**11.2 Principles**

**11.2.1 Data Separation Principle (P1)**

The COEL Specification implements a separation of data types for specific roles and this principle extend this to the actors. Data Engines keep data on *what* Consumers do (COEL Behavioural Atoms) and the Operator keeps data on *who* Consumers are (DIPI). No single organisation holds both sets of data together. This means that it would need a double accidental or malicious disclosure for connected information to be released.

**11.2.2 Data Atomisation Principle (P2)**

Data is deliberately broken down into small chunks of information by the Operator and coded with the Consumer’s ConsumerID, thus each separate COEL Behavioural Atom has a very low privacy risk.

**11.2.3 Atomised Consent Principle (P3)**

Consumers give informed consent to the Operator or are provided appropriate notice under the requirements set out in this section. This allows the Operator to sign up the Consumer with a ConsumerID. This ConsumerID is the indicator to Identity Authority and other Ecosystem actors that appropriate consent or notice is in place. The requirement for every COEL Behavioural Atom to have a ConsumerID (or associated DeviceID) in combination with the detailed consent fields, ensures each Atom has that Consumer’s consent / notice written into the structure of the data. The time stamp uniquely associated with each COEL Behavioural Atom allows full auditing of this principle.

**11.2.4 Separation of Competence Principle (P4)**

Data Engines are expert data handlers. They know how to run robust, secure and always on cloud based data services; they handle COEL Behavioural Atoms not Consumers. Service Providers are expert at manipulating behavioural data to deliver services and service content; they handle COEL Behavioural Atoms not Consumers. Operators are experts at Consumer facing services and handling DIPI; they handle Consumers not COEL Behavioural Atoms. The Identity Authority is expert at overseeing the Ecosystem.

**11.2.5 No Conflict of Interest Principle (P5)**

Consumers need to see that there are no conflicts around their data. To ensure this, the Identity Authority acts on behalf of the Consumer in partnership with Operator, Service Provider, Data Engine and regulators.

**11.2.6 Active Support Principle (P6)**

All actors will actively promote these principles, safeguard the structure of the Ecosystem and support good data practice for both individuals and enterprises.

**11.2.7 Transparency Principle (P7)**

The roles and identities of all the actors in the Ecosystem who are working together on behalf of a Consumer will be clear and visible to that Consumer.

**11.3 Actors' Responsibilities**

The roles will be performed by a number of actors that create the Ecosystem. Actors can have multiple roles but certain combinations are not permissible as described in the requirements and the table below. The table shows all the possible roles an actor can have (✓ = role that an actor can take on; ✗ = role that an actor cannot take on).

This is followed by tables that include responsibilities for actor – example below:

11.3.3 references security related to the service provider

Revision history indicates an update to add sections for ‘Privacy-by-Design’, ‘Security’ & ‘Identity Management’. This text was brought over from RPE.