NIST Internal Report 8112 (Draft)

Attribute Metadata

Paul A. Grassi
Ellen M. Nadeau
Ryan J. Galluzzo
Abhiraj T. Dinh

COMPUTER SECURITY

NIST Internal Report 8112 (Draft)

Attribute Metadata

Paul A. Grassi
Ellen M. Nadeau
Applied CyberSecurity Division
Information Technology Laboratory

Ryan J. Galluzzo
Abhiraj T. Dinh
Deloitte & Touche LLP
Rosslyn, VA

August 2016

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie E. May, Under Secretary of Commerce for Standards and Technology and Director

National Institute of Standards and Technology Internal Report 8112
xxx pages (MonthTBD 2016)
CODEN: NSPUE2

Comments on this publication may be submitted to: nsticworkshop@nist.gov

Public comment period: 01 August 2016 - 30 September 2016

All comments are subject to release under the Freedom of Information Act (FOIA).

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-8930
Email: nsticworkshop@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

This NIST Internal Report contains a metadata schema for attributes that may be asserted about an individual during an online transaction. The schema can be used by relying parties to enrich access control policies, as well as during runtime evaluation of an individual's ability to access protected resources, and for an individual's. Attribute metadata could also create the possibility for data sharing permissions and limitations on individual data elements. There are other possible applications of attribute

metadata, such as evaluation and execution of business logic in decision support systems; however the metadata contained herein is focused on supporting an organization's risk-informed authorization policies and evaluation.

Keywords

Access control, assertions, attributes, attribute metadata, attribute values, attribute value metadata, authorization, federation, identity, identity federation, information security, metadata, privacy, risk, risk management, security, trust

Acknowledgements

The authors would like to thank Josh Freedman for his significant contributions to this report, as well as Sean Brooks and Naomi Lefkovitz for their considerate inclusion of privacy related content. In addition, we would like to thank Anil John and the Federal Identity, Credential, and Access Management (FICAM) Attribute Tiger Team for their leadership in developing the initial set of attribute metadata necessary for federal systems. Finally, we express significant gratitude to Darran Rolls of SailPoint Technologies, Inc., as well as Gerry Gebel and David Brossard of Axiomatics, for their insightful review of this report.

Executive Summary

This NIST IR proposes a schema for attribute metadata and attribute value metadata intended to convey information about a subject's attribute(s) to allow for a relying party (RP) to:

- Obtain greater understanding of how the attribute and its value were obtained, determined, and vetted;
- Have greater confidence in applying appropriate authorization decisions to subjects external to the domain of a protected system or data;
- Develop more granular access control policies;
- Make more effective authorization decisions; and
- Promote federation of attributes.

This document defines a set of optional elements to support cross-organization confidence in attribute assertions as well as the semantics and syntax required to support interoperability. The schema contains two core components, `attribute metadata` and `attribute value metadata` which, along with their suggested elements, are described below:

- **Attribute Metadata** - Metadata for the attribute itself, not the specific attribute's value. For example, this metadata may describe the `format` in which the attribute will be transmitted, height will always be sent in inches regardless of what the actual value may be (e.g., `height= 72`). This schema provides a set of attribute metadata from which to choose when constructing an attribute sharing agreement (trust-time) and the rationale for their inclusion.

Metadata	Description	Recommended Values
Description	An informative description of the attribute.	None
Allowed Values	A defined set of allowed values for the attribute.	None
Format	A defined format in which the attribute will be expressed.	None
Verification Frequency	The frequency at which the Attribute Provider will re-verify the attribute.	None

- **Attribute Value Metadata** - These elements focus on the asserted value for the attribute. Following the same example as above, the attribute value would be the actual height. A possible attribute value metadata for the height could be the name of the originating organization that provisioned the height, for example the DMV in the subject's home state. This schema provides a set of attribute value metadata, proposed values for those metadata fields, and rationale for their inclusion.

Metadata Element	Description	Values
Verifier	The entity that verified the attribute's value.	•Origin •Provider •Not Verified
Verification Method	The method by which the attribute value was verified as true, and belonging to the specific individual.	•Document Verification •Record Verification •Document Verification with Record Verification

Metadata Element	Description	Values
		•Proof of Possession •Not Verified
Last Update	The date and time when the attribute was last updated.	No restrictions
Expiration Date	The date an attribute's value is considered to be no longer valid.	No restrictions
Last Verification	The date and time when the attribute value was last verified as being true and belonging to the specified individual.	No restrictions
Origin	The legal name of the entity that issues or creates the initial attribute value.	•Origin's name •None
Provider	The legal name of the entity that is providing the attribute.	•Provider's Name •None
Pedigree	Description of the attribute value's relationship to the authoritative source of the value.	•Authoritative •Sourced •Self-Asserted •Derived
Individual Consented	Captures whether the user has expressly consented to providing the attribute value.	•Yes •No •Unknown
Date Consented	The date on which express consent for release of the attribute value was acquired.	No restrictions
Acceptable Uses	Allowed uses for entities that ingest attributes	•Authorization •Secondary Use •No Further Disclosure
Cache Time To Live	The length of time for which an attribute value may be cached.	No restrictions
Data Deletion Date	Indicates the date a certain attribute should be deleted from records.	No restrictions
Classification	The U.S. Federal Government security classification level of the attribute.	•Unclassified •Controlled Unclassified •Confidential •Secret •Top Secret
Releasability	The U.S. Federal Government restrictions regarding to whom and attribute value may be released.	•NATO •FVEY •NOFORN •Public Release •None

The schema in this document is intended to demonstrate the value of attribute and attribute value metadata in supporting U.S. Federal Government use cases and it is envisioned that the core set of metadata proposed here can serve as a library or menu from which both commercial and federal implementers can draw common semantics, syntaxes, and values to support their specific needs. This will serve as a jumping off point for the development of a metadata standard that can enable greater federation across markets and sectors.

Table of Contents

1. Introduction

Access control policy increasingly depends on evaluating the attributes of the individual (or subject) attempting to access a protected resource [SP 800-162]. As enterprise domains continue to expand, architectures become further distributed, business relationships become more complex, and organizations increasingly depend on federated identities, methods are needed for evaluating externally asserted attributes to make the best and most appropriate authorization decision possible. Such mechanisms will increase the ability of organizations to consume attributes as well as enrich and enforce critical access control policies. At the "Advanced Identity Workshop: Applying Measurement Science in the Identity Ecosystem" (hereafter just "workshop") held at NIST in Gaithersburg on January 12 and 13, 2016, NIST proposed an initial set of attribute metadata as a step towards enabling greater federation and trust of identity attributes among identity ecosystem participants. This NIST Internal Report (NISTIR) represents a refined list of optional metadata that may be adopted when participating in a federated environment.

1.1. Purpose

This NISTIR proposes a schema for attribute metadata and attribute value metadata, intended to convey information about a subject's attribute(s) to allow for a relying party (RP) to:

- Obtain greater understanding of how the attribute and its value were obtained, determined, and vetted;
- Promote greater confidence in applying appropriate authorization decisions to subjects external to the domain of a protected system or data (i.e., external users);
- Enable more effective authorization decisions; and
- Promote federation of attributes.

The model proposed in this document will help RPs determine the most appropriate attribute metadata elements for a given transaction. In the future, it could serve as a foundation for an attribute confidence scoring structure to further simplify the process of aligning attribute based authorization decisions with the risk environment.

In addition, as a NISTIR, this document is intended to be treated as an "implementers' draft" so that developers and access control policymakers can determine the efficacy and required adjustments of the attribute metadata elements. By issuing this as an implementers' draft, NIST seeks to obtain feedback on agencies' and industries' experiences with this approach in order to identify next steps, such as potentially transitioning this document to a Special Publication or a contribution to a private sector standards developer.

1.2. Scope

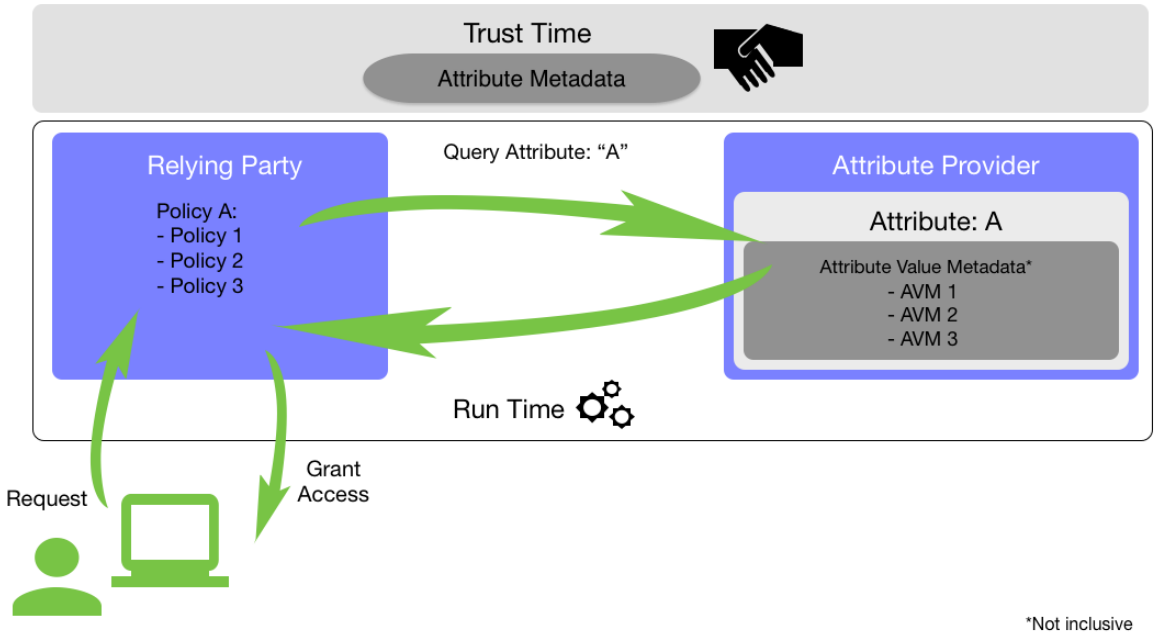
This NISTIR defines a set of optional elements of an attribute metadata schema to support cross-organization confidence, such as two executive branch agencies, in attribute assertions. It also provides the semantics and syntax required to support interoperability. As mentioned, NIST does not intend to make any of this schema required in federal systems and attribute-based information sharing. Rather, this schema represents a compendium of possible metadata elements to assist in risk-based decision making by an RP. This schema is focused on subjects (individual users); objects and data tagging, while related, are out of scope.

Specifically, this document addresses the following:

- **Attribute Metadata** - Metadata for the attribute itself, not the specific attribute's value. For example, this metadata may describe the format in which the attribute will be transmitted, height will always be sent in inches regardless of what the actual value may be (e.g., `height= '72'`). This schema provides a set of attribute metadata from which to choose when establishing an attribute sharing agreement (i.e., trust time) and the rationale for their inclusion.
- **Attribute Value Metadata** - These elements focus on the asserted value for the attribute. Following the same example as above, the attribute value would be the actual height (72"). A possible attribute value metadata for the height could be the name of the originating organization

that provisioned the height, for example the DMV in the subject's home state. This schema provides a set of attribute value metadata, proposed values for those metadata fields, and rationale for their inclusion.

- **Use Cases** - To demonstrate the applicability of the proposed metadata schema, this document also provides example use cases in which the application of the proposed schema would be used to support authorization decision making, thus allowing for greater confidence in federated identities and attributes.
- **Example Assertions** - Finally, this report includes example assertions illustrating what a technical implementation of the schema would look like leveraging market standards such as Extensible Access Control Markup Language (XACML).



While the schema in this document is intended to demonstrate the value of attribute metadata in supporting U.S. Federal Government use cases, the ideal metadata schema could be used in both commercial and public sector implementations, thus serving as a foundation to enable greater federation across markets and sectors. Furthermore, NIST intends for the schema to be protocol and technology agnostic, thus capable of being supported across the spectrum of modern runtime access control architectures.

2. Definitions and Acronyms

Assertion

A statement from an attribute provider to a relying party that contains identity attributes about a subject. Assertions may also contain authentication or other identity information about the subject.

Attribute

A claim of a named quality or characteristic inherent in or ascribed to someone or something.

Attribute Based Access Control (ABAC)

Access control based on attributes associated with subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which access may take place.

Attribute Claim (or "Claim")

A statement asserting a property of a subject without necessarily containing authentication or other identity information, independent of format. For example, for the attribute 'birthday', a claim could be 'older than 18' or 'born in December'.

Attribute Metadata

Data providing information about the context and structure of an attribute. See metadata.

Attribute Provider (AP)

Manages and provides assertions of identity attributes to other relying and federated parties.

Attribute Provider Statement (APS)

A document that captures the security, privacy, data protection, and attribute management practices of a given attribute provider or party acting as an attribute provider for a given set of transactions.

Attribute Value Metadata (AVM)

Data describing an asserted value for an associated attribute.

Authorization

The decision to permit or deny a subject access to resources (e.g., network, data, application, services) based on the evaluation of access control policies.

Credential Service Provider (CSP)

An entity that issues digital credentials to subjects and issues or registers authenticators for subjects' use. A CSP may be an independent third party, or may issue credentials for its own use. A CSP may provide and verify attributes or may include attributes provided or verified by other entities.

Federation

A process that allows for the conveyance of identity attributes and authentication information across a set of networked systems.

Identity Provider (IDP)

A CSP in a federation that manages the subject's primary authentication credentials and issues assertions derived from those credentials.

Metadata

Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about information or information about information.

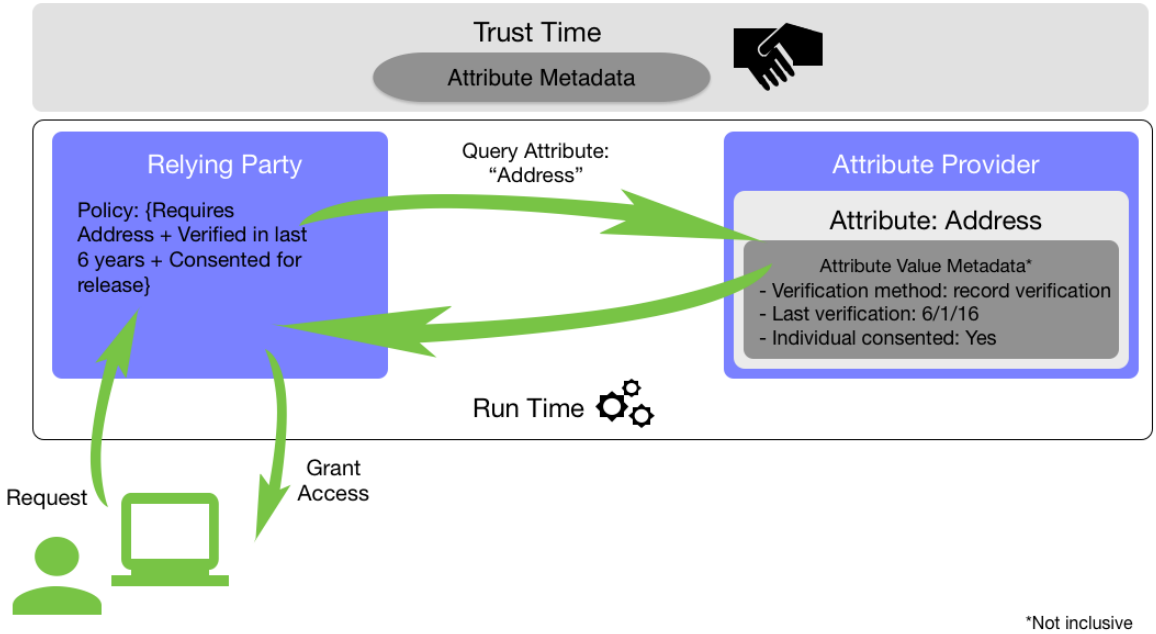
Relying Party (RP)

An entity that relies upon a subject's authenticator(s) and credentials or an IDP's assertion of a subject's identity, typically to process a transaction or to grant access to information or a system.

3. Metadata

The term *attribute* is used throughout this document to refer to a defined characteristic of an individual — often referred to as subject attributes. *Home address* is one example of an attribute of a person. The term *attribute value* is used throughout to refer to a specifically assigned value for an attribute; for example, Jane Doe's *home address* is *1 Main St., Anytown, VA 11111*. Attribute providers collect and maintain these elements—the attribute and its value—together. In a federated environment, these attributes are asserted to the relying party (RP) to support the provision of a benefit or service, or when authorizing access to a protected resource. Attributes and attribute values may also be associated with devices or non-person entities; however, these entities are not addressed in this document.

Oftentimes, a set of asserted attributes and their values is enough on its own to support access to systems or applications. In the instance above, the information provided may be sufficient to allow Jane to benefit from a service her town provides for residents. Alternatively, in more sensitive contexts (e.g., national security systems, systems that enable access to personally identifiable information), RPs may want additional information about the specific attributes and attribute values they are receiving. Who provided Jane's home address? Did she self-assert it, or did the attribute provider (AP) retrieve it from a database, such as the DMV or her employer? These data of the attributes, or metadata, enable the RP to interrogate the attribute value and information about the value itself during authorization policy evaluation. Information about the value may include where the attribute came from, whether it has been verified, and how often it is updated. This allows the RP to make a more informed decision about whether or not to trust an attribute when making access control decisions.



The attribute metadata and attribute value metadata listed in each section of this schema are not mandatory. Collectively, these elements aim to support transactional needs in federations and trust frameworks across the private and public sectors. NIST envisions that communities and federations will leverage the included metadata elements to develop their own profiles.

When implementing this schema, organizations must evaluate and understand both the authorization considerations and the privacy implications associated with a given use case or transaction type. With the

additional granularity that attribute and attribute value metadata can provide, new information can be revealed which may provide a broader profile of an individual than was intended or anticipated. For instance, asserting that the verifier of Jane's address is her employer reveals more than just 1 Main St., Anytown, VA to the receiving entity. The receiving entity now knows who she works for in addition to where she resides, something that Jane may not be aware of and may not wish to reveal. When deciding which metadata elements to select, the involved parties should conduct a privacy risk assessment to consider these possibilities, and to identify the potential negative impacts to privacy that could arise from including certain metadata elements. To guide this privacy risk assessment process, privacy considerations associated with the metadata elements are included throughout this document. This is certainly not an exhaustive list; there might be additional privacy considerations apart from those listed, and the listed considerations might change over time. Ultimately, the listed considerations may aid in deciding which elements of metadata to include, maximizing the benefit of a transaction while minimizing problems for the individuals associated with the metadata. If a metadata element does reveal information about an individual, but is still necessary to a transaction and thus must be included, the appropriate parties should consider how to provide visibility of the metadata to the individual, so he or she can predict the transfer of certain information.

3.1. Attribute Metadata

Attribute metadata provide information that is applicable to the attribute being asserted, regardless of the value of that attribute. Attribute metadata are intended to be static, discussed, and agreed upon by federated parties in advance of the actual assertion. For this reason, attribute metadata are considered "trust time" metadata and can be encapsulated in agreements such as attribute provider statements (APS), contracts, or trust frameworks. Table 1 provides the list of attribute metadata that organizations can consider when establishing identity federation agreements. This is unlike attribute value metadata, which are dynamic and thus asserted and evaluated at runtime.

Table 1: Attribute Metadata

Metadata	Description	Recommended Values
Description	An informative description of the attribute	None
Allowed Values	A defined set of allowed values for the attribute	None
Format	A defined format in which the attribute will be expressed	None
Verification Frequency	The frequency at which the AP will re-verify the attribute	None

3.1.1. Description

The `description` metadata element ensures that all entities participating in the federation of attributes have the same semantic understanding of the attribute. This enables both trust and interoperability by providing a common understanding of what the attribute and its value(s) represent. There are no set values for this metadata element as it is intended to be a free form, text-based definition.

3.1.2. Allowed Values

This metadata element provides a common, agreed-to set of values for an attribute. This ensures that when an attribute provider transmits the attribute, the receiving organization is able to appropriately process the values. Variations between provider and RP in expressing values for an attribute—for example, a value outside of an expected range—adversely impact interoperability and performance of authorization activities. For this reason, resolution of this metadata element is highly recommended.

3.1.3 Format

This metadata element describes the format for expressing attribute's value. For example, the attribute `height` may always be expressed in meters rather than centimeters. As with `allowed values`, up front agreement around the format of expressed attributes supports technical interoperability of assertions during run time as well as appropriate policy evaluation of the attributes when determining access to resources.

3.1.4. Verification Frequency

In most situations, it is highly beneficial for the RP and the AP to agree to set rates for periodic verification of attribute values. This metadata element captures the frequency with which this re-verification occurs, to ensure that both parties have established valid verification intervals. When determining if verification frequency is appropriate to include for a particular attribute, the parties should consider the fluidity of the attribute and its value; for example, date of birth may never need to be re-verified. They should also consider the risk associated with the transaction, or the environment in which the RP and AP are operating. Including this attribute metadata element may negate the need for some of the currency attribute value metadata elements discussed later in this paper.

3.2. Attribute Value Metadata

While attribute metadata are important, it is the granular attribute value metadata—for example, information about attribute values' authoritativeness, the processes used to create or establish them, and the frequency with which they are refreshed—that is designed to enable greater trust across systems. RPs can establish semantics and syntax of attribute value metadata at trust time in order to make authorization decisions about access to resources or benefits at run-time. Regardless of the access control methodology leveraged by an organization, integrating attribute value metadata into decision support systems can enable more informed decisions and support richer policy development.

3.2.1. Metadata Categories

While attribute value metadata may be used for many purposes by RPs, certain metadata elements are more commonly tied to specific types of decisions. To facilitate RP decision-making and increase interoperability, this schema establishes five categories based on common uses of metadata: accuracy, currency, provenance, privacy, and classification. Each category of metadata elements is important for enabling the federation of attributes across a community or environment. Metadata associated with accuracy, currency, and provenance may facilitate cross-system trust by establishing a consistent picture of the attribute value itself and the practices that generated that value, while privacy and classification can be leveraged to convey specific restrictions and protections that may need to be put in place based on certain data types, transactions, or use cases. Table 2 presents the five categories and their definitions. Table 3 provides a breakdown of the number of metadata elements by category.

The sections that follow list and provide details on the elements in each category.

Table 2: Categories of Attribute Value Metadata

Metadata Category	Description
Provenance	Metadata relevant or pertaining to evaluating the source of the attribute's value
Accuracy	Metadata relevant or pertaining to determining if the attribute's value is correct and belongs to a specific subject
Currency	Metadata relevant or pertaining to determining the "freshness" of a given attribute's value
Privacy	Metadata relevant or pertaining to privacy aspects of a given attribute's value
Classification	Metadata relevant or pertaining to the security classification of a given attribute's value

Table 3: Distribution of Attribute Value Metadata Elements

Metadata Category	Number of Elements
Accuracy	2
Provenance	3
Currency	3
Privacy	5
Classification	2
Total	**15**

3.2.1.1. Accuracy Metadata Elements

Metadata Element	Description	Recommended Values
Verifier	The entity that verified the attribute's value	•Origin •Provider •Not Verified
Verification Method	The method by which the attribute value was verified as true and belonging to the specific individual	•Document Verification •Record Verification •Document Verification with Record Verification •Proof of Possession •Not Verified

Verifier

Verified attributes allow RPs to make informed decisions around whether or not to trust an attribute's value during policy evaluation. In addition, understanding who verified an attribute value may influence the RP's decision about whether or not to accept an attribute value as part of an access control decision. The verifier metadata element is intended to answer this "who" question. Namely: did the organization that established the attribute value perform the verification themselves or was the verification done at a later date by the AP? Acceptable values for this metadata field include:

1. **Origin** - The attribute's value was verified by the entity that issued or created it (e.g., a Social Security Number verified by the Social Security Administration).
2. **Provider** - The attribute's value was verified by the attribute provider.
3. **Not Verified** - The value of the attribute was not verified.

Verification Method

This metadata element contains information on the process used to confirm that an attribute value is both true *and* belongs to the specified individual. This is sometimes necessary to support an authorization decision, but may not always be required. The acceptable values for `verification method` are intended to provide insight into the verification processes used by providers and enable greater confidence in a given attribute's value. This is particularly beneficial if there are multiple providers for instances of a single attribute. Recommended values for this element are:

1. **Document Verification** - The attribute value was verified by inspecting a document that is acceptable to the RP (e.g., driver's license, medical record, utility bill). Transactional participants may want to determine the types of acceptable documents for attribute value verification in advance.
2. **Record Verification** - The attribute value was verified against an authoritative record or database. For the purposes of this schema, the term "authoritative" is used consistently with its definition in SP 800-63-3.
3. **Document Verification with Record Verification** - The attribute value was verified against both an acceptable document and an authoritative record or database.
4. **Proof of Possession** - Confirmation of an individual's ability to demonstrate possession of a device or account is used to verify the attribute's value. Certain attributes and their values, such as phone numbers and email addresses, can be verified by direct communication (SMS, voice, or email) with the entity to which the value is attributed. This method of verification may not be applicable to all attribute values. However, to a certain set of attributes, this is a legitimate approach to determining that the attribute's value is both valid and associated with the appropriate individual.
5. **Not Verified** - The attribute's value has not been verified.

3.2.1.2. Currency Metadata

Metadata Element	Description	Recommended Values
Last Update	The date and time when the attribute was last updated	No restrictions
Expiration Date	The date an attribute's value is considered to be no longer valid	No restrictions
Last Verification	The date and time when the attribute value was last verified as being true and belonging to the specified individual	No restrictions

Last Update
`Last Update` contains information on the date and time when an attribute's value was last refreshed. The age of the attribute can be derived from this attribute value. `Last Update` also allows RPs to determine the currency of the attribute value, and whether the attribute was refreshed recently enough to be used in a particular transaction.

Expiration Date
Attribute values sent from an AP to an RP may only be valid for its defined use for a set amount of time, depending on requirements, policy, or legal factors. The date after which an attribute's value is considered no longer valid for its defined use is the `Expiration Date`. Though `Expiration Date` and `Last Update` both allow an RP to determine if an attribute's value is current and sufficient, `Expiration Date` differs from `Last Update` in that there is a specified date or threshold after which the attribute's value becomes void for its defined use. RPs have the freedom to accept attributes after they have been considered expired for their original intended use, but this decision is made at their own discretion based upon the intended use of the attribute value, the type of interaction it is supporting, and the environment in which they operate. For example, an RP may choose to accept a recently expired driver's license number for access to a low assurance service. However, it is unlikely that an agency would accept a lapsed security clearance for access to classified data.

Last Verification
RPs may not trust certain attribute values unless they've been verified within a certain time period. This is particularly true for certain attribute values such as *security clearance*, where the original established date of the value alone may not be sufficient for granting access to national security systems or data. `Last Verification` provides the most recent date and time at which the value was verified as true and belonging to the specified individual. This metadata focuses on the last date that verification occurred, and does not include any information about *methods* of verification.

3.2.1.3. Provenance Metadata

Metadata Element	Description	Recommended Values
Origin	The legal name of the entity that issues or creates the initial attribute value	•Origin's name •None
Provider	The legal name of the entity that is providing the attribute	•Provider's Name •None
Pedigree	Description of the attribute value's relationship to the authoritative source of the value	•Authoritative •Sourced •Self-Asserted •Derived

Origin
The `Origin` element conveys the legal name of the entity that established the initial attribute value. This may or may not be an authoritative entity, or the provider; if, for example, the AP generates the attribute value through a derivation process, then the AP would be the origin. The key distinction between the origin and the provider is the act of initially generating, capturing, or provisioning the attribute's value, rather than just asserting the attribute's value to an RP. Inclusion of this metadata element provides the RP with substantial insight, but at a potential cost to the individual as it may also reveal additional

information about the subject to whom the attribute value is bound. For example, this value could reveal employment status and location, socio-economic information, or even health history; all of which may have unintended and potentially negative consequences. Selection and use of this metadata element should be carefully considered based on both authorization needs as well as privacy requirements. For example, when leveraging attributes for access to moderate assurance level services that involve customers (i.e., non-enterprise users) it may be sufficient for the RP to request an attribute value's `verification method` without the `origin` element-which can reveal unnecessary information about a subject. The original source of the information may not be essential as long as the value has been verified using an acceptable method.

Provider
This specifies the legal name of the entity that supplies the attribute value to the RP. This element enables RPs to understand and evaluate individual attribute values that may be included in a bundle of attributes. For example, if a full service credential provider generates an assertion with several identity attributes provided by multiple APs, the `provider` element enables the RP to understand, at a granular level, where each has come from and determine whether or not that value can be used for access to specific resources. In instances where a single attribute is asserted directly to the RP, this element may not be necessary since the assertion itself will carry the provider information as well as a certificate or digital signature. The privacy considerations for this element are similar to those for origin. Divulging an individual's relationship with a particular provider allows for broader profiling, and the sharing of information that an individual might not know is being passed on, and might not want to be passed on.

Pedigree
`Pedigree` refers to the attribute value's relationship to an authoritative source. Essentially, it allows for the RP to better understand the process by which an attribute's value is generated and to determine whether or not it is from an acceptable authoritative source. Since this may reveal an individual's association with a separate entity, and potentially additional information can be inferred from this association, the privacy considerations mirror those explained above for provider and origin. Recommended values for this element include:

1. **Authoritative** - The attribute's value was acquired directly from the source of authority. For example, an AP has received a driver's license number directly from the state DMV which issued the license.
2. **Sourced** - The attribute's value has been acquired from one or more non-authoritative sources. For example, an AP purchases a driver's license number from a third-party data aggregator.
3. **Self-Asserted** - The value was provided to the AP directly by the individual with whom the attribute value is associated. For example, an AP receives a driver's license number directly from the individual who claims ownership of the license through a web form or questionnaire. Self-asserted attributes may also be verified or unverified.
4. **Derived** - The attribute value was produced through the analysis and manipulation of related attribute values and data. For example, if an AP requests a user's age, but it's not on file, then the AP may leverage the user's date of birth to assert age.

Taken in conjunction with the accuracy metadata, this information can enable the RP to better understand the origin of an attribute value, how it relates to its authoritative source, and how it has been verified — all of which help an RP establish a more complete picture of the value's usefulness and trustworthiness.

3.2.1.4. Privacy Metadata

Metadata Element	Description	Recommended Values
Individual Consented	Captures whether the user has expressly consented to providing the attribute value	•Yes •No •Unknown
Date Consented	The date on which express consent for release of the attribute value was acquired	No restrictions
Acceptable Uses	Allowed uses for entities that receive attributes	•Authorization •Secondary Use •No Further Disclosure
Cache Time To Live	The length of time for which an attribute value may be cached	No restrictions
Data Deletion Date	Indicates the date a certain attribute should be deleted from records	No restrictions

Individual Consented
RPs may have specific legal, policy, or business requirements regarding whether a user consented to the release of a specific attribute. This element enables organizations to meet those requirements, ensuring that they've gained express consent from an individual. Recommended values include:

1. **Yes** - The individual expressly consented to the release of the attribute's value for the purposes of the transaction.
2. **No** - The individual has not expressly consented to the release of the attribute's value.
3. **Unknown** - It is not known by the provider whether or not the individual has expressly consented to release of the attribute.

Date Consented
In addition to requiring information around whether the individual has consented to release of the attribute value, some RPs may wish to understand when that consent was received. Individual sentiments towards privacy and specific pieces of data may change over time. As a result, organizations may wish to employ the `date consented` metadata element when leveraging an attribute value in an access or eligibility decision.

Acceptable Uses
This explains to RPs what business cases the metadata can be used to support according to policy restrictions conveyed by the AP. For example, the attribute value might purely be useful in authorization, determining a user's eligibility for services; alternatively, values might be eligible for use beyond the initially intended purpose, or not eligible for any further disclosure. Additionally, organizations or trust frameworks might also create their own categories of acceptable uses based on their policies. Recommended values for this element include:

1. **Authorization** - The attribute value can be used to determine user eligibility for services or privileges and can be used to provide those services.
2. **Secondary Use** - The attribute value may be used for purposes beyond that for which they were initially divulged. Additional use requires separate, explicit consent from user at initiation.
3. **No Further Disclosure** - The attribute value should not be passed on to other parties for any purpose unless required by law.

Cache Time to Live
This metadata element describes the length of time which a specific attribute value may reside in cache memory for use again in future transactions. Due to the sensitivity of certain attributes values, this metadata element enables the parties involved to properly cache and handle the values they are sending and retrieving as part of their transactions. Unlike many of the other metadata elements in this schema,

the cache time to live enables attribute providers to express requirements to the RP around the protection of the information they are delivering as part of an assertion. In some cases the time to live may be dictated by regulation or law and this information needs to be relayed to RP systems so data are handled accordingly. The more sensitive an attribute value, the shorter time it will likely be enabled to live in temporary memory. As an example, the cache time to live for something like a credit card CVV may be just a couple of seconds, whereas the cache time to live for birth date may be substantially longer — potentially hours or days.

Data Deletion Date
This refers to long-term holding of attribute values. Minimizing data, and indicating the retention time for this data, is a generally accepted privacy tenant. Some attribute values produce little to no privacy risk for individuals, and can potentially be used forever without producing any negative consequences. Other values are more likely to produce problems for individuals; a deletion date ensures that this sensitive information is disposed of at a certain point.

3.2.1.5. Classification Metadata

Metadata Element	Description	Recommended Values
Classification	The U.S. Federal Government security classification level of the attribute	•Unclassified •Controlled Unclassified •Confidential •Secret •Top Secret
Releasability	The U.S. Federal Government restrictions regarding to whom an attribute value may be released	•NATO •FVEY •NOFORN •Public Release •None

Classification
Making certain attribute values available to RPs can carry national security implications. In situations where this may be the case, identification of such attribute values at the time of exchange can be absolutely crucial to ensuring that they are appropriately handled and protected across the attribute's lifecycle. The recommended values for use in this schema are:

1. **Unclassified** - Unclassified attribute values are those that carry with them no national security implications. This does not, however, indicate that they are not sensitive, not in need of specific protections, or available publicly.
2. **Controlled Unclassified** - These attribute values are not sensitive enough to have a negative impact on national security, but are none the less sensitive enough that they should be protected from improper access or exposure (e.g., FOUO information).
3. **Confidential** - Attribute values, which if subject to unauthorized disclosure, could be expected to cause damage to national security.
4. **Secret** - Attribute values, which if subject to unauthorized disclosure, could be expected to cause serious damage to national security.
5. **Top Secret** - Attribute values, which if subject to unauthorized disclosure could be expected to cause exceptionally grave damage to national security.
6. **Company Confidential** - Attribute values which, if released, may cause damage to the organization that produced, generated, or maintains the values and/or its employees. For example the professional title or specialization of a specific employee, if exposed, may inadvertently reveal information about a sensitive company project.

As with all classified information, the determination of the classification level for any attribute must be made by the appropriate U.S. Federal Government authority and the integrity of this classification must be maintained as the attribute and its values are transmitted or stored in by IT systems.

Releasability
Refers to restrictions that may be placed on the releaseability of an attribute's value. The recommended values for this element include:

1. **NATO** - The attribute's value is releasable to NATO allies only and should not be distributed to other foreign nationals.
2. **NOFORN** - The attribute's value is not releasable to any foreign nationals.
3. **FVEY** - The attribute's value is releasable to Five Eye nations only.
4. **Public Release** - The attribute's value is explicitly approved for public release.
5. **Externally Releasable for Business Purposes** - The attribute's value has been explicitly approved for release to parties externally, but for approved business purposes only. For example, this may be leveraged by an entity to approve the release or attribute values as part of a federated environment supporting their supply chain.
6. **Do Not Release** - The attribute's value has not been approved for release beyond the originating organization.
7. **None** - There are no distribution or release caveats associated with the attribute's value. This, however, does not mean that the attribute value may be freely distributed.

4. Use Cases

This section details three use cases as a means of demonstrating the ways in which attribute metadata and attribute value metadata can be leveraged to enrich authorization decisions, facilitate cross boundary interoperability and trust, and enable adoption of federated attributes. Each use case carries with it a set of authorization and privacy considerations as well as suggested metadata necessary to fulfill evaluation of the requisite authorization policy, as well as an example of what an attribute value metadata assertion may look like.

The use cases are:
1. Federated Access to Classified Documents in an Information Sharing Environment
2. Citizen Access to Federal Benefits
3. Law Enforcement Access to Intelligence Database

4.1. Federated Access to Classified Document in an Information Sharing Environment

Overview

Monique, an Army employee with a current TS-SCI clearance, attempts to access an information system that stores classified information, hosted on a shared Secure Internet Protocol Router Network (SIPRNet) site by the Air Force. Furthermore, the system, due to its sensitivity and the number of possible individuals that have legitimate need to access it, is protected by Attribute Based Access Control (ABAC). The ABAC evaluates access policy to enforce decisions based on attributes specific to the user and the resource (not addressed in the schema). When Monique attempts access to the resource, an attribute query is routed to her agency, the Army, to obtain the attributes needed to grant or deny access. The Army then asserts the requested set of attributes, which are evaluated against the access control policy of the Air Force hosted site so a decision can be made. While in an actual implementation there may be many different attributes required to access the protected resource, for the purposes of illustration, this use case will only focus on the clearance attribute. Furthermore, in this scenario it is assumed that the semantics and syntax associated with the attribute itself are established.

Attribute	**Value**
Clearance	TS-SCI

Authorization Considerations

In a traditional ABAC scenario, the assertion from the Army system would only provide the value that they maintain within their own records. As a result, the receiving agency's access control system is only able to make a decision based upon the asserted attribute value and nothing more— i.e., the employee's clearance is TS-SCI so therefore they are authorized for access. Information such as: how current the clearance is, when it was last verified by the asserting agency, and from where the value originated are not factored into the process. With the inclusion of attribute metadata, the relying agency is able to make an informed, risk-based decision by adding the evaluation of the attribute metadata into their ABAC policies. For example, they could determine that anyone accessing this specific resource must have a TS-SCI clearance that: originated from a DoD entity, has been verified in the last six months, and was verified by the providing entity against an authoritative database.

Authorization Policy
1. Origin MUST be an organization that is part of the Department of Defense
2. Verification of clearance MUST have been done in the last six months
3. Verification of clearance MUST have been done against an authoritative database

Through the establishment of attribute value metadata, these further considerations and requirements can be expressed in policy and compared to asserted information.

Privacy Consideration

In this scenario privacy considerations factoring into the selection of attribute value metadata are limited, the selected information is an absolute for access based on national security requirements and only the requested value and metadata are being returned to a trusted party as part of the assertion.

Suggested Attribute Value Metadata

Based on the scenario's authorization and privacy considerations, the table below illustrates the metadata that is applied to support appropriate authorization decisions by the relying agency. It also provides notional values.

Element	Value
Verifier	**Origin** - The clearance was verified by the originating entity—which in this case is the same as the provider
Verification Method	**Record Check** - The attribute value was verified against the sponsoring agency's clearance database
Last Verification	**6/10/16** (assume an access request date of 7/1/2016)
Origin	**United States Army**
Pedigree	**Authoritative** - The attribute's value was generated and in this case asserted as well by the authoritative source

XACML Example Policy

Attribute and metadata names, and valid values, are fictional. These will ultimately depend on the technologies of the attribute sources that is being queried to evaluate policy. URL's and namespaces, in some cases, have been removed for brevity.

```
  <xacml3:Policy Version="1.0" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-
combining-algorithm:deny-overrides" PolicyId="http://www.axiomatics.com/automatic-unique-
id/50f5b25e-dc7f-4672-a673-1a482e53f023">

    <xacml3:Description>Use Case #1</xacml3:Description>
    <xacml3:PolicyDefaults><xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-
19991116</xacml3:XPathVersion></xacml3:PolicyDefaults>
    <xacml3:Target/>
    <xacml3:Rule RuleId="c01d7519-be21-4985-88d8-10941f44590a" Effect="Permit">
      <xacml3:Description>isTSClearance</xacml3:Description>
      <xacml3:Target>
        <xacml3:AnyOf>
          <xacml3:AllOf>
            <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
              <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">TS-
SCI</xacml3:AttributeValue>
              <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.value" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </xacml3:Match>
          </xacml3:AllOf>
        </xacml3:AnyOf>
        <xacml3:AnyOf>
          <xacml3:AllOf>
```

```
            <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
              <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ORIGIN</xacml3:AttributeValue>
              <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.verifier" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </xacml3:Match>
          </xacml3:AllOf>
        </xacml3:AnyOf>
        <xacml3:AnyOf>
          <xacml3:AllOf>
            <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
              <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">authoritative</xacml3:AttributeValue>
              <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.pedigree" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </xacml3:Match>
          </xacml3:AllOf>
        </xacml3:AnyOf>
        <xacml3:AnyOf>
          <xacml3:AllOf>
            <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
              <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">records check</xacml3:AttributeValue>
              <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.verification_method" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
            </xacml3:Match>
          </xacml3:AllOf>
        </xacml3:AnyOf>
      </xacml3:Target>
    </xacml3:Rule>
  <xacml3:Rule RuleId="4bae1384-729b-4e3e-895e-ea8dfefe5704" Effect="Permit">
    <xacml3:Description>isOriginDOD</xacml3:Description>
    <xacml3:Target>
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">DOD</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ARMY</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
        <xacml3:AllOf>
```

```
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">NAVY</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">MARINES</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">AIR
FORCE</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">USCG</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
    </xacml3:Target>
  </xacml3:Rule>
  <xacml3:Rule RuleId="a17ecf55-77c0-4ddc-ab81-fcff342bcf7f" Effect="Permit">
    <xacml3:Description>verificationDateWithinYear</xacml3:Description>
    <xacml3:Target/>
      <xacml3:Condition xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
        <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than">
          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
            <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment" AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
          </xacml3:Apply>
          <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:dateTime-add-
yearMonthDuration">
            <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
              <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:1.0:subject-
category:access-subject" AttributeId="clearance.last_verification" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
            </xacml3:Apply>
```

```
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#yearMonthDuration">P6M</xacml3:AttributeValue>
          </xacml3:Apply>
        </xacml3:Apply>
      </xacml3:Condition>
    </xacml3:Rule>

  </xacml3:Policy>
```

4.2. Citizen Access to Federal Benefits

Overview

Jane is a veteran and she is in the process of establishing an online account to manage her Veterans Affairs educational benefits. The VA system leverages a federated identity model that is integrated with multiple trusted IDPs, which offer high assurance credentials and identity attributes. Furthermore, the VA system leverages the asserted attributes to both populate the online registration form and to make an initial eligibility determination when establishing an account. When Jane initiates the registration process she is notified by her IDP which attributes are being asserted to the VA, for what they are going to be used, and what type of metadata is being provided. Failure to enroll via the online process (if, for example the attribute value metadata is not within policy) triggers a backup offline verification process conducted by the VA.

Attribute	Value
Veteran	Yes

Authorization Considerations

For this transaction, the VA has identified the attribute *Veteran Status* as critical to making an initial authorization decision. Though the VA is likely to have an existing record for Jane, it may not be easily accessible to the application. To ease the process of online enrollment for the service the VA has determined and external assertion of veteran status is sufficient to open an account if the following policy is met:

Authorization Policy
1. Veteran status must have been verified by the provider or the originating authority
2. Veteran status must have been verified through document verification and against an authoritative database
3. The Veteran must have consented to the release of their status

Privacy Considerations

In this use case, some metadata elements with privacy implications, such as `provider`, are necessary for the transaction. Since this must be included, it's important to ensure that Jane is aware of the fact that her information is being transferred as metadata in transactions. By gaining express consent from Jane before releasing her veteran status (as required by the authorization policy), Jane is notified of the transfer of this attribute value, and she gives her permission for the transfer. Other metadata elements with privacy implications, such as `origin`, are not needed in this transaction, technically or policy-wise. Thus, they should be excluded since they're not necessary and their inclusion would potentially reveal a broad profile of Jane (e.g., related to her associations with certain organizations).

Suggested Attribute Value Metadata

Based on the scenario's authorization and privacy considerations, the table below illustrates the attribute value metadata that is applied to support appropriate decisions by the VA system. It also provides notional values.

Element	Value
Verifier	**Provider** - The clearance was verified by the IDP (also acting as the AP in this instance)
Verification Method	**Document verification with Record Check** - The attribute value was verified against a DD-214 provided by Jane and was checked against a National Archives and Records Administration database
Individual Consented	**Yes -** The provider gained Jane's consent before releasing veteran status or any other attribute values

XACML Example Policy

Attribute and metadata names, and valid values, are fictional. These will ultimately depend on the technologies of the attribute sources that is being queried to evaluate policy. URI's and namespaces, in some cases, have been removed for brevity.

```
<xacml3:Policy Version="1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-overrides" PolicyId="9458137c-535b-4f2e-9907-2e8c7d5881ad">
  <xacml3:Description>Use Case #2</xacml3:Description>
  <xacml3:PolicyDefaults>
    <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:XPathVersion>
  </xacml3:PolicyDefaults>
  <xacml3:Target/>
  <xacml3:Rule RuleId="35e6f270-5504-4596-9786-431d7de04402" Effect="Permit">
    <xacml3:Description>isVeteran</xacml3:Description>
    <xacml3:Target>
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#boolean">true</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="UC2" AttributeId="veteran.value"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#boolean">true</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="UC2"
AttributeId="veteran.individual_consented" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">PROVIDER</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="UC2" AttributeId="veteran.verifier"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
```

```
        </xacml3:AllOf>
      </xacml3:AnyOf>
      <xacml3:AnyOf>
        <xacml3:AllOf>
          <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
            <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">&gt;Document Verification with Record
Verification</xacml3:AttributeValue>
            <xacml3:AttributeDesignator Category="UC2"
AttributeId="veteran.verification_method" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </xacml3:Match>
        </xacml3:AllOf>
      </xacml3:AnyOf>
    </xacml3:Target>
  </xacml3:Rule>

</xacml3:Policy>
```

4.3. Law Enforcement Access to an Intelligence Database

Overview

Claude is with the Los Angeles Police Department (LAPD) and is attempting to access an FBI criminal justice database in order to gather additional information for a high-profile case. This database uses a federated identity model with multiple IDPs across affiliated law enforcement agencies. Due to the sensitive information retained within the database, access is protected based by ABAC. The attributes are asserted by the appropriate law enforcement agency (in this case the LAPD) to the FBI, who is then able to evaluate the attributes and make an access decision.

Attribute	Value
Sworn Law Enforcement Officer	Yes
CJIS Privacy Training	Yes

Authorization Considerations

We assume in this example that the access request was sent on 7/1/16. The FBI allows access to this database based around two major requirements. The first requirement is that Claude must be a Sworn Law Enforcement Officer (LEO), verified at least quarterly in order to prevent granting access to retired users. The second requirement is that the Claude must have completed CJIS Privacy Training. Verification of the completion of this training must be done within 12 months.

Authorization Policy
1. Origin MUST be FBI or an affiliated law enforcement agency
2. User MUST be a Sworn Law Enforcement Officer with status validated within the last quarter (3 months)
3. CJIS Privacy Training MUST have been completed within the last 12 months

Privacy Consideration

In this use case, certain metadata elements are necessary to demonstrate compliance with access requirements for this database. However, excessive metadata collection that extends beyond these requirements could unnecessarily reveal information about law enforcement officials accessing the

system. For example, provider metadata is not necessary for this transaction, and could reveal unintended information about Claude by divulging his relationship with the provider organization. Other metadata elements (e.g., origin) are necessary, but might still have privacy implications for Claude by revealing information about him. In these instances, it's important to—when possible—ensure that Claude is aware of which information is being transferred.

Suggested Attribute Value Metadata

Based on the scenario's authorization and privacy considerations, the table below illustrates the metadata that is applied to support appropriate authorization decisions by the FBI. It also provides notional values.

Element	Value
Verifier	**Origin** - The statuses and verification dates for both Sworn LEO and CJIS Privacy Training would be verified by the originating entity (LAPD)
Last Verification (Sworn LEO)	**6/15/16**
Last Verification (CJIS Privacy Training)	**6/1/15**
Origin (both)	**Los Angeles Police Department**
Pedigree (both)	**Authoritative** - The attribute's value was generated and in this case asserted as well by the authoritative source.

Based on information about the user sent to the FBI by the LAPD IDP, the user is a Sworn LEO and has been verified as such within the last month (6/15/16). The user has also completed CJIS Privacy Training. However, the last verified date for the CJIS Privacy Training value was 13 months ago (6/1/15). In accordance with policy and based on interrogation of attribute value metadata, Claude is denied access based on the amount of time since the value for CJIS Privacy Training was verified. Here, the FBI has maintained its policy that simply taking the CJIS Privacy Training is not enough; it must have also been completed and verified within the last year as well. Similar to the "Federated Access to Classified Document in an Information Sharing Environment" example, the inclusion of attribute value metadata allows for more informed and fine grained access control decisions than in a traditional ABAC instance.

XACML Example Policy

Attribute and metadata names, and valid values, are fictional. These will ultimately depend on the technologies of the attribute sources that is being queried to evaluate policy. URI's and namespaces, in some cases, have been removed for brevity.

```
<xacml3:Policy Version="1" RuleCombiningAlgId="urn:oasis:names:tc:xacml:3.0:rule-combining-
algorithm:deny-overrides" PolicyId="72537098-66a9-4283-8790-9c567eb2be1d">
  <xacml3:Description>Use Case #3</xacml3:Description>
  <xacml3:PolicyDefaults>
    <xacml3:XPathVersion>http://www.w3.org/TR/1999/REC-xpath-19991116</xacml3:XPathVersion>
  </xacml3:PolicyDefaults><xacml3:Target/><xacml3:Rule RuleId="1db3d77b-7467-42d3-82cc-
0ae61facdad4" Effect="Permit">
  <xacml3:Description>isSLEO</xacml3:Description>
  <xacml3:Target>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#boolean">true</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3" AttributeId="sleo.value"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
        </xacml3:Match>
      </xacml3:AllOf>
```

```
    </xacml3:AnyOf>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ORIGIN</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3" AttributeId="sleo.verifier"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">LAPD</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3" AttributeId="sleo.origin"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">AUTHORITATIVE</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3" AttributeId="sleo.pedigree"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
  </xacml3:Target>
  <xacml3:Condition xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
    <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than">
      <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-only">
        <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment" AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
      </xacml3:Apply>
      <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:dateTime-add-
yearMonthDuration">
        <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
          <xacml3:AttributeDesignator Category="UC3" AttributeId="sleo.last_verification"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
        </xacml3:Apply>
        <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#yearMonthDuration">P3M</xacml3:AttributeValue>
      </xacml3:Apply>
    </xacml3:Apply>
  </xacml3:Condition>
</xacml3:Rule>
<xacml3:Rule RuleId="0ef722ee-1b81-4c4b-98fa-34fbc5f17ea3" Effect="Permit">
  <xacml3:Description>isPrivTrained</xacml3:Description>
  <xacml3:Target>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:boolean-equal">
```

```
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#boolean">true</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3" AttributeId="cjis_privacy_training.value"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#boolean"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ORIGIN</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3"
AttributeId="cjis_privacy_training.verifier" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">LAPD</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3"
AttributeId="cjis_privacy_training.origin" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:3.0:function:string-equal-ignore-
case">
          <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">AUTHORITATIVE</xacml3:AttributeValue>
          <xacml3:AttributeDesignator Category="UC3"
AttributeId="cjis_privacy_training.pedigree" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
  </xacml3:Target>
  <xacml3:Condition xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17">
    <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-less-than">
      <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-only">
        <xacml3:AttributeDesignator Category="urn:oasis:names:tc:xacml:3.0:attribute-
category:environment" AttributeId="urn:oasis:names:tc:xacml:1.0:environment:current-dateTime"
MustBePresent="false" DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
      </xacml3:Apply>
      <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:3.0:function:dateTime-add-
yearMonthDuration">
        <xacml3:Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:dateTime-one-and-
only">
          <xacml3:AttributeDesignator Category="UC3"
AttributeId="cjis_privacy_training.last_verification" MustBePresent="false"
DataType="http://www.w3.org/2001/XMLSchema#dateTime"/>
        </xacml3:Apply>
        <xacml3:AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#yearMonthDuration">P1Y</xacml3:AttributeValue>
```

```
      </xacml3:Apply>
    </xacml3:Apply>
  </xacml3:Condition>
</xacml3:Rule>

</xacml3:Policy>
```

5. References

[FICAM Roadmap] Federal Identity Credential and Access Management (FICAM) Roadmap and Implementation Guidance, December 2, 2011. Available at: https://www.idmanagement.gov/IDM/servlet/fileField?entityId=ka0t0000000TNNBAA4&field=File__Body__s

[FICAM Attribute Management Roadmap] FICAM Attribute Management Roadmap, April 30, 2015.]

[SP 800-162] NIST Special Publication 800-162, Guide to Attribute Based Access Control Definition and Considerations, January, 2014, available at: http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp.800-162.pdf

[SP 800-63-3] DRAFT NIST Special Publication 800-63-3, Digital Authentication Guideline, May, 2016, available at: https://pages.nist.gov/800-63-3

[OIX Attribute Exchange Trust Framework] The Open Identity Exchange, Attribute Exchange Trust Framework Specification: Technical Specification V1. July 02, 2013. Available at: http://openidentityexchange.org/wp-content/uploads/2014/06/OIX-AXN-Trust-Framework-Specification-1.0-7-5-2013.pdf

[OMB A-130] OMB Circular A-130, Management of Federal Information Resources, November, 28 2000, available at: https://www.whitehouse.gov/omb/circulars_a130_a130trans4/