The Printer Working Group

November 1, 2014
Working Draft

Imaging Device Security
Identification, Authentication and Authorization
(IDS-IAA)

Status: Initial

Abstract: This standard defines a set of requirements, methods, and data models for defining and sharing security identification, authentication and authorization information between various imaging services, devices and users.

This document is a PWG Working Draft. For a definition of a "PWG Working Draft", see: ftp://ftp.pwg.org/pub/pwg/general/pwg-process30.pdf

This document is available electronically at:

ftp://ftp.pwg.org/pub/pwg/ids/wd/wd-ids-iaa10-20140804.pdf

Title: *IDS Identification, Authentication and Authorization (IDS-IAA)*

About the IEEE-ISTO

The IEEE-ISTO is a not-for-profit corporation offering industry groups an innovative and flexible operational forum and support services. The IEEE-ISTO provides a forum not only to develop standards, but also to facilitate activities that support the implementation and acceptance of standards in the marketplace. The organization is affiliated with the IEEE (http://www.ieee.org/) and the IEEE Standards Association (http://standards.ieee.org/).

For additional information regarding the IEEE-ISTO and its industry programs visit:

http://www.ieee-isto.org

About the IEEE-ISTO PWG

The Printer Working Group (or PWG) is a Program of the IEEE Industry Standards and Technology Organization (ISTO) with member organizations including printer manufacturers, print server developers, operating system providers, network operating systems providers, network connectivity vendors, and print management application developers. The group is chartered to make printers and the applications and operating systems supporting them work together better. All references to the PWG in this document implicitly mean “The Printer Working Group, a Program of the IEEE ISTO.” In order to meet this objective, the PWG will document the results of their work as open standards that define print related protocols, interfaces, procedures and conventions. Printer manufacturers and vendors of printer related software will benefit from the interoperability provided by voluntary conformance to these standards.

In general, a PWG standard is a specification that is stable, well understood, and is technically competent, has multiple, independent and interoperable implementations with substantial operational experience, and enjoys significant public support.

For additional information regarding the Printer Working Group visit:

http://www.pwg.org

Contact information:

The Printer Working Group
c/o The IEEE Industry Standards and Technology Organization
445 Hoes Lane
Piscataway, NJ 08854
USA

About the Imaging Device Security Work Group (IDS)

Description of PROJECT NAME.

For additional information regarding IDS visit:

http://www.pwg.org/ids/

Implementers of this specification are encouraged to join the IDS mailing list in order to participate in any discussions of the specification. Suggested additions, changes, or clarification to this specification, should be sent to the IDS Mailing list for consideration.

Table of Contents

List of Figures

List of Tables

No table of figures entries found.

1. Introduction

Provide an introduction for the document.

2. Terminology

2.1 Conformance Terminology

Capitalized terms, such as MUST, MUST NOT, RECOMMENDED, REQUIRED, SHOULD, SHOULD NOT, MAY, and OPTIONAL, have special meaning relating to conformance as defined in Key words for use in RFCs to Indicate Requirement Levels [RFC2119]. The term CONDITIONALLY REQUIRED is additionally defined for a conformance requirement that applies to a particular capability or feature.

2.2 Other Terminology

2.3 Acronyms and Organizations

GPS: Global Positioning System

IANA: Internet Assigned Numbers Authority, http://www.iana.org/

IETF: Internet Engineering Task Force, http://www.ietf.org/

ISO: International Organization for Standardization, http://www.iso.org/

PWG: Printer Working Group, http://www.pwg.org/

3. Requirements

3.1 Rationale for IDS Identification, Authentication and Authorization

Given the need for a standard method of defining, describing, and enforcing security for Imaging Devices, the Imaging Device Security Identification, Authentication and Authorization specification should:

1. Define new IDS Security Model element attributes and values to support identification of Users, Imaging Devices, Jobs, and Documents.
2. Define new IDS Security Model element attributes and values to support authentication of Users and Services.
3. Define new IDS Security Model element attributes and values to support Access Control for Users, Services, Imaging Devices, Jobs, Designated Resources and Documents.

3.2 Use Cases

Add reference to the Model spec.

3.3 Out of Scope

The following are considered out of scope for this specification:

1. Definition of new security encryption protocols
2. Definition of new authentication methods
3. Definition of new security policy definition languages and formats

3.4 Design Requirements

The design requirements for this specification are:

1. Expand the IDS Security Model with new attributes and standard values to support identification of Users, Devices, Imaging Devices, Service, Jobs, and Documents
2. Expand the IDS Security Model with new attributes and standard values to support delegated resource access
3. Define example policies based on existing printing and imaging service specifications
4. Define attributes and values for authentication, authorization, and access control using existing protocols and schema.
5. Provide the ability for vendors to add extensions to the IAA values and attributes

6.

4. Security Elements

The IDS Identification, Authentication and Authorization specification defines core security attributes and values for three Imaging security areas: Identification, Authentication and Authorization. The IDS security attributes and values are assigned to one or more Security Actors (as defined in the IDS Security Model) and carried in a PWG Security Ticket.

4.1 Identification

4.1.1 User Identification

The User Identification elements provide information to identify the User that is performing an operation.

4.1.2 Client Identification

The Client Identification elements provide identification information on any client processes or application that are being used in performing an operation.

4.1.3 Device Identification

The Device Identification elements identify the device that are used by a User or Client while performing an operation.

4.1.4 Service Identification

Service Identification elements are used to identify the service that is performing an operation.

4.2 Authentication

4.3 Authorization

5. Common Security Ticket Elements

The following sets of security elements are common to all security actors and collections.

5.1 Authentication

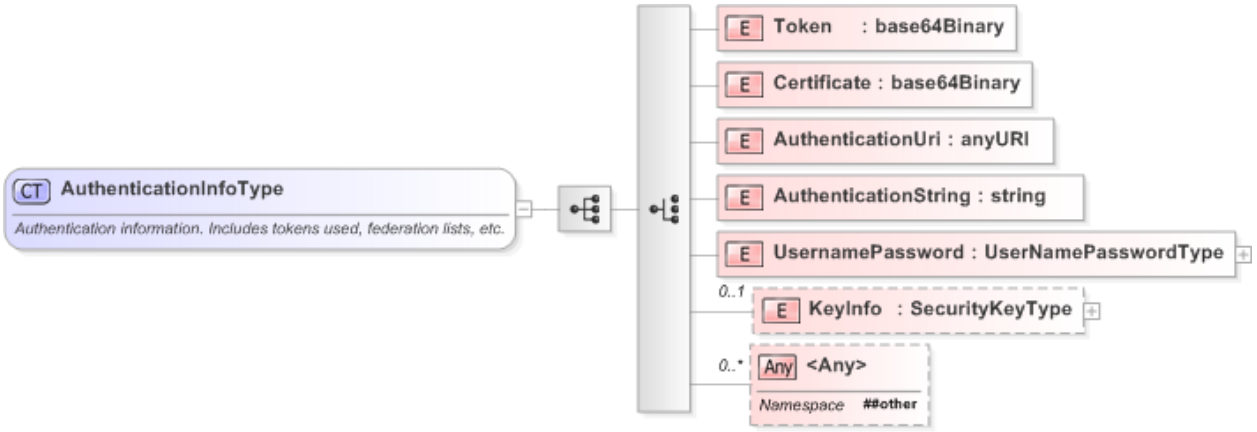


Figure 1: AuthenticationInfo Type

5.1.1 Token

5.1.2 Certificate

5.1.3 AuthenticationUri

5.1.4 AuthenticationString

5.1.5 UsernamePassword

5.1.6 KeyInfo

6. Security Elements

6.1 UserSecurity

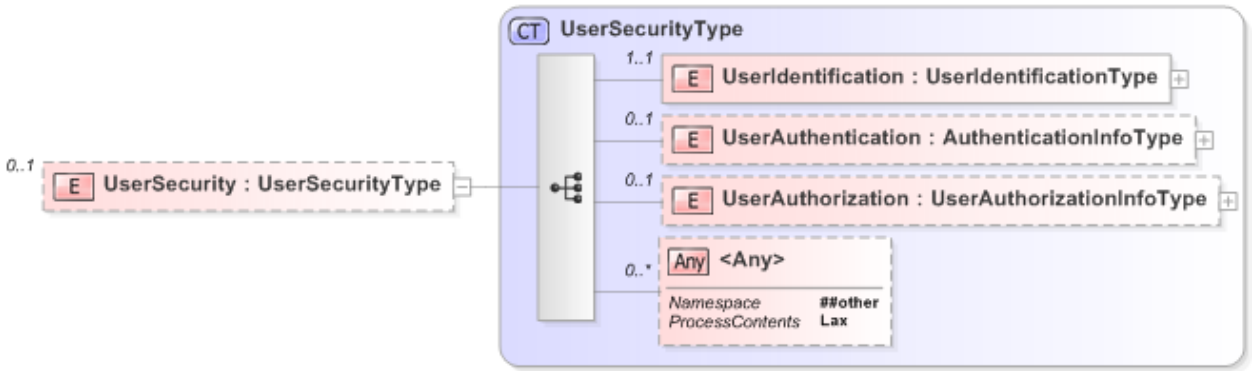


Figure 2: User Security Elements

6.1.1 UserIdentification

The UserIdentification element contains the attributes necessary for identifying an User.

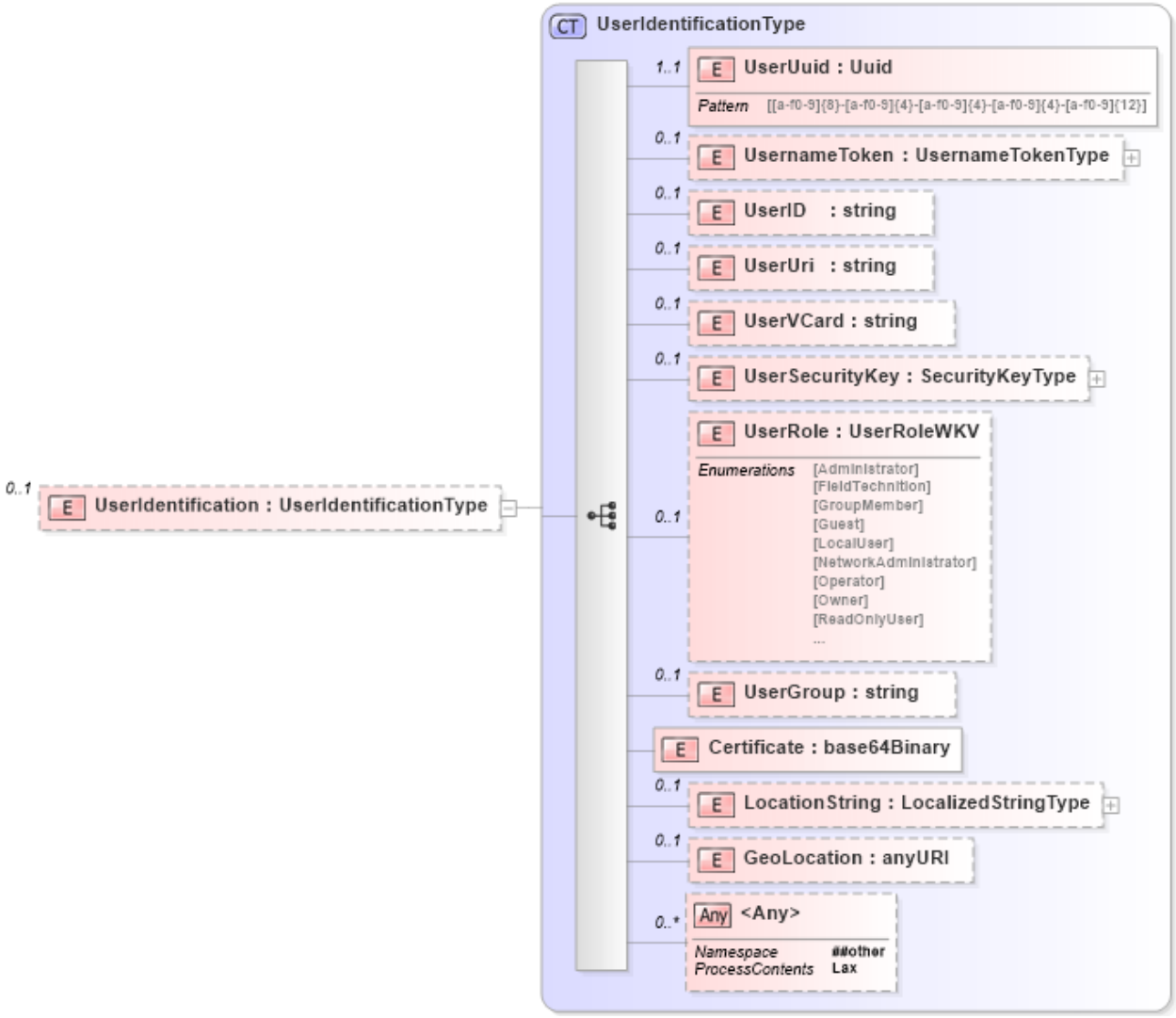


Figure 3: User Identification

6.1.1.1 UserUuid

A UUID value to uniquely identify the User. If a UUID is provided, it's value should be retained for the duration of any operation associated with the SecurityTicket

6.1.1.2 UsernameToken

The system Username associated with the User. This is typically the account name for the User

6.1.1.3 UserId

A system identification value assigned to the User account. This may be an account ID or a user name

6.1.1.4 UserUri

A Uri value that identifies the User, such as an Email address

6.1.1.5 UserVCard

A VCard record that identifies the user.

6.1.1.6 UserSecurityKey

A binary key, such as an OAuth or Active Directory Access token or Kerberos Ticket that can be used to identify a User

6.1.1.7 UserRole

The User's role in an organization or within a system.

6.1.1.8 UserGroup

The organizational groups to which the User belongs

6.1.1.9 Certificate

An X509 Certificate that identifies the User

6.1.1.10 LocationString

The LocationString element is a localized human-readable string describing the current location of the user. This may be an abstract location value such as "In my car"

6.1.1.11 GeoLocation

The Geolocation element represents the GPS coordinates of the current physical location of the user. Generally this location will also refer to the location of the device the User is actually using.

The coordinates MUST be expressed as specified in "A Uniform Resource Identifier for Geographic Locations ('geo' URI)" [RFC5870].

6.1.2 UserAuthentication

6.1.3 UserAuthorization

Figure 4: User Authorization

6.2 Device Security

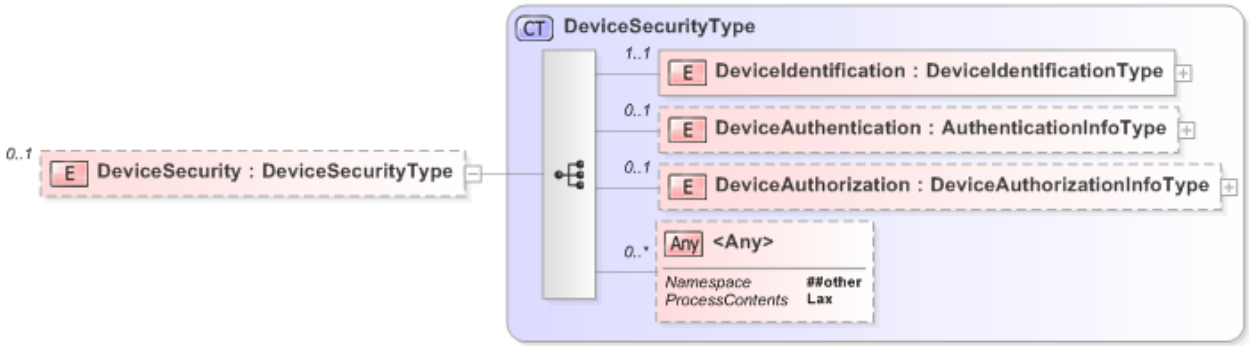


Figure 5: Device Security Elements

6.2.1 DeviceIdentification

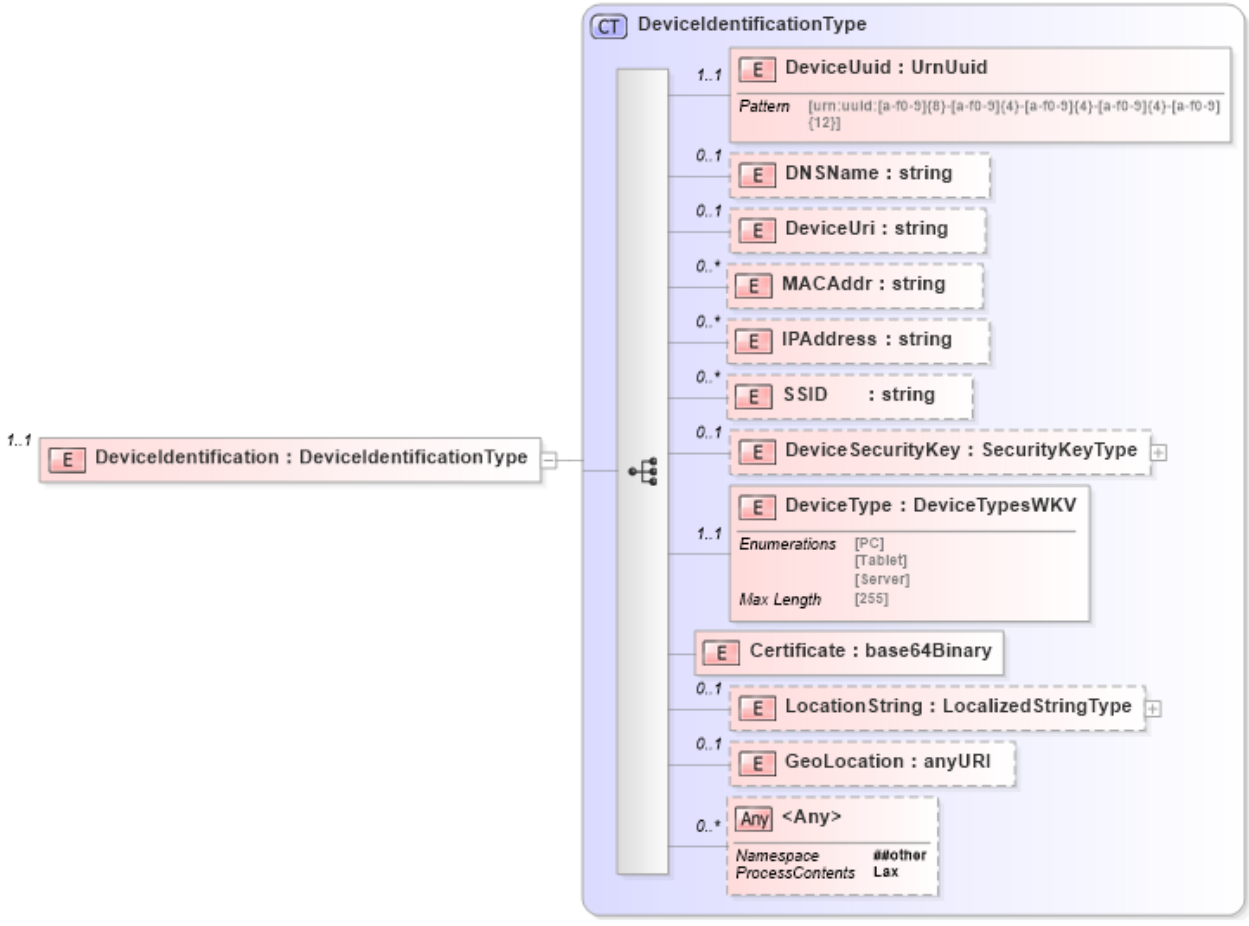


Figure 6: Device Identification

The DeviceIdentification element contains the attributes necessary for identifying a Device.

6.2.1.1 DeviceUuid

A UUID value to uniquely identify the User. If a UUID is provided, the value MUST be retained for as long as the Device is powered up. The value SHOULD be retained for the lifetime of the Device.

6.2.1.2 DNSName

The registered DNS name of the Device

6.2.1.3 DeviceUrl

A Uri value that identifies the Device,

6.2.1.4 MACAddr

The Media Access Control (MAC) hardware addresses of the Device, one element for each network interface

6.2.1.5 IPAddr

The IP Addresses of the Device, one element for each network interface

6.2.1.6 DeviceSecurityKey

A binary key, such as an X.509 Certificate or OAuth token that can be used to identify a Device

6.2.1.7 DeviceType

A value identifying the type of the device

6.2.1.8 Certificate

An X509 Certificate that identifies the Device

6.2.1.9 LocationString

The LocationString element is a localized human-readable string describing the physical location of the hardware device.

6.2.1.10 GeoLocation

The Geolocation element represents the GPS coordinates of the physical location of the hardware device. The coordinates MUST be expressed as specified in RFC5870 [RFC5870].

6.2.2 DeviceAuthentication

6.2.3 DeviceAuthorization

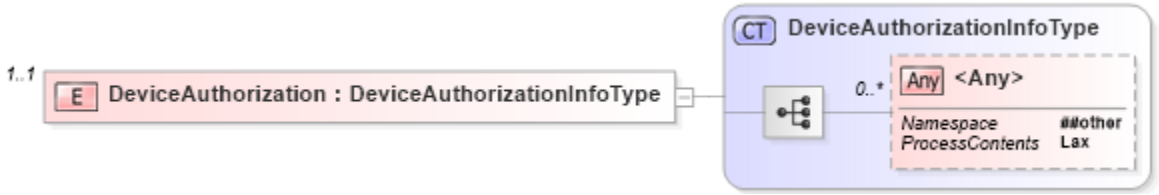


Figure 7: Device Authorization

6.3 Client Security

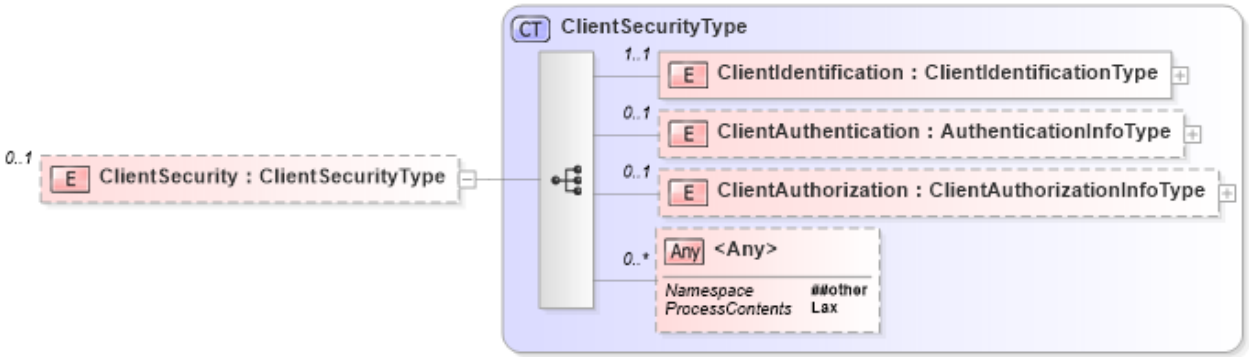


Figure 8: Client Security Elements

6.3.1 ClientIdentification

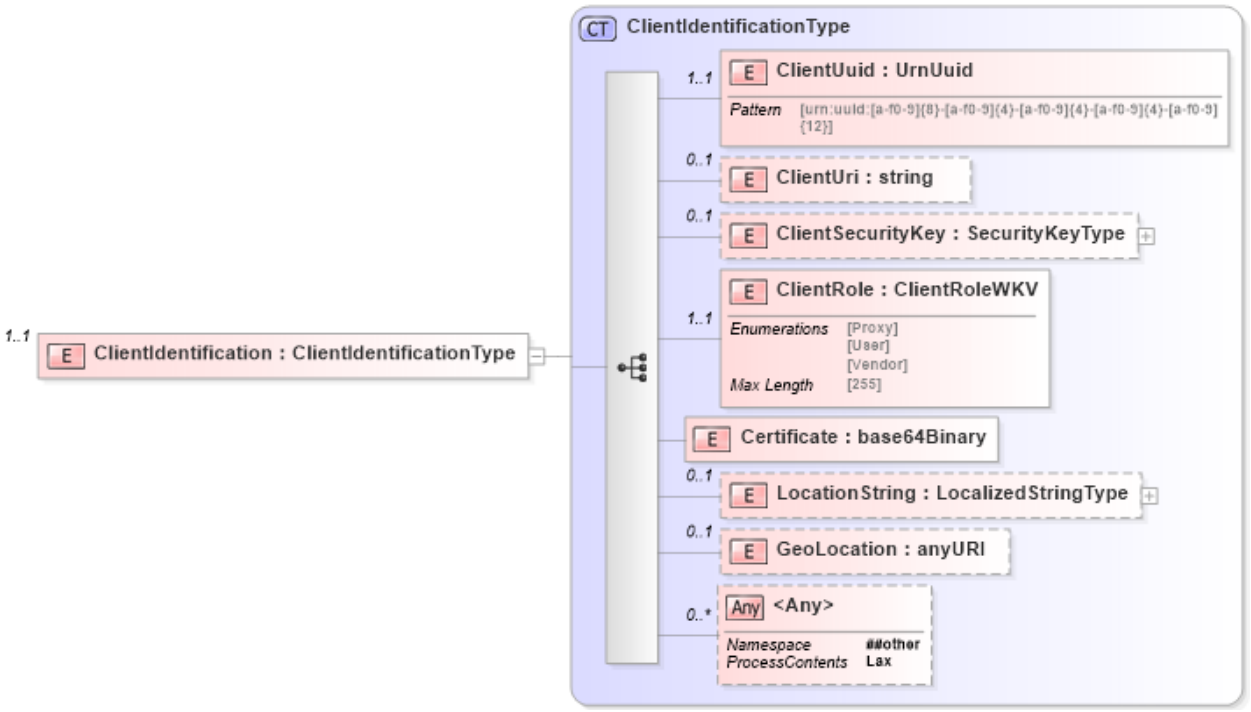


Figure 9: Client Identification

The ClientIdentification element contains the attributes necessary for identifying a Client.

6.3.1.1 ClientUuid

A UUID value to uniquely identify the User. If a UUID is provided, the value MUST be retained for the lifespan of the Client process or application.

6.3.1.2 ClientUri

A Uri value that identifies the Client process or application.

6.3.1.3 ClientSecurityKey

A binary key, such as an X.509 Certificate or OAuth token that can be used to identify a Client process or application.

6.3.1.4 ClientRole

The role of the Client process

6.3.1.5 Certificate

An X509 Certificate that identifies the Client

6.3.1.6 LocationString

The LocationString element is a localized human-readable string describing the physical location of the hardware running service instance.

6.3.1.7 GeoLocation

The Geolocation element represents the GPS coordinates of the physical location of the hardware running service instance. The coordinates MUST be expressed as specified in RFC5870 [RFC5870].

6.3.2 ClientAuthentication

6.3.3 ClientAuthorization

Figure 10: Client Authorization

6.4 Service Security

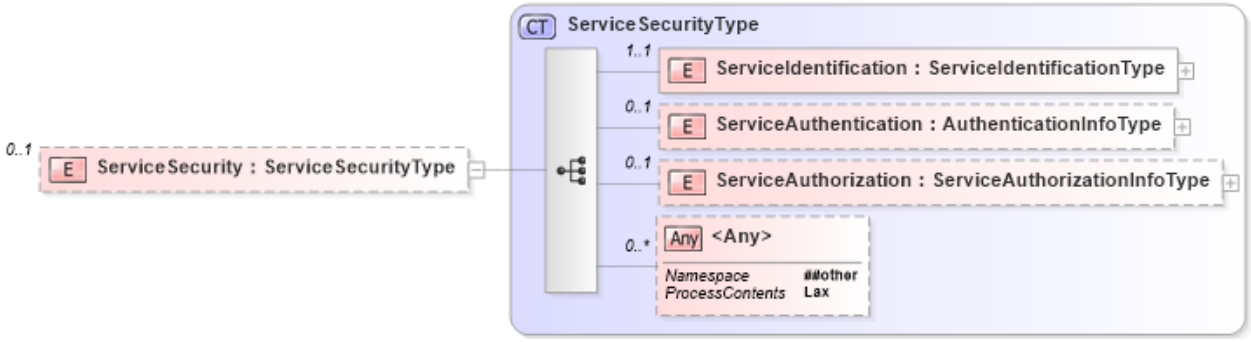


Figure 11: Service Security Elements

6.4.1 ServiceIdentification

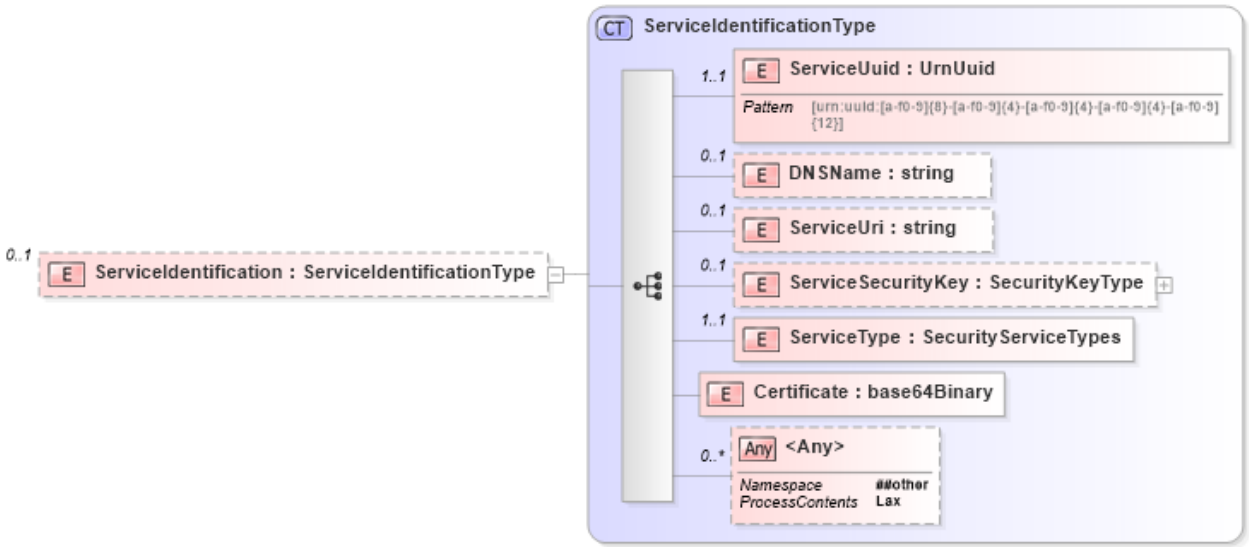


Figure 12 : Service Identification

The ServiceIdentification element contains the attributes necessary for identifying a Service.

6.4.1.1 ServiceUuid

A UUID value to uniquely identify the User. If a UUID is provided, the value MUST be retained for the lifespan of the Service instance. The value SHOULD be retained and the same value used each time a specific instance of the service is executed.

6.4.1.2 DNSName

The DNS name entry for the Service

6.4.1.3 ServiceUri

A Uri value that identifies a Service instance.

6.4.1.4 ServiceSecurityKey

A binary key, such as an X.509 Certificate or OAuth token that can be used to identify a Service instance.

6.4.1.5 ServiceType

A value identifying the type of Service

376 **6.4.1.6 Certificate**

377 An X509 Certificate that identifies the Service

378

379 **6.4.1.7 LocationString**

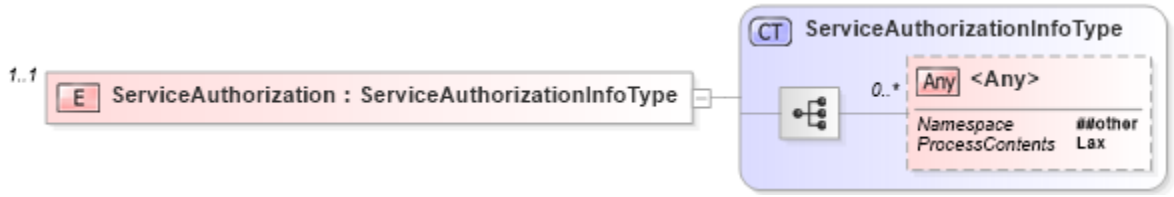
380 The LocationString element is a localized human-readable string describing the physical
381 location of the hardware running service instance.

382 **6.4.1.8 GeoLocation**

383 The Geolocation element represents the GPS coordinates of the physical location of the
384 hardware running service instance. The coordinates MUST be expressed as specified in
385 RFC5870 [RFC5870].

386 **6.4.2 ServiceAuthentication**

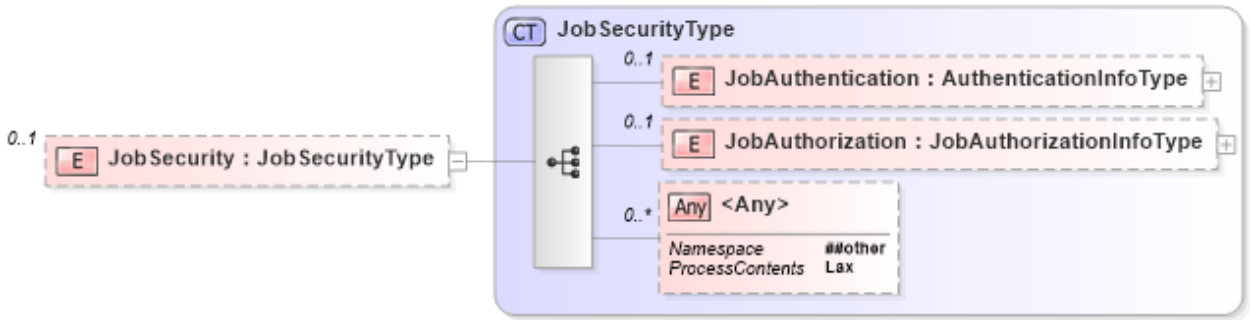
387 **6.4.3 ServiceAuthorization**



388

389 **Figure 13: Service Authorization**

390 ## 6.5 Job Security



391

392 **Figure 14: Job Security Elements**

6.5.1 JobAuthentication

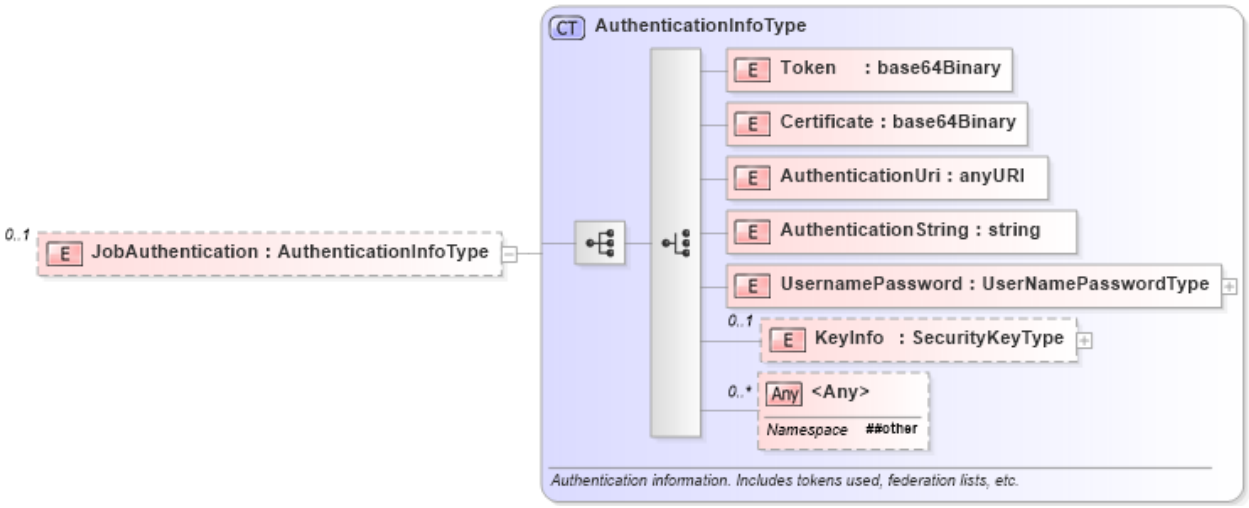


Figure 15: Job Authentication

6.5.2 JobAuthorization

Figure 16: Job Authorization

6.5.3 Document Security

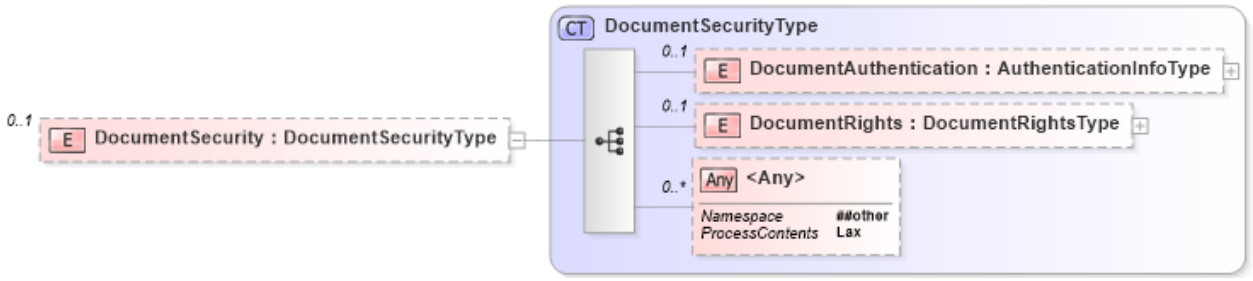


Figure 17: Document Security Elements

6.5.3.1 DocumentAuthentication

The DocumentAuthentication element contains the authentication information necessary for enable access to the document content. This information may range from a simple document password to a document decryption token or key.

6.5.3.2 DocumentRights

The DocumentRights element contains the access and usage rights for the user, device or service defined in a document operation.

General document rights information is carried in the document description and is defined by Dublin core.

7. Conformance Requirements

Provide numbered lists of conformance requirements for the document.

8. Internationalization Considerations

For interoperability and basic support for multiple languages, conforming implementations MUST support the Universal Character Set (UCS) Transformation Format -- 8 bit (UTF-8) [RFC3629] encoding of Unicode [UNICODE] [ISO10646] and the Unicode Format for Network Interchange [RFC5198].

9. Security Considerations

Applicable security considerations are described in the IDS Model Specification. [IDSMODEL]

10. IANA and PWG Considerations

This specification is consistent with the PWG Semantic Model Version 3.0 XML Schema [PWG-SCHEMA]

Provide IANA registration information for this specification.

Subsections include IANA registration templates using the Example style:

```
Some IANA registration text.
```

11. References

11.1 Normative References

[REFERENCE] F. Last author list or standards body, "Title of referenced document", Document Number, Month YYYY, URL (if any)

[PWG-SCHEMA] D. Manchala, “PWG Semantic Model V3.0 Schema”, http://ftp.pwg.org/pub/pwg/sm3/schemas/PWG_SM_3.0_v2.904.zip

[RFC2119] S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119/BCP 14, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[RFC5870] A. Mayrhofer, C. Spanring, RFC 5870, “A Uniform Resource Identifier for Geographic Locations ('geo' URI)”, June 2010, http://www.ietf.org/RFC/RFC5870.txt

11.2 Informative References

12. Authors' Addresses

Primary authors (using Address style):

Joe Murdock
Sharp Labs of America
5750 NW Pacific Rim Blvd
Camas, WA 98607
jmurdock@sharplabs.com

The authors would also like to thank the following individuals for their contributions to this standard:

Nancy Chen
Michael Sweet - Apple
Ira McDonald - High North
Bill Wagner - TIC
Rick Yardumian - Canon

13. Change History

April 2, 2011

Initial revision.

May 24, 2011

Added Roles and Alerts.

August 1, 2011

Updated Security Ticket description and diagrams. Added Security operations.

Oct 5, 2011

Updated for schema changes. Added document security element.

Feb 5, 2014

Converted to new PWG template.

Feb 5, 2014

Updated for Schema changes. Added description of Identification elements. Major reorganization.

November 1, 2014

Updated for Schema changes.

