



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>

1 Copyright © 2014 The Printer Working Group. All rights reserved.

2 This document may be copied and furnished to others, and derivative works that comment
3 on, or otherwise explain it or assist in its implementation may be prepared, copied,
4 published and distributed, in whole or in part, without restriction of any kind, provided that
5 the above copyright notice, this paragraph and the title of the Document as referenced
6 below are included on all such copies and derivative works. However, this document itself
7 may not be modified in any way, such as by removing the copyright notice or references to
8 the IEEE-ISTO and the Printer Working Group, a program of the IEEE-ISTO.

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

10 The IEEE-ISTO and the Printer Working Group DISCLAIM ANY AND ALL WARRANTIES,
11 WHETHER EXPRESS OR IMPLIED INCLUDING (WITHOUT LIMITATION) ANY IMPLIED
12 WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

13 The Printer Working Group, a program of the IEEE-ISTO, reserves the right to make
14 changes to the document without further notice. The document may be updated, replaced
15 or made obsolete by other documents at any time.

16 The IEEE-ISTO takes no position regarding the validity or scope of any intellectual
17 property or other rights that might be claimed to pertain to the implementation or use of the
18 technology described in this document or the extent to which any license under such rights
19 might or might not be available; neither does it represent that it has made any effort to
20 identify any such rights.

21 The IEEE-ISTO invites any interested party to bring to its attention any copyrights, patents,
22 or patent applications, or other proprietary rights which may cover technology that may be
23 required to implement the contents of this document. The IEEE-ISTO and its programs
24 shall not be responsible for identifying patents for which a license may be required by a
25 document and/or IEEE-ISTO Industry Group Standard or for conducting inquiries into the
26 legal validity or scope of those patents that are brought to its attention. Inquiries may be
27 submitted to the IEEE-ISTO by e-mail at: ieee-isto@ieee.org.

28 The Printer Working Group acknowledges that the IEEE-ISTO (acting itself or through its
29 designees) is, and shall at all times, be the sole entity that may authorize the use of
30 certification marks, trademarks, or other special designations to indicate compliance with
31 these materials.

32 Use of this document is wholly voluntary. The existence of this document does not imply
33 that there are no other ways to produce, test, measure, purchase, market, or provide other
34 goods and services related to its scope.

35

36 **About the IEEE-ISTO**

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

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

43 <http://www.ieee-isto.org>

44 **About the IEEE-ISTO PWG**

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

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

59 For additional information regarding the Printer Working Group visit:

60 <http://www.pwg.org>

61 Contact information:

62 The Printer Working Group
63 c/o The IEEE Industry Standards and Technology Organization
64 445 Hoes Lane
65 Piscataway, NJ 08854
66 USA
67

68 **About the Imaging Device Security Work Group (IDS)**

69 Description of PROJECT NAME.

70 For additional information regarding IDS visit:

71 <http://www.pwg.org/ids/>

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

75

Table of Contents

76		
77	1. Introduction.....	7
78	2. Terminology.....	7
79	2.1 Conformance Terminology.....	7
80	2.2 Other Terminology.....	7
81	2.3 Acronyms and Organizations.....	7
82	3. Requirements.....	8
83	3.1 Rationale for IDS Identification, Authentication and Authorization.....	8
84	3.2 Use Cases.....	8
85	3.3 Out of Scope.....	8
86	3.4 Design Requirements.....	8
87	4. Security Elements.....	9
88	4.1 Identification.....	9
89	4.1.1 User Identification.....	9
90	4.1.2 Client Identification.....	9
91	4.1.3 Device Identification.....	9
92	4.1.4 Service Identification.....	9
93	4.2 Authentication.....	9
94	4.3 Authorization.....	9
95	5. Common Security Ticket Elements.....	9
96	5.1 Authentication.....	9
97	5.1.1 Token.....	10
98	5.1.2 Certificate.....	10
99	5.1.3 AuthenticationUri.....	10
100	5.1.4 AuthenticationString.....	10
101	5.1.5 UsernamePassword.....	10
102	5.1.6 KeyInfo.....	10
103	6. Security Elements.....	10
104	6.1 UserSecurity.....	10
105	6.1.1 UserIdentification.....	10
106	6.1.2 UserAuthentication.....	12
107	6.1.3 UserAuthorization.....	12
108	6.2 Device Security.....	13
109	6.2.1 DeviceIdentification.....	13
110	6.2.2 DeviceAuthentication.....	15
111	6.2.3 DeviceAuthorization.....	15
112	6.3 Client Security.....	15
113	6.3.1 ClientIdentification.....	16
114	6.3.2 ClientAuthentication.....	17
115	6.3.3 ClientAuthorization.....	17
116	6.4 Service Security.....	17
117	6.4.1 ServiceIdentification.....	18
118	6.4.2 ServiceAuthentication.....	19
119	6.4.3 ServiceAuthorization.....	19
120	6.5 Job Security.....	19
121	6.5.1 JobAuthentication.....	20

122	6.5.2 JobAuthorization.....	20
123	6.5.3 Document Security	20
124	7. Conformance Requirements.....	21
125	8. Internationalization Considerations	21
126	9. Security Considerations	21
127	10. IANA and PWG Considerations	21
128	11. References	21
129	11.1 Normative References	21
130	11.2 Informative References	22
131	12. Authors' Addresses	22
132	13. Change History	23

List of Figures

136	Figure 1: AuthenticationInfo Type	10
137	Figure 2: User Security Elements.....	10
138	Figure 3: User Identification.....	11
139	Figure 4: User Authorization	13
140	Figure 5: Device Security Elements	13
141	Figure 6: Device Identification	13
142	Figure 7: Device Authorization	15
143	Figure 8: Client Security Elements	15
144	Figure 9: Client Identification	16
145	Figure 10: Client Authorization	17
146	Figure 11: Service Security Elements	17
147	Figure 12 : Service Identification	18
148	Figure 13: Service Authorization	19
149	Figure 14: Job Security Elements.....	19
150	Figure 15: Job Authentication	20
151	Figure 16: Job Authorization.....	20
152	Figure 17: Document Security Elements.....	20

List of Tables

No table of figures entries found.

158 **1. Introduction**

159 Provide an introduction for the document.

160 **2. Terminology**

161 **2.1 Conformance Terminology**

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

167 **2.2 Other Terminology**

168 **2.3 Acronyms and Organizations**

169 *GPS*: Global Positioning System

170 *IANA*: Internet Assigned Numbers Authority, <http://www.iana.org/>

171 *IETF*: Internet Engineering Task Force, <http://www.ietf.org/>

172 *ISO*: International Organization for Standardization, <http://www.iso.org/>

173 *PWG*: Printer Working Group, <http://www.pwg.org/>

174

175

176 3. Requirements

177 3.1 Rationale for IDS Identification, Authentication and Authorization

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

- 181 1. Define new IDS Security Model element attributes and values to support
182 identification of Users, Imaging Devices, Jobs, and Documents.
- 183 2. Define new IDS Security Model element attributes and values to support
184 authentication of Users and Services.
- 185 3. Define new IDS Security Model element attributes and values to support Access
186 Control for Users, Services, Imaging Devices, Jobs, Designated Resources and
187 Documents.

188 3.2 Use Cases

189 Add reference to the Model spec.

190 3.3 Out of Scope

191 The following are considered out of scope for this specification:

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

195 3.4 Design Requirements

196 The design requirements for this specification are:

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

207 6.

208 **4. Security Elements**

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

214 **4.1 Identification**

215 **4.1.1 User Identification**

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

218 **4.1.2 Client Identification**

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

221 **4.1.3 Device Identification**

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

224 **4.1.4 Service Identification**

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

227 **4.2 Authentication**

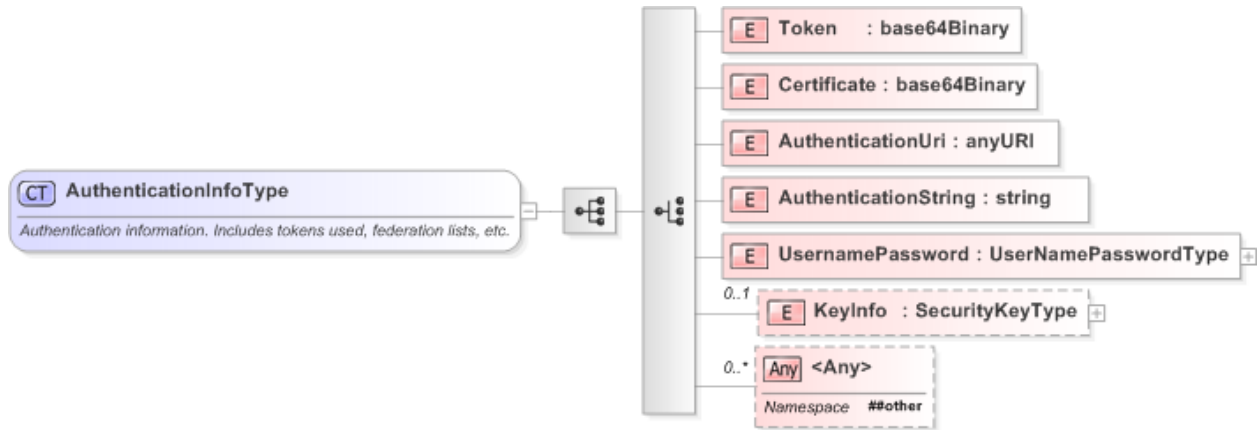
228 **4.3 Authorization**

229 **5. Common Security Ticket Elements**

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

231 **5.1 Authentication**

232



233

234

Figure 1: AuthenticationInfo Type

235 **5.1.1 Token**

236 **5.1.2 Certificate**

237 **5.1.3 AuthenticationUri**

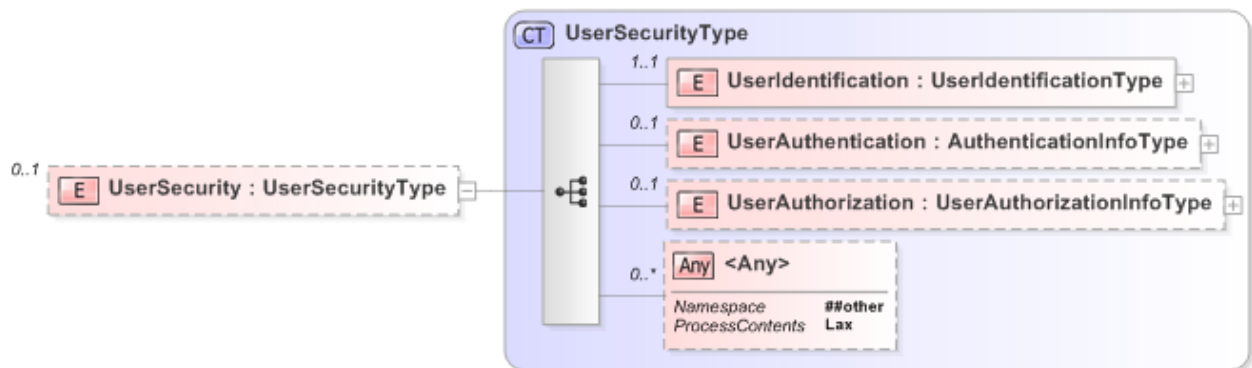
238 **5.1.4 AuthenticationString**

239 **5.1.5 UsernamePassword**

240 **5.1.6 KeyInfo**

241 **6. Security Elements**

242 **6.1 UserSecurity**



243

244

Figure 2: User Security Elements

245 **6.1.1 UserIdentification**

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

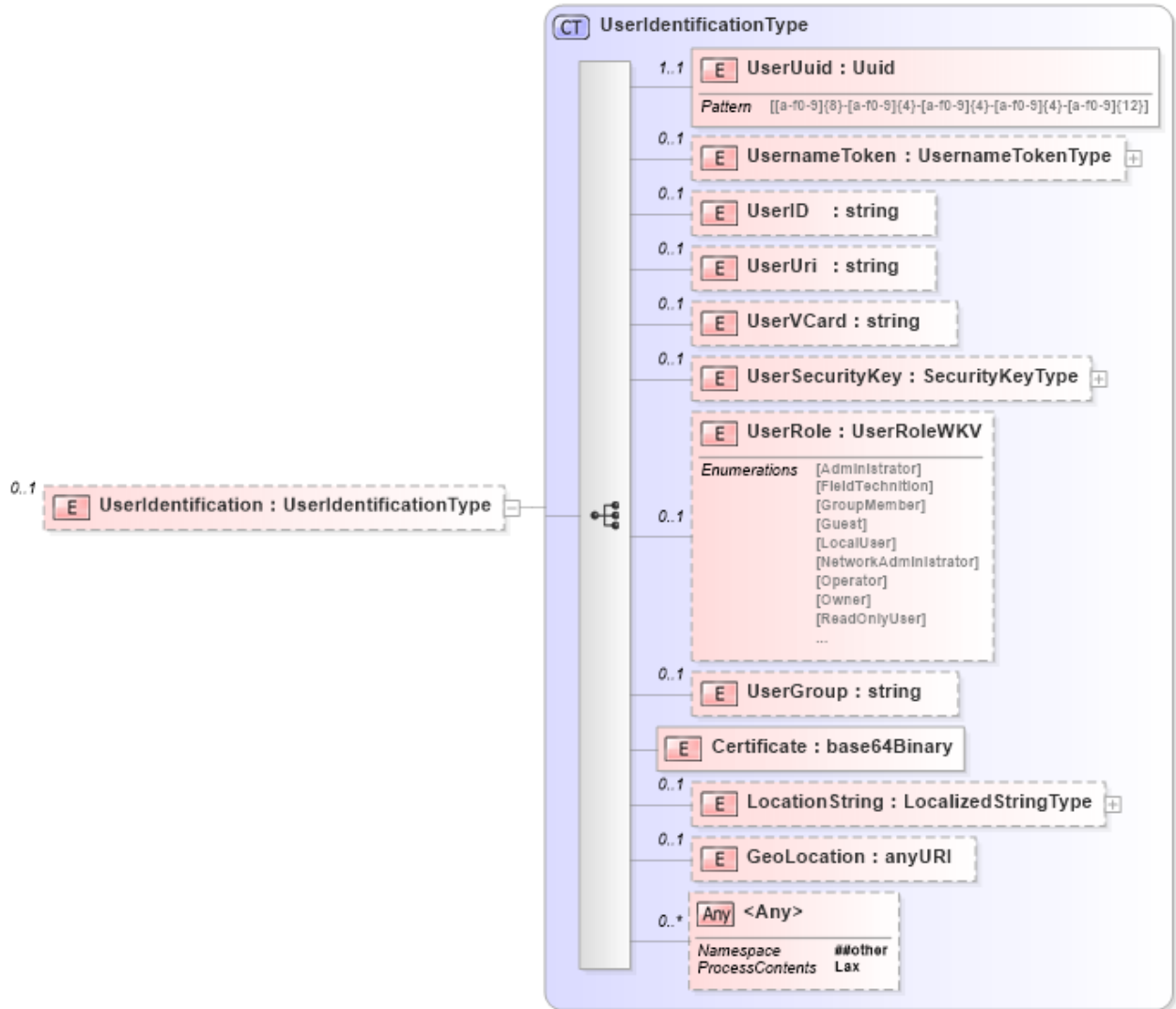


Figure 3: User Identification

247

248

249 **6.1.1.1 UserUuid**

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

252 **6.1.1.2 UsernameToken**

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

255 **6.1.1.3 UserId**

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

258 **6.1.1.4 UserUri**

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

260 **6.1.1.5 UserVCard**

261 A VCard record that identifies the user.

262 **6.1.1.6 UserSecurityKey**263 A binary key, such as an OAuth or Active Directory Access token or Kerberos Ticket that
264 can be used to identify a User265 **6.1.1.7 UserRole**

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

267 **6.1.1.8 UserGroup**

268 The organizational groups to which the User belongs

269 **6.1.1.9 Certificate**

270 An X509 Certificate that identifies the User

271 **6.1.1.10 LocationString**272 The LocationString element is a localized human-readable string describing the current
273 location of the user. This may be an abstract location value such as "In my car"274 **6.1.1.11 GeoLocation**275 The Geolocation element represents the GPS coordinates of the current physical location
276 of the user. Generally this location will also refer to the location of the device the User is
277 actually using.278 The coordinates MUST be expressed as specified in "A Uniform Resource Identifier for
279 Geographic Locations ('geo' URI)" [RFC5870].280 **6.1.2 UserAuthentication**281 **6.1.3 UserAuthorization**

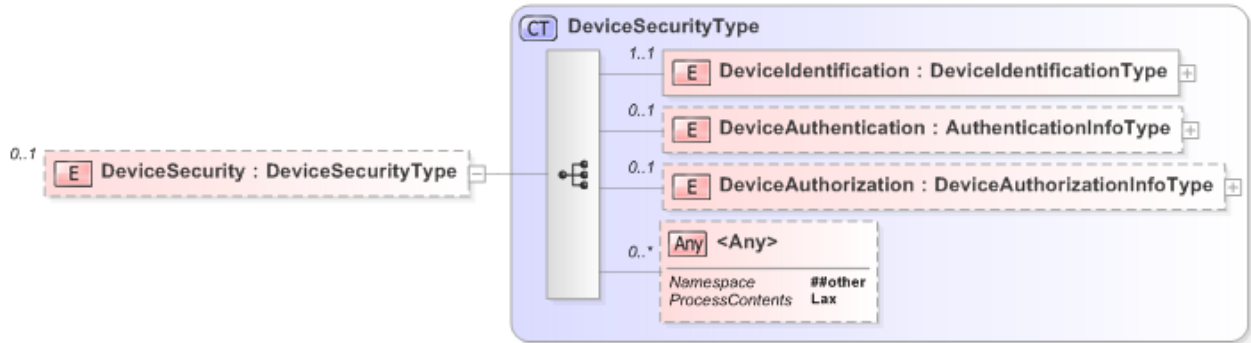
282



283

Figure 4: User Authorization

284 **6.2 Device Security**

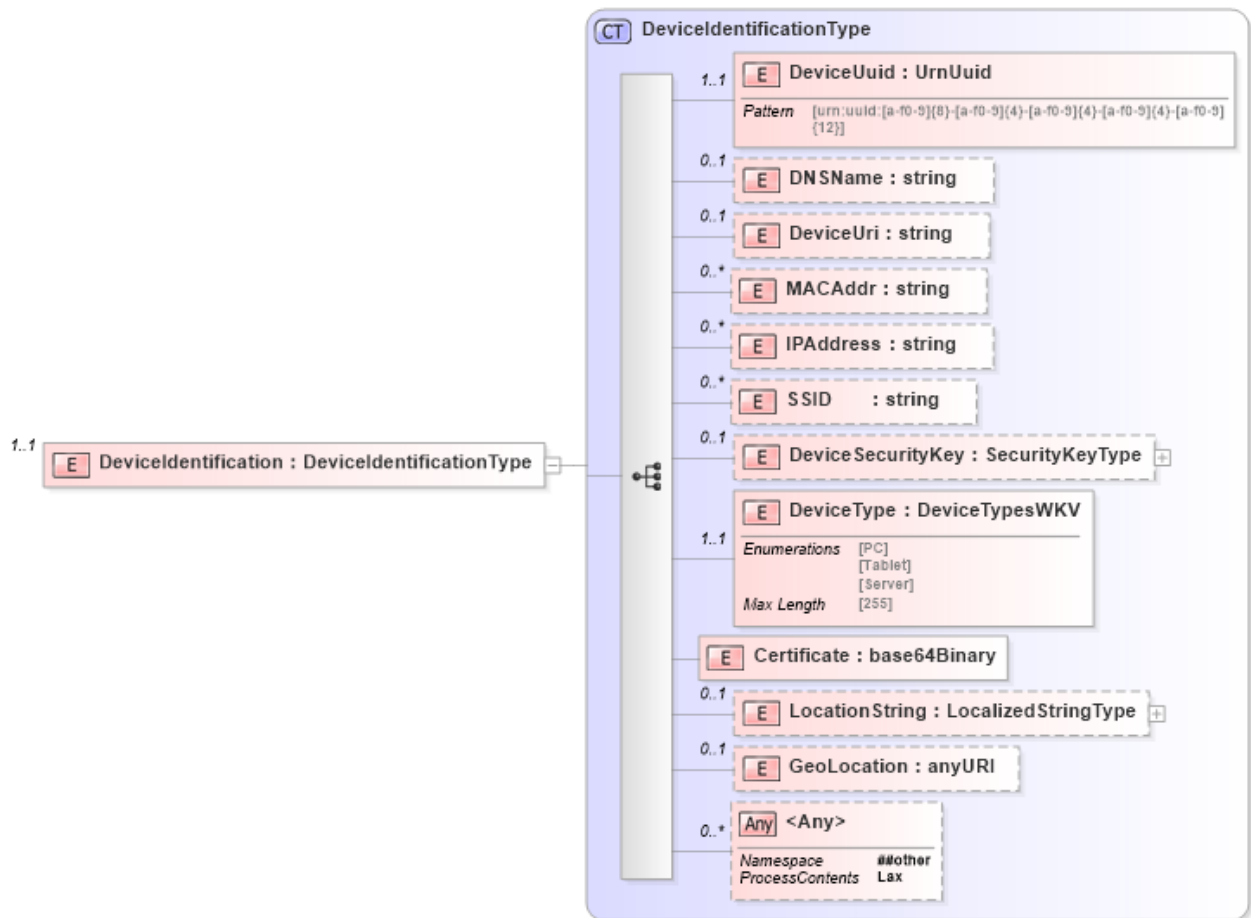


285

286

Figure 5: Device Security Elements

287 **6.2.1 DeviceIdentification**



288

289

Figure 6: Device Identification

290 The DeviceIdentification element contains the attributes necessary for identifying a Device.
291

292 **6.2.1.1 DeviceUuid**

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

296 **6.2.1.2 DNSName**

297 The registered DNS name of the Device

298 **6.2.1.3 DeviceUrl**

299 A Uri value that identifies the Device,

300 **6.2.1.4 MACAddr**

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

303 **6.2.1.5 IPAddr**

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

305 **6.2.1.6 DeviceSecurityKey**

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

308 **6.2.1.7 DeviceType**

309 A value identifying the type of the device

310 **6.2.1.8 Certificate**

311 An X509 Certificate that identifies the Device

312 **6.2.1.9 LocationString**

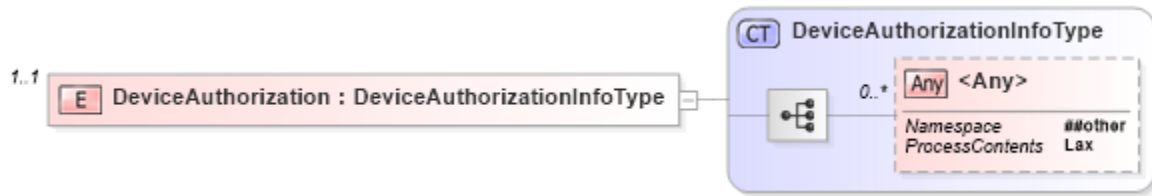
313 The LocationString element is a localized human-readable string describing the physical
314 location of the hardware device.

315 **6.2.1.10 GeoLocation**

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

319 **6.2.2 DeviceAuthentication**

320 **6.2.3 DeviceAuthorization**

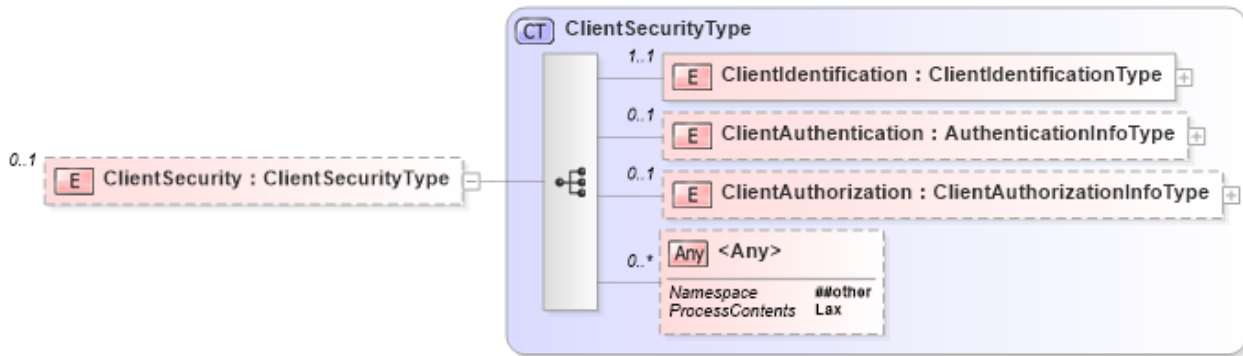


321

322

Figure 7: Device Authorization

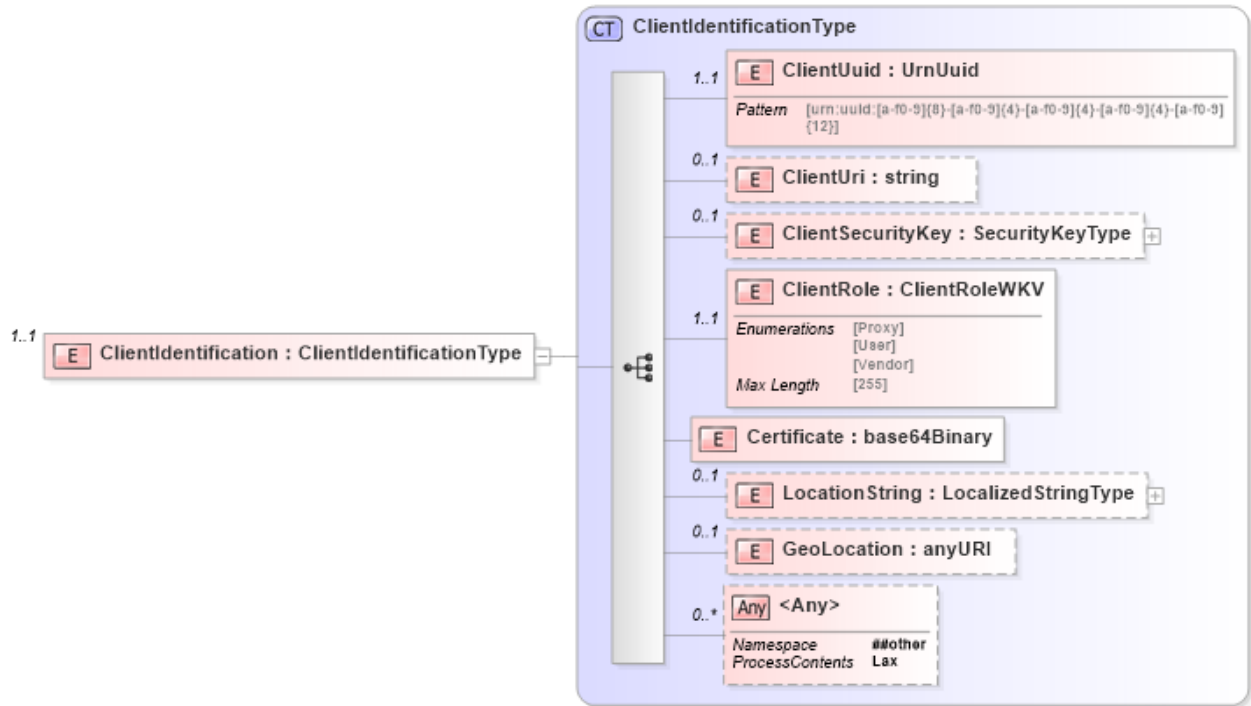
323 **6.3 Client Security**



324

325

Figure 8: Client Security Elements

326 **6.3.1 ClientIdentification**

327

328

Figure 9: Client Identification

329 The ClientIdentification element contains the attributes necessary for identifying a Client.
 330

331 **6.3.1.1 ClientUuid**

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

334 **6.3.1.2 ClientUri**

335 A Uri value that identifies the Client process or application.

336 **6.3.1.3 ClientSecurityKey**

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

339 **6.3.1.4 ClientRole**

340 The role of the Client process

341 **6.3.1.5 Certificate**

342 An X509 Certificate that identifies the Client

343 **6.3.1.6 LocationString**

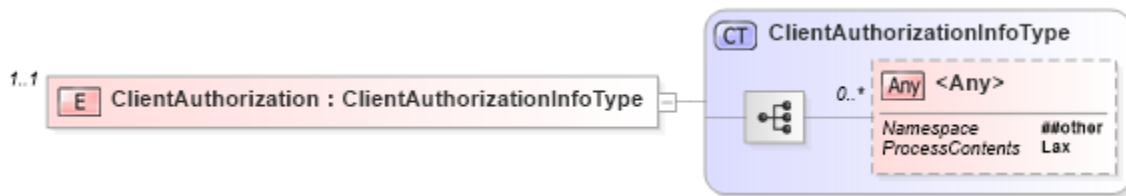
344 The LocationString element is a localized human-readable string describing the physical
345 location of the hardware running service instance.

346 **6.3.1.7 GeoLocation**

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

350 **6.3.2 ClientAuthentication**

351 **6.3.3 ClientAuthorization**

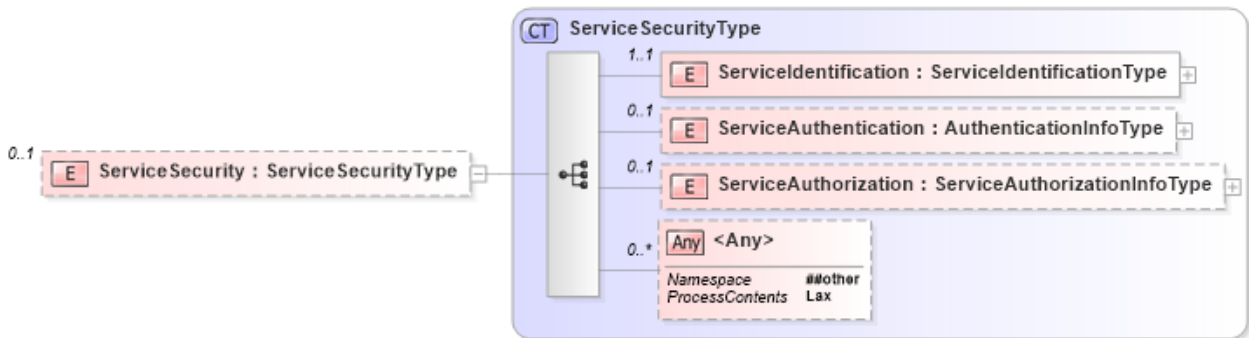


352

353

Figure 10: Client Authorization

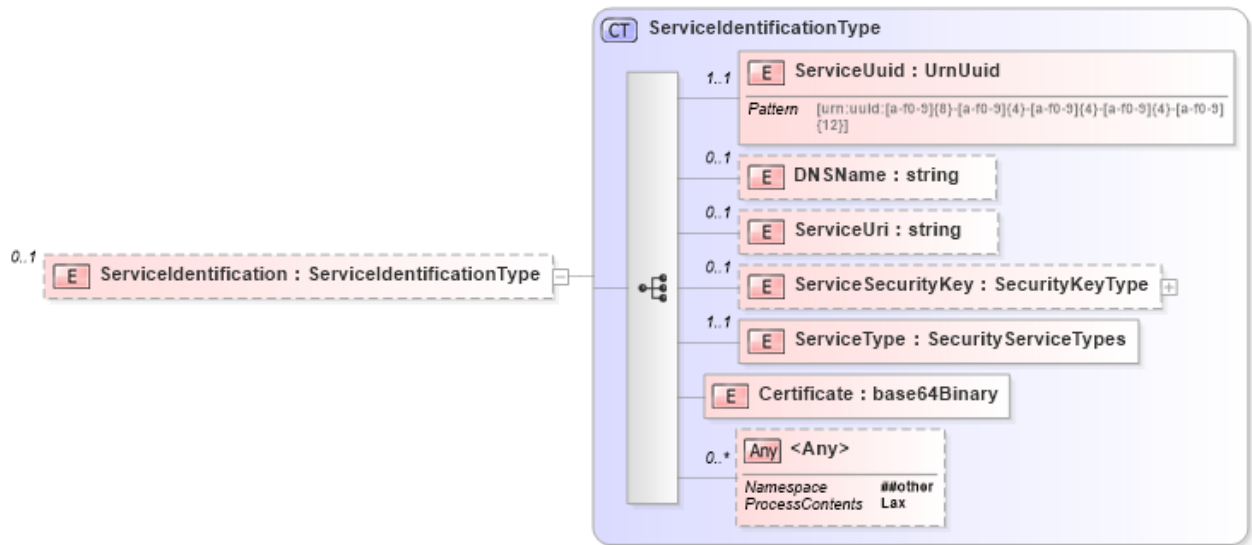
354 **6.4 Service Security**



355

356

Figure 11: Service Security Elements

357 **6.4.1 ServiceIdentification**

358

359

Figure 12 : Service Identification

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

362

363 **6.4.1.1 ServiceUuid**

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

367 **6.4.1.2 DNSName**

368 The DNS name entry for the Service

369 **6.4.1.3 ServiceUri**

370 A Uri value that identifies a Service instance.

371 **6.4.1.4 ServiceSecurityKey**

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

374 **6.4.1.5 ServiceType**

375 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**

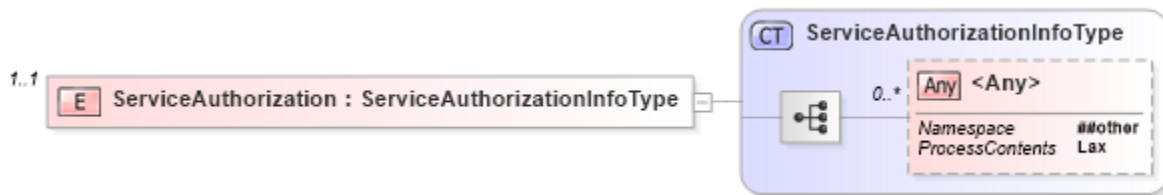
380 The LocationString element is a localized human-readable string describing the physical
381 location of the hardware running service instance.

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**

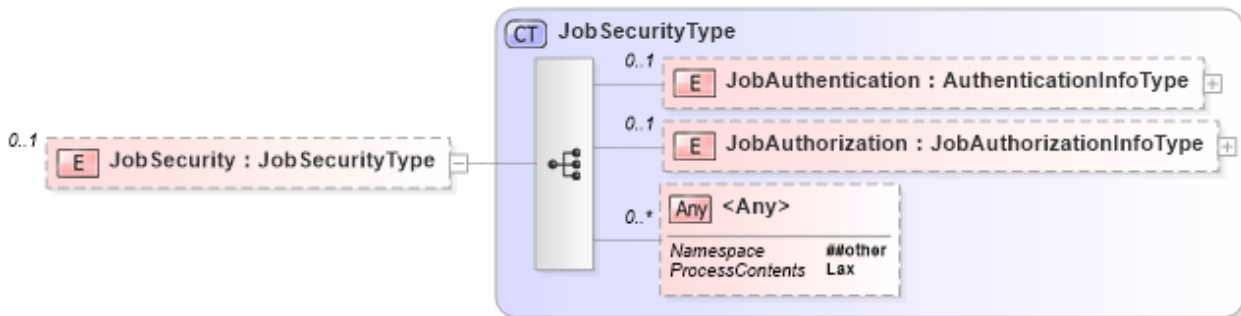


388

389

Figure 13: Service Authorization

390 **6.5 Job Security**

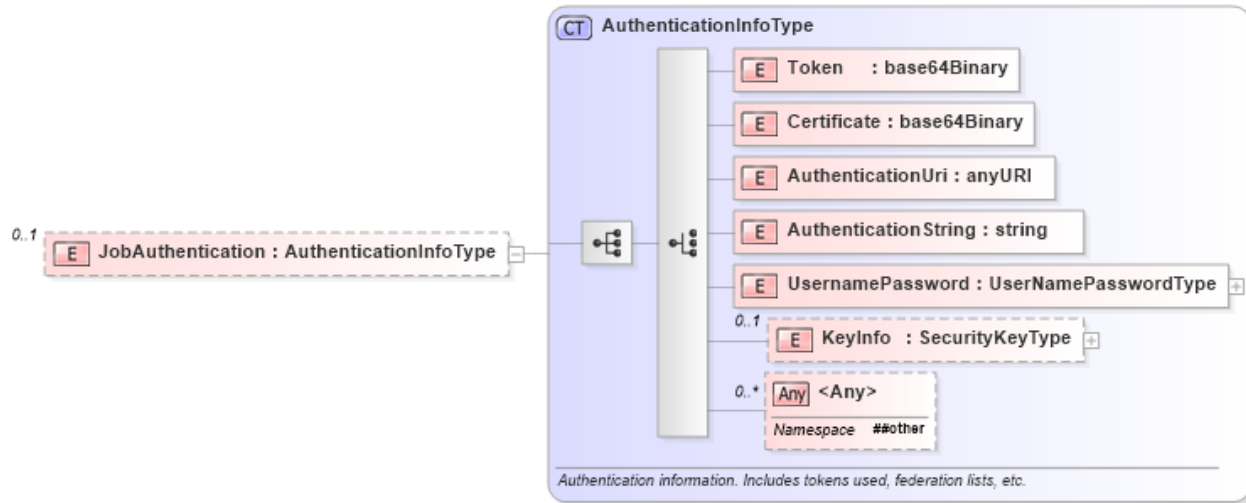


391

392

Figure 14: Job Security Elements

393 **6.5.1 JobAuthentication**



394

395 **Figure 15: Job Authentication**

396 **6.5.2 JobAuthorization**

397



398

399 **Figure 16: Job Authorization**

400 **6.5.3 Document Security**

401

402

Figure 17: Document Security Elements

403 **6.5.3.1 DocumentAuthentication**

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

407 **6.5.3.2 DocumentRights**

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

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

412 **7. Conformance Requirements**

413 Provide numbered lists of conformance requirements for the document.

414 **8. Internationalization Considerations**

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

419 **9. Security Considerations**

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

422 **10. IANA and PWG Considerations**

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

425 Provide IANA registration information for this specification.

426 Subsections include IANA registration templates using the Example style:

427 `Some IANA registration text.`

428 **11. References**

429 **11.1 Normative References**

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

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

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

437 [RFC5870] A. Mayrhofer, C. Spanring, RFC 5870, "A Uniform Resource Identifier
438 for Geographic Locations ('geo' URI)", June 2010,
439 <http://www.ietf.org/RFC/RFC5870.txt>

440 **11.2 Informative References**

441 **12. Authors' Addresses**

442 Primary authors (using Address style):

443 Joe Murdock
444 Sharp Labs of America
445 5750 NW Pacific Rim Blvd
446 Camas, WA 98607
447 jmurdock@sharplabs.com

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

450 Nancy Chen
451 Michael Sweet - Apple
452 Ira McDonald - High North
453 Bill Wagner - TIC
454 Rick Yardumian - Canon
455

456 **13. Change History**

457 **April 2, 2011**

458 Initial revision.

459 **May 24, 2011**

460 Added Roles and Alerts.

461 **August 1, 2011**

462 Updated Security Ticket description and diagrams. Added Security operations.

463 **Oct 5, 2011**

464 Updated for schema changes. Added document security element.

465 **Feb 5, 2014**

466 Converted to new PWG template.

467 **Feb 5, 2014**

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

470 **November 1, 2014**

471 Updated for Schema changes.

472