Open GIS Consortium Inc.

Date: 2003-06-27

Reference number of this OpenGIS© Project Document: **OGC 03-062r1**

Version: 0.3.1

Category: OpenGIS© OGC Interoperability Program Report –Viewpoint Specification

Editor: Richard Martell (Galdos Systems, Inc.)

Critical Infrastructure Collaborative Environment Architecture: Information Viewpoint

Copyright notice

Warning

This document is not an OGC Standard or Specification. This document presents a discussion of technology issues considered in an Interoperability Initiative of the OGC Interoperability Program. The content of this document is presented to create discussion in the geospatial information industry on this topic; the content of this document is not to be considered an adopted specification of any kind. This document does not represent the official position of the OGC nor of the OGC Technical Committee. It is subject to change without notice and may not be referred to as an OGC Standard or Specification. However, the discussions in this document could very well lead to the definition of an OGC Implementation Specification.

Recipients of this document are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Document type: OpenGIS© Draft Interoperability Program Report –Viewpoint Specification
Document subtype: OGC Critical Infrastructure Protection Initiative (CIPI)
Document stage: Draft
Document language: English

Contents

i. Preface

The OpenGIS Consortium (OGC) is an international industry consortium of more than 220 companies, government agencies, and universities participating in a consensus process to develop publicly available geo-processing specifications. This Interoperability Program Report (IPR) is a product of the OGC Critical Infrastructure Protection Initiative (CIPI), the objective of which is to provide a vendor-neutral interoperable framework that enables the publication, discovery, and use of geospatial information concerned with the protection of critical infrastructure systems in a range of sectors.

The OGC Critical Infrastructure Protection Initiative is part of the OGC's Interoperability Program: a global, collaborative, hands-on engineering and testing program designed to deliver prototype technologies and proven candidate specifications into the OGC's Specification Development Program. In OGC Interoperability Initiatives, international teams of technology providers work together to solve specific geo-processing interoperability problems posed by Initiative sponsors.

ii. Document Contributor Contact Points

All questions regarding this document should be directed to the editor or the contributors:

Chuck Heazel
OpenGIS Consortium
cheazel@opengis.com

Richard Martell (editor)
Galdos Systems, Inc.
rmartell@galdosinc.com

iii. Revision history

Date	Release	Description
2003-01-16	0.0.1	▪ Template populated with the preliminary table of contents;
2003-01-22	0.0.2	▪ Refined scope (clause 1); ▪ Updated TOC.
2003-03-05	0.1.0	▪ Added access control framework
2003-03-10	0.1.1	▪ Overlaid with RFQ Annex B info. ▪ Moved X.812 and X.509 details to Annex A. Consider moving to Technical viewpoint.

Date	Release	Description
2003-04-02	0.2.0	▪ Added content dealing with authentication (8.1.1 plus Annex B); ▪ Added more terms to Clause 4; ▪ Reorganized Clause 8.1 (Security functions) in accord with 10746-3.
2003-05-19	0.3.0	▪ Revised with new document number.
2003-06-27	0.3.1	▪ Incorporated comments from Jeff Harrison.

Critical Infrastructure Collaborative Environment (CICE) – Information Viewpoint Specification

1. Introduction

ISO RM-ODP (ISO/IEC 10746) is the architectural framework adopted by the OGC for specifying its reference architectures. The four main parts of the standard define viewpoints on open distributed processing (ODP) systems. This specification addresses the information viewpoint for a system dedicated to the protection of critical infrastructure components—it is concerned with the kinds of information handled by the system and constraints on the use and interpretation of that information.

1.1 Scope

This draft Interoperability Program Report (DIPR) specifies the information viewpoint for the Critical Infrastructure Collaborative Environment (CICE). This open, distributed processing environment crosses organizational boundaries and includes a variety of components deployed within multiple communities. The CICE leverages OGC Web Services to enable:

- the publication of the availability of critical infrastructure services and data;
- the registration and categorization of published service and data providers; and
- the discovery and use of needed critical infrastructure services and data

Critical infrastructure is a very broad term that encompasses many large-scale systems in a range of sectors: energy, telecommunications, transportation, public health services, and more. Safeguarding such systems involves a welter of political, economic, and legal issues that will not be raised here. Rather, the CICE is more about the creation and maintenance of a *common information space* to support sense-making and decision-making activities on the part of incident response teams.

1.2 Conformance

Assessing conformance requires consistency across the various viewpoints (i.e. clear mappings of concepts) and across the models they define. In general, the set of viewpoint specifications should not make mutually contradictory statements. Furthermore, each specification should include correspondence statements that relate it to other viewpoints.

1.2.1 Viewpoint correspondences

*** TO DO**

1.2.2 Reference points

A reference point identifies a behaviour or proposition that must be satisfied at a particular interaction point. A reference point may be declared as a conformance test point used to test observed behaviour. Part two of the RM-ODP standard distinguished four categories of reference points: programmatic, perceptual, interworking, and interchange (not all need be used in every viewpoint specification).

1.3 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this Interoperability Program Report. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this document are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies.

ISO/IEC 10746-2:1996, *Information Technology – Open Distributed Processing –Reference Model: Foundations*.

ISO/IEC 10746-3:1996, *Information Technology – Open Distributed Processing –Reference Model: Architecture.*

ITU-T Recommendation X.509 (2000). *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*. Common text with ISO/IEC 9594-8:2001.

1.4 Terms and definitions

For the purposes of this Interoperability Program Report, the terms and definitions given in ISO 10746-2, ISO 10746-3, and ITU-T Rec. X.509 apply. For convenience, some of these terms are repeated below.

1.4.1 Attribute certificate

A data structure, digitally signed by an Attribute Authority, that binds some attribute values with identification information about its holder. [X.509]

1.4.2 Critical infrastructure

Elements of a system that are so vital that disabling any of them would incapacitate the entire system. [T1.253]

1.4.3 Policy

A set of obligation, prohibition, or permission rules that either constrain or enable actions, as related to a purpose. [ISO 10746-2]

1.4.4 Public-key certificate

The public key of a user, together with some other information, rendered unforgeable by encipherment with the private key of the certification authority which issued it. [X.509]

1.4.5 Security domain

A domain in which the members are obliged to follow a security policy established and administered by a security authority. [ISO 10746-3]

1.5 Conventions

1.5.1 Symbols and abbreviated terms

The following symbols and abbreviated terms are used in this document.

API	Application Programming Interface
CI	Critical infrastructure
OGC	OpenGIS Consortium
XML	Extensible Markup Language

1.5.2 Requirement levels

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2 Framework Data

2.1 Establishing the geographic context

The first step in any CIPI scenario is to establish the geographic context of the event(s). CIPI-1 will support this need through data interchange standards for geographic information which are supported by a number of existing data providers. Some of the resources leveraged will include available aspects of the U.S. National Spatial Data Infrastructure (NSDI) Framework Data and Canadian Geospatial Data Infrastructure (CGDI) framework data. The National Spatial Data Infrastructure (NSDI) for the United States include the following 7 GIS Framework layers identified by the Federal Geographic Data Committee (FGDC):

- Orthophotography
- Cadastral
- Transportation
- Geodetic Control
- Elevation
- Hydrography
- Governmental Units

2.1.1 The Foundation: Geography

Underlying the geographic information model is the concept of geometry. A Geometry Model provides a way of expressing the real-world location characteristics of an object. By using a common geometry model, it is possible to combine data from a number of different sources into a single spatial context. Relevant specifications for the CIPI-1 geometry model are:

- ISO 19107 – ISO Geometry Model
- GML 2.0 - OGC Geography Markup Language version 2.1
- GML 3.0 – OGC Geography Markup Language version 3.0

2.1.2 Vector Data: Geospatial features

Vector data are the classes of data that represents geospatial features. This data combines the geometry of a geospatial feature with descriptive information (attributes) that describe that feature. As such, vector data is well suite for data processing applications. Vector data does not contain display information. Rendering and display of vector data is the responsibility of the application or portrayal service. Relevant specifications for CIPI-1 Vector data are:

- GML 2.0 OGC Geography Markup Language version 2.1
- GML 3.0 – OGC Geography Markup Language version 3.0 (draft)

GML is a markup language that is used to encode both spatial and non-spatial geographic information. By building on broader Internet standards from the World Wide Web Consortium (W3C), GML is used to express geographic information in a manner that can be

readily shared on the Internet. GML is not the first meta-language used to describe geographic information, but it is the first to be widely accepted within the GIS community. Other formats have been developed as a means to store and exchange spatial and temporal geographic information, however supporting tools to validate and reference the information were often not available. One of the advantages of using GML is that it enables one to leverage the whole world of XML technologies. In particular, GML builds on eXtensible Markup Language (XML), XML Schema, XLink, and XPointer). GML data can also be easily mixed with non-spatial data.

One of the primary objectives of GML is to provide a language for expressing geographic objects in a manner that is shareable over the Internet. GML provides a set of core schema components (e.g. features, geometry, topology, temporal, etc) together with a simple semantic model between objects and properties that is similar to Entity-Relationship diagrams or the class/property model of RDF (Resource Description Framework). Using the GML model and its schema components, users can describe the geographic types, whether concrete or conceptual, that are used within their application domain. The set of objects is created in the form of one or more GML Application Schemas, that is XML Schemas that make use of the GML schema components, and which comply with the GML semantic model and syntactic rules. A key benefit of GML is that the application schemas can be published and shared over the Internet, something that would be critical to any regional, national or international information infrastructure. "

The following GML Application Schemas are currently defined for representing U.S. NSDI Framework Data:

- TIGER/GML
- Transportation (Under Development)

2.1.3 Gridded Data

Gridded data are the classes of data items that contain a matrix of values representing measured phenomenon. A collection of elevation points, for example, is a common form of gridded data. In addition, a Gridded data set may contain information on where and when the data was collected as well as supporting data describing the conditions when it was collected.

2.1.3.1 Gridded Data: Raster

Raster data are the classes of gridded data items that represent a picture. This data consists of a single layer of pixels that can be readily visualized by a user. Relevant specifications for CIPI-1 Raster data are:

- JPEG –*ISO/IEC 11544*
- PNG – Portable Network Graphics W3C Recommendation version 1.0
- TIFF – Tagged Image File Format version 6.0

2.1.3.2 Gridded Data: Imagery

Imagery data are the classes of gridded data items that represent one or more pictures (bands) and the associated metadata. This data differs from Raster Data in its complexity. An Imagery data set may consist of one or more Raster data sets often taken using different parts of the electromagnetic spectrum. In addition, imagery data sets contain information on where and when the image was collected as well as supporting data describing the conditions when it was collected. Relevant specifications for CIPI-1 Imagery data are:

- NITF – National Imagery Transmission Format v 2.1 MIL-STD-2500A
- GeoTIFF – Geographic Tagged Image Format

2.1.3.3 Gridded Data: Elevation

Elevation data are the classes of gridded data items that represent discrete elevation points (lat, long, and elevation). Relevant specifications for CIPI-1 elevation data are:

- DEM – Digital Elevation Models
- DTED – Digital Terrain Elevation Data MIL-PRF-89020B

2.2 Sectoral models

TBD

2.3 Representing dynamic situations

Once the geographic context has been established it is necessary to be able to track dynamic events and to exchange information in real-time.

2.3.1 Annotations

Annotations are a special case of Vector Data. Like Vector data, they represent individual features containing both geometry and attributes. Unlike Vector data, however, they do not usually describe a geospatial feature. Rather, attribute features are used to provide additional information about another geospatial data element. Attribute data only has meaning when evaluated in conjunction with the data element that is being described. Relevant specifications for CIPI-1 Annotation data are:

- XIMA – XML for Imagery and Map Annotations (OGC discussion paper)

2.3.2 Web Map Context

A Web Map Context document includes information about the server(s) providing layer(s) in the overall map, the bounding box and map projection shared by all the maps, sufficient operational metadata for Client software to reproduce the map, and ancillary metadata used to annotate or describe the maps and their provenance for the benefit of human viewers.

- Web Map Context (OGC Implentation Specification)

3 Accessing and displaying information: Management and Control Data

3.1 Query Languages

All of the services used in the CICE have a queryable interface. To use those interfaces, it is necessary that the client and server have a common understanding of what constitutes a valid query. Standardized query languages provide the common vocabulary and grammar needed to enable this sliver of interoperability. Relevant specifications for CIPI-1 Query Languages are:

- OGC Filter Encoding Language – Filter Encoding Specification (OGC discussion paper)

3.2 Styling Description Languages

The Web Map Service provides users with the ability to customize the symbolization of the data they are requesting. In order to work across all WMS implementations, there must be a standard way of expressing the desired symbolization. Standardized Styling Description Languages address that need. Relevant specifications for CIPI-1 Styling Description Languages are:

- SLD – Style Layered Description Specification (OGC Implementation Specification)

3.3 Symbology

How geospatial data is interpreted is very much dependent on the background and training of the user. Users of military systems, for example, use a very different representational scheme than land use planners. Symbology data is that data that captures the representational symbology that is appropriate for a work context. The association of symbology data elements with a geospatial feature allows the use to apply the appropriate symbology to geospatial data regardless of the source.

- MIL-STD-2525 – Common Warfighting Symbology

- NIMA GeoSym and FGDC Homeland Security Working Group (HSWG) Emergency Mapping Symbology Matrix

3.4 Resource discovery

3.4.1 Service Description Languages

The CICE supports the concept of service publication, discovery, and binding. To enable this capability, there must be a common language for publishing the information necessary for a potential client to assess the suitability of a service and to understand how to bind to it. Service Description Languages provide a standard way of expressing that information. Relevant specifications for CIPI-1 Service Description Languages are:

- SIM – Service Information Model
- WSDL – Web Service Definition Language version 1.1(W3C Note)

3.4.2 Data Description Languages

The CICE supports the concept of data publication and retrieval. To enable this capability, there must be a common language for publishing the information necessary for a potential client to assess the suitability of a data item or provider and to understand how to access it. Standardized Data Description Languages provide a standard way of expressing that information. Relevant specifications for CIPI-1 Data Description Languages are:

- FGDC – Federal Geographic Data Committee discovery metadata standard.

4 Quality of Service characteristics

4.1 Security functions

A number of common security functions are described in ISO 10746-3:

- *Authentication* — assuring the claimed identity of an entity;
- *Access control* — preventing unauthorized interactions with an object;
- *Confidentiality* — preventing the unauthorized disclosure of information;
- *Integrity* — detecting and/or preventing the unauthorized creation, alteration, or deletion of data;
- *Non-repudiation* — preventing an object that participated in an interaction from denying its involvement in all or part of the interaction;
- *Auditing* — monitoring and collecting information about security-related actions;
- *Key management* — providing facilities for the management of cyptographic keys.

Not all of these functions are implicated in CIPI work items. Authentication and access control functions have been the subject of testbed implementations.

4.1.1 Authentication

The X.811 standard describes a general framework for providing authentication services that verify the claimed identity of a principal. The following definitions are introduced:

- **Authentication**: The provision of assurance of the claimed identity of an entity.
- **Authentication information** (AI): Information used for authentication purposes.
- **Distinguishing identifier**: Data that unambiguously distinguishes an entity in the authentication process. This Recommendation | International Standard requires that such an identifier be unambiguous at least within a security domain.
- **Principal**: An entity whose identity can be authenticated.

Principals include many kinds of entities, including human agents, software agents, and enterprises. A principal has one or more distinguishing identifiers associated with it, and these can reflect different degrees of granularity (e.g. group memberships, or a unique identifier such as a network address). In some cases distinguishing identifiers may have to be used in conjunction with an identifier of the security domain in order to unambiguously identify the principal.

The fundamental information flows are depicted in Figure 1. A *trusted third party* is a security authority that is trusted by a claimant and/or verifier to perform various security-related functions. Exchange authentication information passes between a claimant and a verifier (exchange AI); claim authentication information is used by a claimant to generate exchange AI; verification information is used to verify a claimed identity. An authentication exchange is a sequence involving one or more transfers of exchange AI.

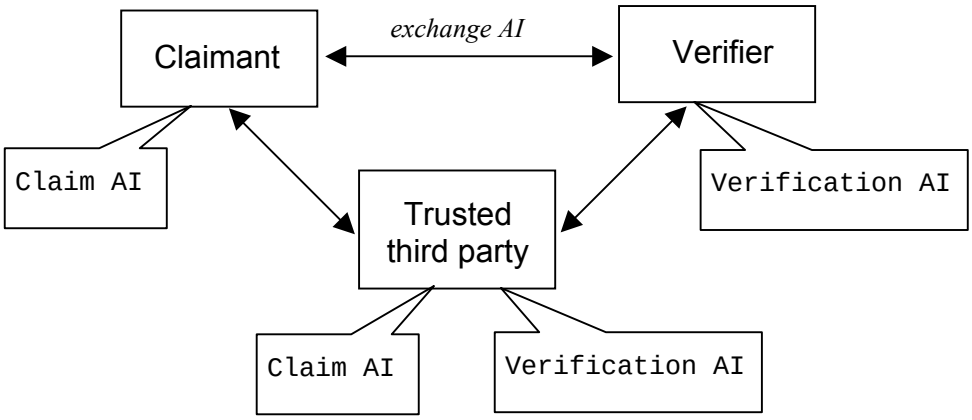

Figure 1: Fundamental information flows in the X.811 framework

Authentication can be unilateral or mutual, depending on whether only one or both principals are authenticated in an exchange. Different authentication methods will realize the framework shown in Figure 1 according to the mechanisms they employ. For example, client certificates used within a PKI enable a strong form of remote authentication where the role of trusted third party is fulfilled by a Certificate Authority (CA). The CA certifies a public key by issuing a public-key certificate (PKC) which binds the public-key to the entity which holds the corresponding private-key; authentication is then generally accomplished through the exchange of challenges and signed challenges that serve to verify the identity of the claimant.

CIPI web services exchange messages using the HTTP application protocol. There are several authentication methods in common use for HTTP traffic (see Annex B). For CIPI services, certificate-based authentication using Public Key Certificates is mandatory (see 8.1.4). Other methods may also be supported, however (e.g. HTTP Basic, Kerberos).

4.1.2 Access control

The X.812 standard [X.812] describes a general access control framework that encompasses several fundamental access control functions. The following definitions are introduced:

- **Access Control Decision Information** (ADI): The portion (possibly all) of the ACI made available to the ADF in making a particular access control decision.
- **Access control policy**: The set of rules that define the conditions under which an access may take place.
- **Access Control Decision Function** (ADF): A specialized function that makes access control decisions by applying access control policy rules to an access request, ADI (of initiators, targets, access requests, or that retained from prior decisions), and the context in which the access request is made.
- **Access Control Enforcement Function** (AEF): A specialized function that is part of the access path between an initiator and a target on each access request and enforces the decision made by the ADF.

The following excerpt from clause 5.2.1 summarizes the kinds of information required to render an access control decision.

> In order to perform this decision, the ADF is provided with the access request (as part of the decision request) and the following types of Access Control Decision Information (ADI):
>
> – initiator ADI (ADI derived from the ACI bound to the initiator);
> – target ADI (ADI derived from the ACI bound to the target);
> – access request ADI (ADI derived from the ACI bound to the access request).

The fundamental access control functions are shown in Figure 2. Other inputs include the access control policies defined by some security domain authority, and contextual information (e.g. time of access). A common scenario realizes an *incoming access control* capability, where an AEF component enforces an access control policy and the target cannot receive a request that violates the policy for the target. This means that if the ADF component renders an authorization decision that denies access, the AEF must block the request.

The OASIS XACML specification [XACML] uses terminology that differs slightly from the X.812 standard. A Policy Enforcement Point (PEP) corresponds to an AEF in X.812; a Policy Decision Point (PDP) corresponds to an ADF. The XACML terms will be favored here.

The various access decision inputs are conveyed as indicated below; examples of each appear in Annex A.

- Access Request ADI is represented by an XACML Request context that is generated by the PEP.
- access control policies are expressed using the XACML grammar; such policies may define target resources at varying levels of granularity (e.g. a service endpoint, a particular record)

Initiator ADI is provided through a X.509 Privilege Management Infrastructure (PMI) that employs Attribute Certificates (AC) to bind privilege attributes to a subject; the ACs are accessible via LDAP v3 [RFC3377].

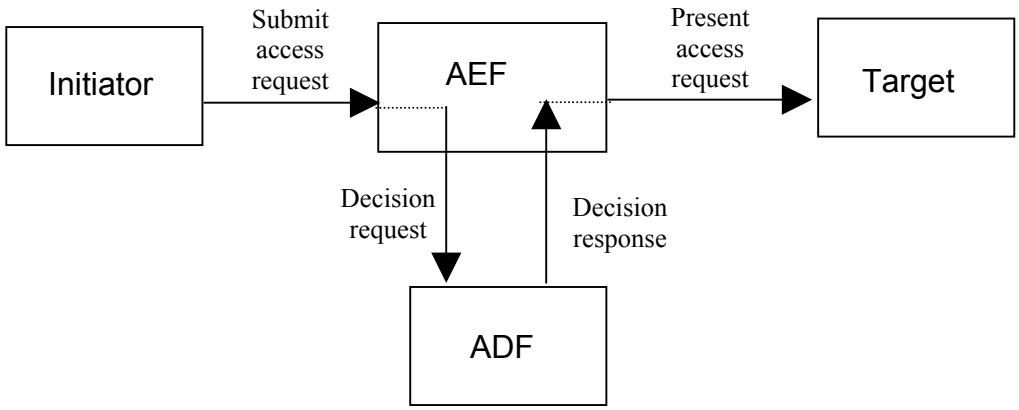

Figure 2: Fundamental access control functions in the X.812 framework

Security Credentials are the metadata that captures the security roles and authorizations that a user has been granted. Traditionally this information has been included in the public key certificate. Certificates, however, have limited capability to carry this information. To address this limitation, Security Profile Servers are being investigated as an alternative source for Security Credential. Under this approach, a service would first authenticate the user through the public key certificate, then using that certificate, retrieve the users credentials from a Security Profile Server. The development of a common representation of those credentials is one of the CIPI work items. Candidate specifications for CIPI-1 Security Profile Information are:

- X.509 Attribute Certificates

To implement a security policy it is necessary to know who is making the request, what their credentials are, and what restrictions have been placed on the resource being accessed. The public key certificate and the Security Profile data address the first two of these questions. Security Attributes address the third. Since access control takes place behind the interface, public specifications are not needed to enable interoperability. In the CICE, however, there will be a need to standardize on some security policies. A representation of resource security attributes is useful for the construction of implementable security policies. Relevant specifications for CIPI-1 Security Attributes are:

- X.812 / OASIS XACML (see Annex A)
- XML-ISM – IC Metadata Standards for Information Assurance (IC-MSIA) Information Security Markings

4.1.3 Key management

Authentication and Identification within the CICE will be performed using a public key infrastructure. Central to a public key infrastructure is the certificate. A certificate is an encrypted data item (document) that contains information about the user requesting access. The nature of the encryption is such that only one person should have been able to perform it. If the user identified in the certificate is the same as the only person who could have preformed the encryption, then the user is authenticated. This assumes that the authenticating system can read the certificate. Standards for certificates address this issue. The relevant specification for public key certificates is ITU-T Recommendation X.509 [X.509].

The basic components deployed in support of the DoD PKI systems are:

- Certificate Authority (CA) Server(s)
- Directory Server

Interfaces to the DoD PKI system are:

- Registration Authority (RA)
- Local Registration Authority (LRA)
- DoD employee's Internet browser residing on their local computer (End User)

In general, personal certificates serve two purposes:

- They make the End-User's public key available for others to use to send encrypted messages to the End-User.
- They certify the identity of End-Users when they send messages to others or interact with other applications.

Netscape browsers and servers use certificates when communicating through the Secure Socket Layer (SSL) protocol. The server proves its identity to the browser by sending the browser its certificate. Certificates can be used to replace multiple passwords for authentication so that users need only remember a single password that accesses their private key. They can also be used to send secure e-mail so that a message can be signed to verify the identity of the person who sent it. The message can include the signer's certificate, which the recipient can use to verify the digital signature. This verification insures that others have not altered the message. Secure e-mail can also be encrypted so that it cannot be read by anyone during transit.

Certificates are issued by a Certificate Authority (CA). The Local Registration Authority (LRA) delivers requests for certificates to the CA. An LRA is established by a Registration Authority (RA) to allow for the remote registration of users. It is the responsibility of the LRA to verify the identity of users and that users understand liabilities and responsibilities associated with possession of a private key and agree to abide by the established rules.

Failure of users to abide by the established rules can result in the revocation of their certificates by the RA.

Rules are as follows:

- Protect these instructions until the registration process is complete.
- Use certificate and private key for OFFICIAL USE ONLY.
- Comply with guidelines for selecting a strong password as stated in the registration process (use at least eight (8) characters, letters & numbers, NO dictionary words, meaning words not found in the dictionary).
- Protect your password and private key and do not allow others to use them.
- Report the compromise of these instructions and/or your password/private key to your LRA.

A user may be either a human or component (software). When the user is a software component an individual will be responsible for the operation of the component. It is the responsibility of this individual to request appropriate certificates from the LRA and ensure that PKI policies regarding the certificates are abided by.

Annex A
(normative)

Access decision information

Access request ADI

In the XACML specification a *Context* is the canonical representation of a decision request and the resulting authorization decision. The request context is constructed by the PEP component and submitted to some PDP within its security domain; there are no restrictions concerning how these components are distributed: they could be co-located on the same node, or the PDP could be implemented as a stand-alone authorization service for a site or security domain.

Information is gleaned from an access request in order to generate an XACML request context; this includes details such as the identity of the subject, the access time, the target resource, and the action to be performed. Listing 1 provides an example generated from a WRS `getRecord` request. In this case the target resource is the service instance as a whole identified by its endpoint. Subject information is extracted from a client certificate provided as part of the SSL/TLS handshaking process; a variety of credentials may be examined, depending on the authentication mechanism being employed (e.g. a username/password pair for BASIC authentication). The action attribute indicates the name of the operation that is being invoked (i.e. getRecord).

Listing 1: Sample XACML context request

```
<?xml version="1.0" encoding="UTF-8"?>
<Request xmlns="urn:oasis:names:tc:xacml:1.0:context">
<Subject
  SubjectCategory="urn:oasis:names:tc:xacml:1.0:subject-category:access-
subject">
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:request-
time"
    DataType="http://www.w3.org/2001/XMLSchema#dateTime">
    <AttributeValue>2003-03-04T11:25:35-08:00</AttributeValue>
  </Attribute>
  <Attribute
    AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-qualifier"
    DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name">
    <AttributeValue>
    CN=JITC DoD PKI Class 3 ID CA,OU=PKI,OU=DoD,O=U.S. Government,C=US
    </AttributeValue>
  </Attribute>
  <Attribute
    AttributeId="urn:oasis:names:tc:xacml:1.0:subject:authentication-
method"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>CLIENT-CERT</AttributeValue>
```

```
  </Attribute>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id"
    DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name">
    <AttributeValue>
    CN=Fogg.Phineas.3010001450,OU=CONTRACTOR,OU=PKI,OU=DoD,O=U.S.
Government,C=US
    </AttributeValue>
  </Attribute>
</Subject>
<Resource>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-
id"
    DataType="http://www.w3.org/2001/XMLSchema#anyURI">

<AttributeValue>https://www.secure.acme.com/registry/wrs</AttributeValue>
  </Attribute>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:resource:scope"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>Descendants</AttributeValue>
  </Attribute>
</Resource>
<Action>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
namespace"
    DataType="http://www.w3.org/2001/XMLSchema#anyURI">
    <AttributeValue>http://www.opengis.net/wrs</AttributeValue>
  </Attribute>
  <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:action:implied-
action"
    DataType="http://www.w3.org/2001/XMLSchema#string">
    <AttributeValue>getRecord</AttributeValue>
  </Attribute>
</Action>
</Request>
```

Listing 2 is an example of a positive response issued by the PDP after evaluating a context request in light of applicable policies. A context response returns one or more <Result> elements that includes one of the following decision values: “Permit”, “Deny”, “NotApplicable” or “Indeterminate”. If the decision is anything other than “Permit”, then the PEP *must* deny access to the resource and block the initial request.

Listing 2: sample XACML context response

```
<?xml version="1.0" encoding="UTF-8"?>
<Response xmlns="urn:oasis:names:tc:xacml:1.0:context">
  <Result ResourceId="https://www.secure.acme.com/registry/wrs">
    <Decision>Permit</Decision>
    <Status>
      <StatusCode Value="urn:oasis:names:tc:xacml:1.0:status:ok" />
    </Status>
  </Result>
</Response>
```

Access control policies

The XACML specification defines a policy model that is encoded using XML Schema. A policy has four main components:

- a target;
- a rule-combining algorithm identifier;
- a set of rules;
- obligations.

Listing 3 is an example of a simple global policy set that requires all subjects accessing a registry service to be identified by the JITC Class 3 Certificate Authority (the CIPI-1 CA). The referenced ancillary policy specifies a number of rules that apply to all WRS requests submitted to a particular registry endpoint (i.e. the target resource is identifed as "https://www.secure.acme.com/registry/wrs" (Listing 4).

Listing 3: A global XACML policy set

```
<?xml version="1.0" encoding="UTF-8"?>
<PolicySet xmlns="urn:oasis:names:tc:xacml:1.0:policy"
  PolicySetId="urn:galdosinc:cipi-1:policySet:1"
  PolicyCombiningAlgId="urn:oasis:names:tc:xacml:1.0:policy-combining-
algorithm:deny-overrides">

  <Description>This policy set governs the CIPI-1 WRS
policies</Description>
  <Target>
    <Subjects>
      <Subject>
        <SubjectMatch
MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue
            DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name">
            CN=JITC DoD PKI Class 3 ID CA,OU=PKI,OU=DoD,O=U.S.
Government,C=US
          </AttributeValue>
          <SubjectAttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id-
qualifier"
            DataType="urn:oasis:names:tc:xacml:1.0:data-type:x500Name"/>
        </SubjectMatch>
      </Subject>
    </Subjects>
    <Resources>
      <AnyResource/>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>
  <!-- Include cipi-1 related rules policy -->
  <PolicyIdReference>urn:galdosinc:cipi-1:policy:1</PolicyIdReference>

</PolicySet>
```

Listing 4 includes the policy referenced in the global policy set. The following two rules are asserted by this policy:

- ACP-1.1: All subjects who access the secure registry must belong to the “cipi-1” group;
- ACP-1.2: Subjects assigned to the “Media” role cannot perform any transaction operations (i.e. transaction or registerResource). They can perform any query operation.

Listing 4: A simple rule-based policy

```
<?xml version="1.0" encoding="UTF-8"?>
<Policy xmlns="urn:oasis:names:tc:xacml:1.0:policy"
  PolicyId="urn:galdosinc:cipi-1:policy:1"
  RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-
algorithm:deny-overrides">

  <Description>Authorization requirements cipi-1 participants</Description>
  <!-- Policy applies to all requests -->
  <Target>
    <Subjects>
      <AnySubject/>
    </Subjects>
    <Resources>
      <Resource>
        <ResourceMatch
          MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
          <AttributeValue
DataType=“http://www.w3.org/2001/XMLSchema#anyURI”>
          https://www.secure.acme.com/registry/wrs
          </AttributeValue>
          <ResourceAttributeDesignator
            AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id"
            DataType=“http://www.w3.org/2001/XMLSchema#anyURI”/>
        </ResourceMatch>
      </Resource>
    </Resources>
    <Actions>
      <AnyAction/>
    </Actions>
  </Target>

  <!-- All users must be from the cipi-1 group -->
  <Rule RuleId="urn:opengis:cipi:security:policy:rule:acp-1.1"
Effect="Permit">
    <Description>
    Only subjects in the cipi-1 group can access the registry
    </Description>
    <!-- Who the rule applies to -->
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType=“http://www.w3.org/2001/XMLSchema#string”>
```

```
            cipi-1
            </AttributeValue>
            <SubjectAttributeDesignator AttributeId="group.values"
              DataType="http://www.w3.org/2001/XMLSchema#string"/>
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <AnyAction/>
      </Actions>
    </Target>
  </Rule>

  <!-- Media subjects can perform read operations only -->
  <Rule RuleId="urn:opengis:cipi:security:policy:rule:acp-1.2"
Effect="Deny">
    <Description>
    Subjects from the role.roleNamed "Media" cannot perform write
operations. All other roleNames can perform all operations.
    </Description>
    <!-- Who does the rule apply to -->
    <Target>
      <Subjects>
        <Subject>
          <SubjectMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">
            Media
            </AttributeValue>
            <SubjectAttributeDesignator AttributeId="role.roleName"
              DataType="http://www.w3.org/2001/XMLSchema#string" />
          </SubjectMatch>
        </Subject>
      </Subjects>
      <Resources>
        <AnyResource/>
      </Resources>
      <Actions>
        <Action>
          <ActionMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#anyURI" >
            http://www.opengis.net/wrs
            </AttributeValue>
            <ActionAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-
namespace"
              DataType="http://www.w3.org/2001/XMLSchema#anyURI" />
          </ActionMatch>
          <ActionMatch
            MatchId="urn:oasis:names:tc:xacml:1.0:function:regexp-string-
```

```
match">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string" >
              registerResource|transaction
            </AttributeValue>
            <ActionAttributeDesignator
              AttributeId="urn:oasis:names:tc:xacml:1.0:action:implied-
action"
              DataType="http://www.w3.org/2001/XMLSchema#string" />
          </ActionMatch>
        </Action>
      </Actions>
    </Target>
  </Rule>
</Policy>
```

The PDP component receives a context request, looks up any additional Initiator ADI if needed (see clause 10.1.2.4), and then consults a policy store to fetch relevant access control policies; with these ADI resources in hand, an authorization decision is rendered and a context response is returned to the PEP.

Attribute Certificates

The latest revision of the X.509 standard (also published as ISO 9594-8) deals with both public-key certificate frameworks and attribute certificate frameworks. The two security frameworks reflect a basic division of labor: the Privilege Management Infrastructure (PMI) deals with authorization concerns, and the Public Key Infrastructure (PKI) focuses on authentication issues.

The two frameworks traffic in different credentials: a Public Key Certificate (PKC) binds a subject to a public key for the purpose of authentication; an Attribute Certificate (AC) binds shorter-lived privilege attributes to a subject for authorization purposes (e.g. role/group memberships, security clearances). A simple analogy has been drawn in RFC 3281: think of a PKC as a passport, and an AC as a visa.

The RFC 3281 specification [RFC3281] defines an Internet profile for the use of X.509 Attribute Certificates. It provides a common baseline for applications requiring broad interoperability. The essential AC exchanges are illustrated in Figure 3. The X.509 standard defines an AC using ASN.1 notation; this is partially reproduced in Listing 5.

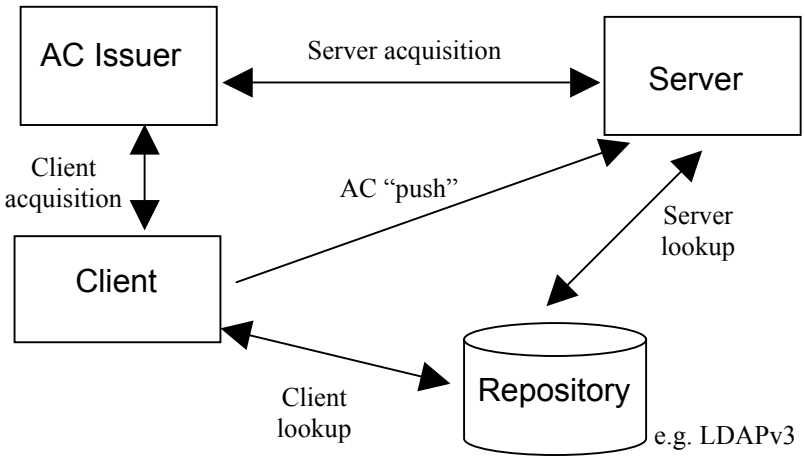

Figure 3: Abstract view of AC exchanges (RFC 3281)

Listing 5: Partial ASN.1 definition of an Attribute Certificate (X.509)

```
AttributeCertificate ::= SEQUENCE {
     acinfo                 AttributeCertificateInfo,
     signatureAlgorithm     AlgorithmIdentifier,
     signatureValue         BIT STRING
}

AttributeCertificateInfo ::= SEQUENCE {
     version                AttCertVersion -- version is v2,
     holder                 Holder,
     issuer                 AttCertIssuer,
     signature              AlgorithmIdentifier,
     serialNumber           CertificateSerialNumber,
     attrCertValidityPeriod AttCertValidityPeriod,
     attributes             SEQUENCE OF Attribute,
     issuerUniqueID         UniqueIdentifier OPTIONAL,
     extensions             Extensions OPTIONAL
}
```

The attributes field gives information about the AC holder. When the AC is used for authorization, this field will generally contain a set of privileges to support various access control policies. The following attributes are defined in section 4.4 of RFC 3281:

- `id-aca-authenticationInfo` – identifies the AC holder to the service by a name; it may include optional service specific authentication information (e.g. a username/password pair).
- `id-aca-accessIdentity` – identifies the AC holder to the server/service.
- `id-aca-chargingIdentity` – identifies the AC holder for charging purposes.
- `id-aca-group` – carries information about group memberships of the AC holder.

- `id-at-role` – carries information about roles assigned to the AC holder.
- `id-at-clearance` – carries clearance information (associated with security labelling) about the AC holder.

Attribute Certificates can be conveniently stored in LDAP directories maintained by some security domain administrator; they are exchanged in their DER-encoded form using the LDAP protocol. In Figure 2, a PDP component may assume the “Server” role and contact the subject's home directory in order to fetch available ACs. The ACs then provide additional information used to evaluate an access decision request.

Annex B
(informative)

Common HTTP/1.1 authentication mechanisms

RFC 2617 outlines the Basic and Digest authentication mechanisms.

[insert summary]

HTTP connections may also make use of TLS (Transport Layer Security—it is derived from SSL v3 developed by Netscape Communications) to provide channel-oriented security. As a higher level protocol, HTTP can be layered transparently on top of TLS in order to confer privacy and data integrity between two communicating applications [RFC2246]. The TLS Handshake Protocol allows the server and client to authenticate each other and to negotiate cryptographic parameters; while such authentication is optional, it is typically required for one—or both—peers. The use of an X.509 Public Key Infrastructure (PKI) is the basis of this authentication.

The TLS handshake protocol is summarized in section 7.3 of RFC 2246, but for convenience the basic message exchanges are presented below

[sketch of TLS handshake]

Bibliography

[T1.523] ANSI Standard T1.253-2001. *Telecom Glossary 2000*. Available [online]: <http://www.atis.org/tg2k/>.

[RFC2119] IETF/RFC 2119. *Key words for use in RFCs to Indicate Requirement Levels*. March 1997. Available [online]: <http://www.ietf.org/rfc/rfc2119.txt>.

[RFC2246] IETF/RFC 2246. *The TLS Protocol Version 1.0*. Available [online]: <http://www.ietf.org/rfc/rfc2246.txt>.

[RFC2617] IETF/RFC 2617. *HTTP Authentication: Basic and Digest Access Authentication*. Available [online]: <http://www.ietf.org/rfc/rfc2617.txt>

[RFC2828] IETF/RFC 2828. *Internet Security Glossary*. May 2000. Available [online]: <http://www.ietf.org/rfc/rfc2828.txt>.

[RFC3281] IETF/RFC 3281. *An Internet Attribute Certificate Profile for Authorization*. April 2002. Available [online]: <http://www.ietf.org/rfc/rfc3281.txt>.

[RFC3377] IETF/RFC 3377. *Lightweight Directory Access Protocol (v3): Technical Specification*. September 2002. Available [online]: <http://www.ietf.org/rfc/rfc3377.txt>.

[X.509] ITU-T Recommendation X.509(2000). *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*. Common text with ISO/IEC 9594-8:2001.

[X.811] ITU-T Recommendation X.811(1995). *Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Authentication Framework*. Common text with ISO/IEC 10181-2:1996.

[X.812] ITU-T Recommendation X.812(1995). *Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework*. Common text with ISO/IEC 10181-3:1996.

[XACML] *eXtensible Access Control Markup Language (XACML) Version 1.0*. OASIS Standard, 18 February 2003. Available [online]: <http://www.oasis-open.org/committees/xacml/repository/oasis-xacml-1.0.pdf>