The Printer Working Group

April 26, 2015
Interim

Imaging System Security Model (ISS-Model)

Status: Interim

Abstract: This document defines a model and set of security requirements that are common to and shared between PWG standards and recommendations.

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-model10-20150426.pdf

Title: Imaging System Security Model (IDS-Model)

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 (IDS) Work Group

Description of IDS.

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

1. Introduction....8
2. Terminology....8
2.1 Conformance Terminology....8
2.2 Other Terminology....8
2.3 Acronyms and Organizations....10
3. Requirements....11
3.1 Rationale for Imaging System Security Model....11
3.2 Use Cases....11
3.2.1 Identify, Authenticate and Authorize a User....11
3.2.2 Enforce security requirements....12
3.2.3 Find a secure Imaging System....12
3.2.4 Ensure encrypted data In Transit....12
3.2.5 Control job access at the Imaging Device....12
3.2.6 Control secure remote operation....12
3.2.7 Audit Document Trail....12
3.2.8 Imaging Job Confidentiality....12
3.2.9 Tracking Imaging System Usage....13
3.2.10 Imaging System Resource Access Control....13
3.3 Out of Scope....13
3.4 Design Requirements....13
4. PWG Security Model....13
4.1 Security Functions....14
4.1.1 Identification....14
4.1.2 Authentication....14
4.1.3 Authorization....14
4.2 Security Declaration Models....14
4.3 Actors....15
4.3.1 Device Actor....15
4.3.2 Service Actor....15
4.3.3 Client Actor....15
4.3.4 User Actor....15
4.4 Security Objects....15
4.4.1 Device/System....16
4.4.2 Service....16
4.4.3 Job....16
4.4.4 Document....16
4.5 Roles and Types....16
4.5.1 User Roles....16
4.5.2 Client Roles....17
4.5.3 Device Roles....17
4.5.4 Service Roles....18
4.5.5 Device Types....18
5. Security Ticket....19
5.1 Signature....19
5.2 Security Elements....20

5.2.1 UserSecurity Elements 21
5.2.2 DeviceSecurity Elements 22
5.2.3 ClientSecurity Elements 23
5.2.4 ServiceSecurity Elements 23
5.2.5 JobSecurity Elements 24
5.2.6 DocumentSecurity Elements 25
6. Security Operations 26
6.1 GetServiceElements (SecurityElements) 26
6.1.1 GetSecurityElementsRequest 26
6.1.2 GetSecurityElementsResponse 27
6.1.3 GetSecurityElements Operations 28
7. Alerts and Notifications 28
7.1 Security Alerts 29
8. Conformance Requirements 29
9. Conformance Recommendations 29
9.1 IEEE2600-2008 Conformance 29
9.2 Imaging System health and network access 29
9.3 Audit Log Generation and Availability 30
10. Internationalization Considerations 30
11. Security Considerations 30
11.1 Protection of End User's Data 30
12. IANA and PWG Considerations 31
13. References 31
13.1 Normative References 31
13.2 Informative References 32
14. Authors' Addresses 33
15. Change History 33

List of Figures

Figure 1: Security Ticket 19
Figure 2: Security Owner 20
Figure 3: Security Elements 21
Figure 4: User Security 21
Figure 5: Device Security 22
Figure 6: Client Security 23
Figure 7: Service Security 24
Figure 8: Job Security 24
Figure 9: Document Security 25
Figure 10: GetSecurityElement Request 26
Figure 11: GetSecurityElement Response 27
Figure 12 : GetSecurityElements Sequence Diagram 28

List of Tables

188 Table 1: User Roles 17
189 Table 2 : Client Roles.....17
190 Table 3: Device Roles.....17
191 Table 4: Service Roles.....18
192 Table 5 : Device Types 19
193 Table 6: Security Alert Codes.....29
194
195

1. Introduction

This standard defines a model and set of security requirements that are common to and shared between PWG standards and recommendations.

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

Actor: An entity (i.e. a person or a software process) that attempts or requests to perform an action on some security object.

Client: An application or software process that communicates with a service on behalf of a User.

Client Device: A hardware device on which a Client application or process is executed.

Correlated Attributes: An ordered set of related attributes that describe an instance of firmware or software. The purpose of these Correlated Attributes is to allow ease-of-access and verification for each instance.

Delegated Resource: A resource where the Owner has shared access rights to a different actor.

Directory Service: A directory service is a collection of software and processes that store information about Users, Devices, Services or other resources.

Endpoint: An endpoint is the directly addressable location of a device or resource in a communications network. In the PWG Security Model, an endpoint is usually the location of a service providing a resource or function or the location of a physical device. Endpoints are typically specified as a protocol-specific network address, such as an Internet Protocol (IP) address or DNS name, or as the URL of a specific service instance. A device or service may have more than one endpoint.

Executable Imaging Resource: A Service that provides Imaging Resources by processing Imaging Documents, Jobs or data.

Imaging Device: A device capable of processing Imaging Jobs.

Imaging Document: An object created and managed by an Imaging System that contains the description, processing, and status information. An Imaging Document object may have attached data and is bound to a single Imaging Job.

Imaging Job: An object created and managed by an Imaging System that contains description, processing, and status information. The Imaging Job also contains zero or more Imaging Document objects.

Imaging Operations: A set of Service and Job operations that can be performed on an Imaging System or service, such as Copy, Scan, Print, Fax, etc.

Imaging Resource: An object or set of objects that can be access by an Imaging System or Imaging Service when processing an Imaging Job. Imaging Resources may consist of static data or be an Executable Imaging Resource.

Imaging Service: A Service that is capable of processing Imaging Jobs

Imaging System: A hardware device or software process, or any combination of such devices or software processes, that processes or produces hardcopy (i.e. paper) or Imaging Documents.

Network Accessible Device: A Device that can be directly accessed by a Client.

Kerberized Printing: authenticated printing based on SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows [RFC4559], Transport Layer Security/1.2 [RFC5246], and Upgrading to TLS Within HTTP/1.1 [RFC2817].

Network Accessible/Accessibility: Refers to the ability of one device to communicate directly with another, for example a Client is able to connect to a Device, query for supported attributes, submit Job creation requests, and so forth.

Network Visible Entity: A Network-visible Entity (NVE), also known as NVE socket, is the resource that is addressable through a network. Typically, an NVE is a socket client for a service available in a node. [JAVVIN].

Secure Transport: encryption of the HTTP connection using Transport Layer Security [RFC5246]. The security session may be negotiated at the initiation of the connection ("HTTPS") or by Upgrading to TLS Within HTTP/1.1 [RFC2817].

Security Actor: an authenticated actor with rights to modify security policies or perform other security-related operations such as shutting down services

Security Attribute: A data element and value that defines structured security information, such as a password or access code.

Security Domain: A bounded group of security objects and security subjects to which applies a single security policy executed by a single security administrator [ECMATR46]

Service: Software providing access to physical, logical, or virtual resources and (typically) processing of queued Jobs.

System Account: A special type of account of a computer system used to run system or application processes that require less restricted access than an administrative or root account to system resources and processes.

System Administrator: An Actor who is authorized to manage all aspects of a System

System User: An Actor who is authorized to perform basic functions on a System

User: An Actor who has the authorization to perform normal functions of a System, Service or Device

2.3 Acronyms and Organizations

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/

MFD: Multi-Function Device

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

3. Requirements

3.1 Rationale for Imaging System Security Model

Given the following existing and developing specifications:

- PWG 5110.3-2013, "PWG Common Log Format" [PWG5110.3]
- RFC 2911 "Internet Printing Protocol/1.1: Model and Semantics" [RFC2911]
- RFC 3995 "Internet Printing Protocol: Event Notifications and Subscriptions" [RFC3995]
- PWG 5100.12-2011 "IPP/2.0 Second Edition" [PWG5100.12]
- PWG 5100.14-2013 "IPP Everywhere" [PWG5100.14]
- IEEE 2600-2008 IEEE Standard for Information Technology: Hardcopy Device and System Security [IEEE2600]
- PWG Semantic Model [PWG5108.1]
- PWG Cloud Imaging Requirements and Model [PWG-CLOUD]

And given the need for a standard method of defining, describing, and enforcing security for Imaging Systems, the Imaging System Security Model should:

1. Provide recommendations for Imaging System Security policies based on accepted security best practices.
2. Define new Semantic Model elements to support identification of Users, Clients, Imaging Systems, Imaging Services, Subscriptions, Jobs, and Documents.
3. Define new Semantic Model elements to support authentication of Users, Clients, Imaging Systems and Imaging Services.
4. Define new Semantic Model elements to support Access Control for Users, Clients, Subscriptions, Imaging Systems, Imaging Services, Jobs, Documents and Delegated Resources.

3.2 Use Cases

3.2.1 Identify, Authenticate and Authorize a User

Mike wants to print a document from his mobile phone to a hotel printer. The hotel provides print service for hotel guest, and needs to ensure that only a guest uses a printer. Mike wants to make sure that he is using an available free hotel printer.

3.2.2 Enforce security requirements

John is using his laptop computer to print 100,000 copies of his company's product plan through an Internet printing service. The Internet printing service has a relationship with another printer service that can print the brochures in multiple locations that are close to John's company's branch offices. Since these product plans contain proprietary information, John and the print service need to ensure that all systems and companies involved in the process are properly identified and vetted.

3.2.3 Find a secure Imaging System

Jerry is travelling in a foreign country and needs to securely print a document without fear that a chosen printer may create an illicit copy of the document. He configures his PC to find and use only printers that have been certified by a trusted certification authority to meet a specific level of security.

3.2.4 Ensure encrypted data In Transit

Jane is travelling to a branch office of her company and wants to use a public printing service to securely print a sensitive document on a company printer at her destination so the document is available when she arrives.

3.2.5 Control job access at the Imaging Device

After Jane remotely sent her encrypted print job to a branch office printer, she wants to make sure that no one can pick up her jobs before her. She needs the print service or printer to hold the print job until she enters a release code to begin printing.

3.2.6 Control secure remote operation

Tom is working from home but needs some office documents scanned and sent to his home PC. While his administrative assistant can load the necessary documents into the scanner, the company needs to limit where and to whom the scanned documents can be sent. .

3.2.7 Audit Document Trail

A corporation suspects that confidential non-public data has been compromised by printing a document that contains the information. The investigating forensics team wants to audit the document trail from the host location to all instances of it being printed, and identify trace all access to the data stream, or the printed document. The forensic team also wants to know the times and locations that each person had access to the data.

3.2.8 Imaging Job Confidentiality

Bob would like to be able to generate an Imaging Job on one Imaging System but have it rendered on a different Imaging System. Both devices are connected via a network. The contents of the Imaging Job are confidential and should not be disclosed to unauthorized

parties capable of intercepting (either actively or passively) the job in transit between the devices.

3.2.9 Tracking Imaging System Usage

Bob would like to utilize an Imaging System that is administratively controlled by Alice. Alice would like to unambiguously identify "who" is using the Imaging System, based on identity credentials that have been previously issued to Bob.

3.2.10 Imaging System Resource Access Control

Bob would like to utilize an Imaging System administratively controlled by Alice. The Imaging System is capable of multiple functions and consumes resources that Alice deems valuable. Alice would like to control which functions and consumables of the device Bob is capable of using,

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
4. Authentication of Network Connected devices

3.4 Design Requirements

The design for the Imaging System Security Model should:

1. Define new Semantic Model elements and values to support identification of Users, Client Devices, Imaging Systems, Imaging Services, Jobs, and Documents.
2. Define new Semantic Model elements and values to support delegated resource access.
3. Provide recommendations for Imaging System Security policies based on accepted security best practices.
4. Define methods for authentication, authorization, and access control using existing protocols and schema.
5. Provide the ability for vendors to add extensions to the Semantic Model Elements.

4. PWG Security Model

The PWG Security Model is based on the idea of defining and attaching a set of Security Attributes to the operations and data defined by other PWG specifications, such as Imaging Services, Imaging Operations, Job Tickets and Documents. These Security

Attributes provide the information necessary to perform the basic security functions defined by the model: Identification, Authentication and Authorization.

The PWG Security Model can apply security requirements and credentials to different type of entities. This specification describes two types of security entities, the Actor, and a Security Object.

4.1 Security Functions

The IDS Model defines core Security Attributes and values for the identification, Authentication and Authorization of Imaging Systems. The Security Attributes and values can be applied to one or more Actors and are carried in a PWG Security Ticket.

4.1.1 Identification

Depending on the local site policy, authentication typically involves the identification of an Actor based on three factors: “what you know” such as a username and password; “what you have” such as presenting an ID card, a digital certificate, or entering a SecurID code; or “who you are” information such as fingerprint, palm print, Iris scan, facial scan, etc.

4.1.2 Authentication

The identity of a Actor can easily be stolen or copied and should not be trusted without being authenticated. The Authentication of a Actor requires that the Identity information provided for an Actor, be combined with additional information, such as a password, PIN code or biometric information. The combination of this information can then be validated by a known and trusted authentication service or database.

4.1.3 Authorization

Depending on the local site access policy, the access rights for an authenticated Actor may be restricted in what operations may be performed and what resources may be accessed. By defining the rights and permissions that belong to specific Actors, resources and operations, a site can control access to resources and capabilities. Authorization of an Actor for access to a resource or operation is then accomplished by validating the policy rights and restrictions for an Actor against the access policy for a resource or operation. The validation is performed buy an external or local Authorization Service. This document inherits the choices for implementation of authorization covered in [IEEE2600] and [IEEE2600.1-2009].

4.2 Security Declaration Models

In order to provide clear, independent and transportable definitions for common PWG security requirements, a standard language must be used to express security requirements. While several standards for expressing security information exist, PWG security specifications will use the Extensible Access Control Markup Language (XACML)

411 for describing Access Control and Authorization information. XACML is standard XML
412 Schema that represents authorization and access policies [OASIS-XACML].

413 4.3 Actors

414 An actor is an entity (i.e. a person or a software process) that attempts or requests to
415 perform an action on some security object.

416 4.3.1 Device Actor

417 An Client Device is a physical hardware entity, such as a smart phone, tablet, computer, or
418 Imaging System. Devices may perform actions as requesting access and authentication to
419 a network. Such actions can be an allowed or disallowed within a Security Domain based
420 on parameters provide by the device such as OS version, Device and System Health, and
421 supported communication protocols and encryption levels, or the physical location of the
422 device (GeoLocation), and thus the location of User or Services available on that device.

423 4.3.2 Service Actor

424 A Service is “a mechanism to enable access to one or more capabilities, where the access
425 is provided using a prescribed interface and is exercised consistent with constraints and
426 policies as specified by the service description.” [OASIS-SOA]

427 It may be a separate application executed by a user, or a process executing as part of a
428 device operating system. In the context of this document, the Service is a visible entity
429 that a User or another Service connects to in order to perform a function.

430 4.3.3 Client Actor

431 A Client is a software process that communicates with a service. A client may be an
432 autonomous process or interact based on input from a User.

433 4.3.4 User Actor

434 An individual User of a device or service, usually a human, but could be a System
435 Account. The Security attributes of a User are global to a particular Security Domain, but
436 may be overridden by the attributes of the device currently being used by the User; i.e.
437 while a User may be authorized to use a particular service, if they are accessing the
438 service from a controlled location, as determined by the device being used, access may be
439 denied.

440 4.4 Security Objects

441 A Security Object is an entity upon which some action or operation can be performed. The
442 scope or allowable effect of the action may be limited or modified by a set of attributes
443 applied to the object and action.

4.4.1 Device/System

In the PWG security model, a Device or System may also be an object to which an action can be directed.

4.4.2 Service

Similar to a device, a Service may also be viewed as an object that can be acted upon.

4.4.3 Job

Since many PWG specifications are concerned with the creation and processing of jobs, the PWG Security Model allows for the application of Security Attributes to a specific job.

4.4.4 Document

Similar to jobs, the PWG Security Model provides for the application of Security Attributes to a specific document.

4.5 Roles and Types

To assist in the definition and organization of allowed operations and capabilities, each User, Device and Service may be assigned to one or more specific roles used assign and categorize the capabilities and operation allowed. For this purpose, the following standard role definitions are provided. A specific implementation may add additional roles as desired.

4.5.1 User Roles

Role	Description
Administrator	A User who is authorized to manage all aspects of a Device or Service.
FieldTechnician	A Field Technician is allowed to install physical devices and accessories. The Field Technician is also allowed to perform the installation and setup of imaging services.
GroupMember	A Group Member is allowed to access any operation and resources allowed for the assigned group
Guest	A User who has limited and temporary access to basic imaging functions such as print, fax or scan.
LocalUser	An Actor who is interacting with an Imaging System or Imaging Service from within physical proximity to the Device or Service)
NetworkAdministrator	A User who is authorized to manage network configuration and access parameters of the Imaging System or Imaging Services.
Operator	A User that has special rights on the Imaging System. The Operator typically oversees the Imaging System.

	The Operator is allowed to query and control the Imaging System, Jobs and Documents based on site policy.
Owner	The User who owns a particular object (usually the creator) such as a Job, an Imaging System or Imaging Service, or an Imaging Service registration.
ReadOnlyUser	This is a role that allows a User to only perform query and read operations on the managed elements.
RemoteUser	A User who is interacting with an Imaging System or Imaging Service from a remote location (i.e. a location not within physical proximity to an Imaging System)
SecurityAdministrator	An Actor who is authorized to manage security aspects of the Imaging System and Imaging Services, such as defining access by User roles, installing security certificates, etc.
ServiceTechnician	An Actor responsible for repairing a malfunctioning Imaging System, performing routine preventive maintenance, and other tasks that typically require advanced training on the device internals [RFC3805]
NormalUser	An Actor who is authorized to perform basic imaging functions such as print, fax or scan.
Proxy	A Client or process that is acting as an intermediary on behalf of a User or Imaging Service.
SystemUser	An Actor who is authorized to perform basic functions on a System

462 **Table 1: User Roles**

463 ### 4.5.2 Client Roles

Role	Description
User	A client representing a User
Proxy	A process that is acting as an intermediary on behalf of another Client or Service
Vendor	A custom role defined by the system vendor.

464 **Table 2 : Client Roles**

465 ### 4.5.3 Device Roles

Role	Description
Client	A device directly used by a User (i.e. tablet)
Server	Service provider

466 **Table 3: Device Roles**

4.5.4 Service Roles

Role	Description
Client	A Client of the Service
Server	A Service provider
Identification Service	A Service that provides identification information for an Actor, such as a Smart Card processing service.
Key Distribution Service	A Service that supplies session tickets and temporary session keys, such as those used in the Kerberos authentication protocol.
Authentication Service	An Authentication Provider (e.g. a key generator or 2-factor device or service); A Service that can perform authentication of Actors and Objects based on provide Security Attributes
Authorization Service	A Service that provides access control decisions
Directory Service	A Service that provides access to directory information, such as user names and accounts
Copy Service	An Imaging Service that provides hardcopy duplication of hardcopy documents
Print Service	An Imaging Service that provides for hardcopy printed output of digital information.
Scan Service	An Imaging Service that provides digital representation of a hardcopy documents
FaxOut Service	An Imaging Service that sends outbound Facsimile jobs
FaxIn Service	An Imaging Service that receives inbound Facsimile jobs
Transform Service	An Imaging Service that transforms digital input into another form of digital output
System Control Service	A service that provides control over other Imaging Services, such as scan and print, within a system

Table 4: Service Roles

4.5.5 Device Types

The PWG Security Model distinguishes between different types of computing devices.

Type	Description
Computer	A stationary general purpose computing device such as a desktop PC.
Mobile Device	A processing device that is primarily designed to be carried by a user, such as a laptop, smart phone or tablet computer.
Server	A computing device that provides one or more services for consumption by another Computer or User.

Embedded Device	A system that has dedicated purpose software embedded in computer hardware. Embedded Devices often have constrained capabilities which lead to hard limits on process states and data access.
Imaging Device	A device specifically designed to process Imaging Jobs, such as a printer, scanner, or MFD.

Table 5 : Device Types

5. Security Ticket

The PWG Security Ticket is a container that can be used to attach selected Security Attributes to various PWG operations and work objects, such as Jobs and Documents. The PWG Security Ticket provides several collections of security information, organized into three collections, each collection describing the security parameters for each actor involved in a session or transaction. This specification provides an overview of the PWG Security Ticket. More detail information about specific Security Attributes can be found in the “Imaging System Security Identification, Authentication and Authorization” specification [IDS-IAA].

In this specification, the PWG Security Ticket is expressed using an abstract model based on XML Schema and SOAP. Other Protocol Bindings for the PWG Security Ticket are not defined by this document.

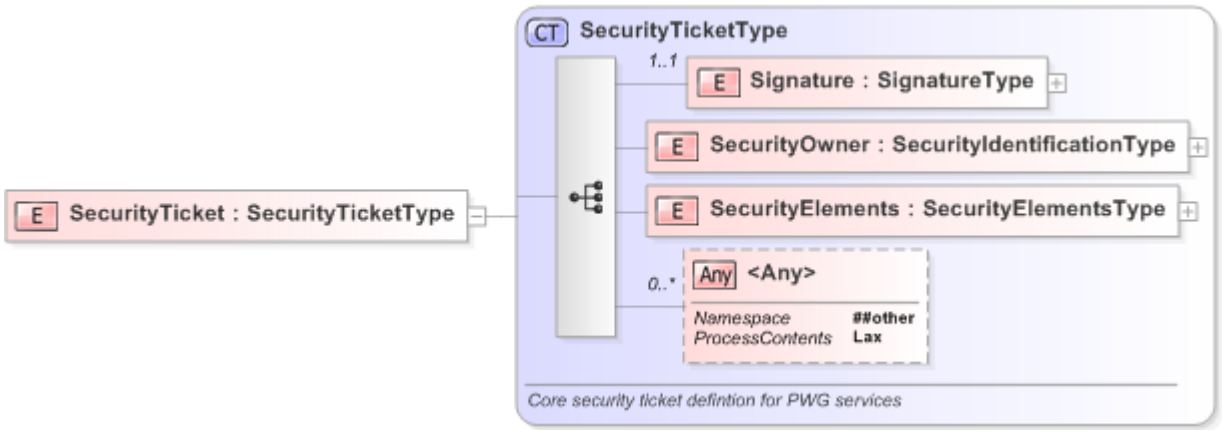


Figure 1: Security Ticket

5.1 Signature

The Signature element provides validation that the Security Ticket has not been compromised. It is an XML signature element as specified in XML signature Syntax and Processing [RFC3275]. Security Owner

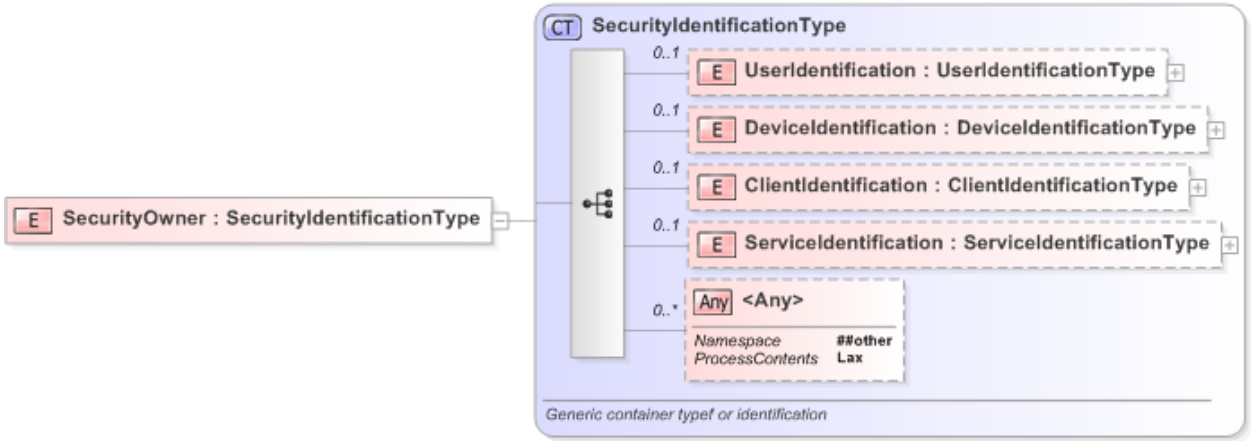


Figure 2: Security Owner

The SecurityOwner element contains Security Identification element for the entity that created the security ticket. The SecurityOwner may consist of multiple Actors in tandem, and thus may be identified by multiple sets of Actor attributes:

User Information about the actual User, such as username, etc.

Device Information about the device currently being used for access

Client Information about any separate client process, application or tool that the User is using

Service Information about any Service being used.

Detailed information about each of these Security Identification elements can be found in IDS Identification, Authentication and Authorization specification [IDS-IAA].

5.2 Security Elements

The document defines a set of common security elements that are used in different contexts. These elements are organized into sets based on Actors.

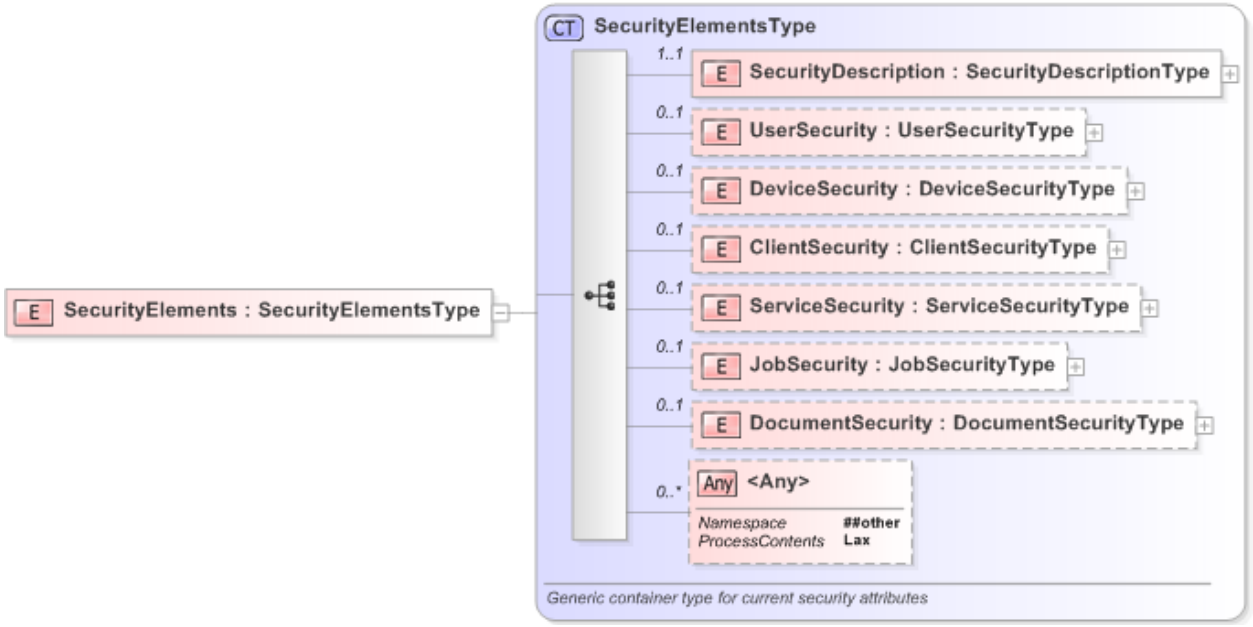


Figure 3: Security Elements

5.2.1 UserSecurity Elements

The UserSecurity element describes the security parameters for a specified User.

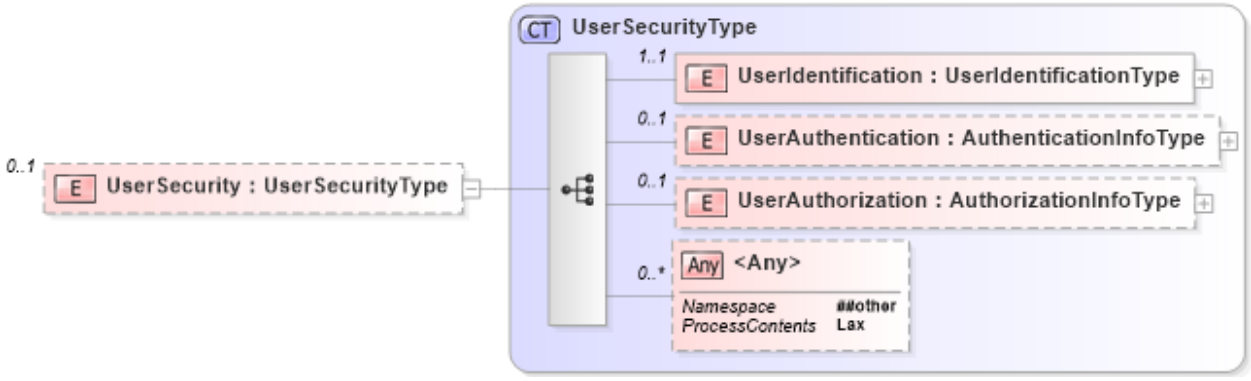


Figure 4: User Security

UserSecurity includes elements to provide information for the Identification, Authentication and Authorization (Access Rights) of the User.

5.2.1.1 UserIdentification

The UserIdentification element is a container for values and attribute that can be used to identify the User. Examples include a User's name, an account name, a User ID, an email address, etc.

519 **5.2.1.2 UserAuthentication**

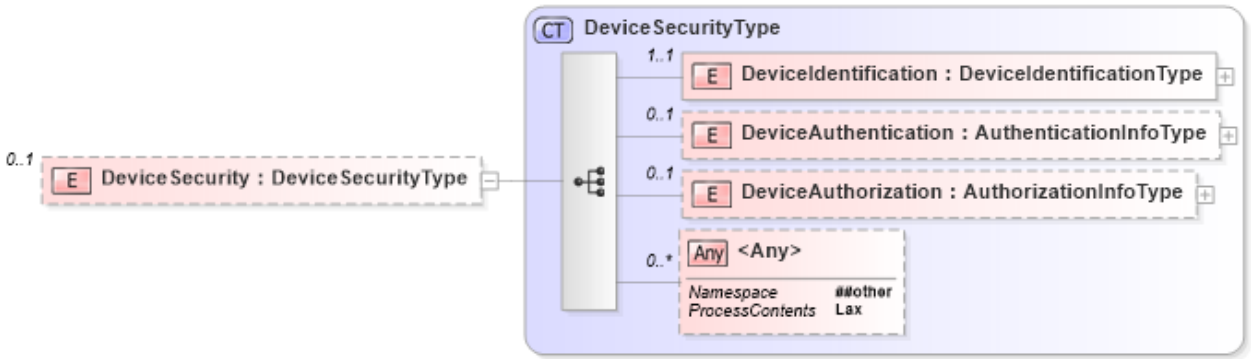
520 The UserAuthentication element contains information that can be combined with
521 corresponding UserIdentification information to prove that the User is who they say they
522 are, such as a password.

523 **5.2.1.3 UserAuthorization**

524 The UserAuthorization element is a container for values and attributes that may be used
525 for authorization decisions, such as the location of the User.
526

527 **5.2.2 DeviceSecurity Elements**

528 The DeviceSecurity element provides the Security Attributes for a particular Device Actor
529 or Object.



530

531 **Figure 5: Device Security**

532 DeviceSecurity includes elements to provide information for the Identification,
533 Authentication and Authorization (Access Rights) of the Device.

534 **5.2.2.1 DeviceIdentification**

535 The DeviceIdentification element is a container for values and attribute that can be used to
536 identify the Device. Examples include the DNS name of a device, the MAC or IPAddress,
537 or a UUID value assigned to the Device.

538 **5.2.2.2 DeviceAuthentication**

539 The DeviceAuthentication element contains information that can be combined with
540 corresponding DeviceIdentification information to confirm the identity of the Device.

541 **5.2.2.3 DeviceAuthorization**

542 The DeviceAuthorization element is a container for values and attributes that may be used
543 for authorization decisions, such as the type or location of a Device.

5.2.3 ClientSecurity Elements

A ClientSecurity element provides the Security Attributes for a particular Client.

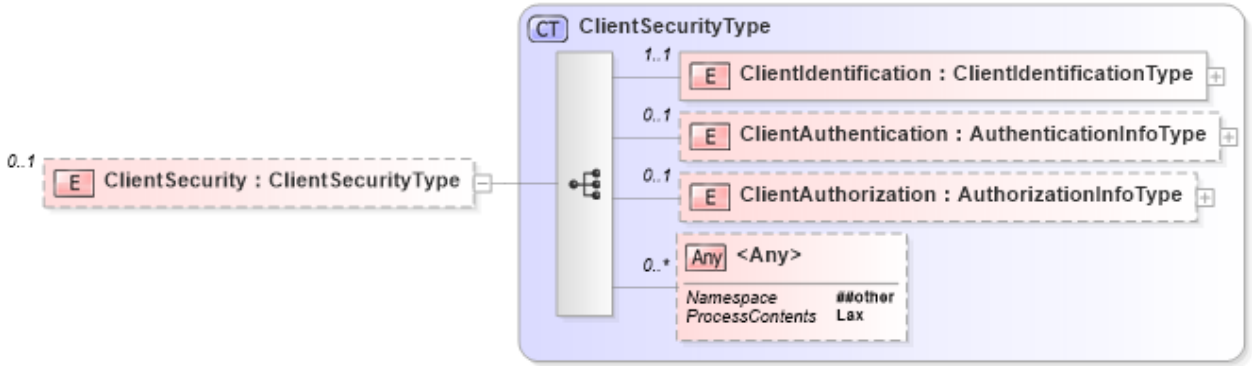


Figure 6: Client Security

ClientSecurity includes elements to provide information for the Identification, Authentication and Authorization (Access Rights) of the Client.

5.2.3.1 ClientIdentification

The ClientIdentification element is a container for values and attribute that can be used to identify the Client, such as a UUID value assigned to the Client.

5.2.3.2 ClientAuthentication

The ClientAuthentication element contains information that can be combined with corresponding ClientIdentification information to validate the Client.

5.2.3.3 ClientAuthorization

The ClientAuthorization element is a container for values and attributes that may be used for authorization decisions, such as the type or location of Client.

5.2.4 ServiceSecurity Elements

A ServiceSecurity element provides the Security Attributes for a particular service actor or object. This Service may be a logical entity on a device such as a Print Service on an MFD, or may be a remote Service such as a Web Service.

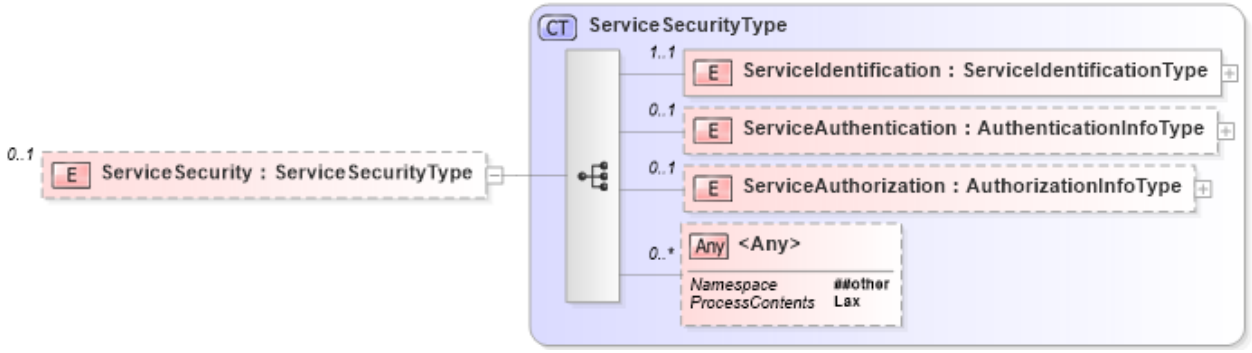


Figure 7: Service Security

ServiceSecurity includes elements to provide information for the Identification, Authentication and Authorization (Access Rights) of the Service.

5.2.4.1 ServiceIdentification

The ServiceIdentification element is a container for values and attribute that can be used to identify the Service, such as a UUID value assigned to the Service.

5.2.4.2 ServiceAuthentication

The ServiceAuthentication element contains information that can be combined with corresponding ServiceIdentification information to validate the Service.

5.2.4.3 ServiceAuthorization

The ServiceAuthorization element is a container for values and attributes that may be used for authorization decisions, such as the type or location of Service.

5.2.5 JobSecurity Elements

The JobSecurity element contains the authentication attributes that control access to the Job information.

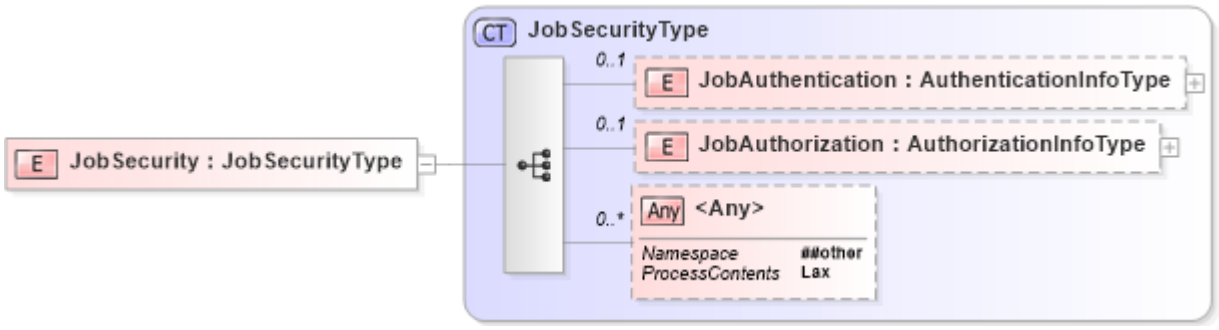


Figure 8: Job Security

JobSecurity includes elements to provide information for the Authentication and Authorization (Access Rights) of the Job.

5.2.5.1 JobAuthentication

The JobAuthentication element contains information to validate the Job, such as a certificate to verify that the Job was created by a trusted User or Client.

5.2.5.2 JobAuthorization

The JobAuthorization element is a container for values and attributes that may be used for authorization decisions, such as the type of Imaging Services allowed to process a job.

5.2.6 DocumentSecurity Elements

The DocumentSecurity element contains the authentication and rights attributes that control access to document content, including encryption access information.

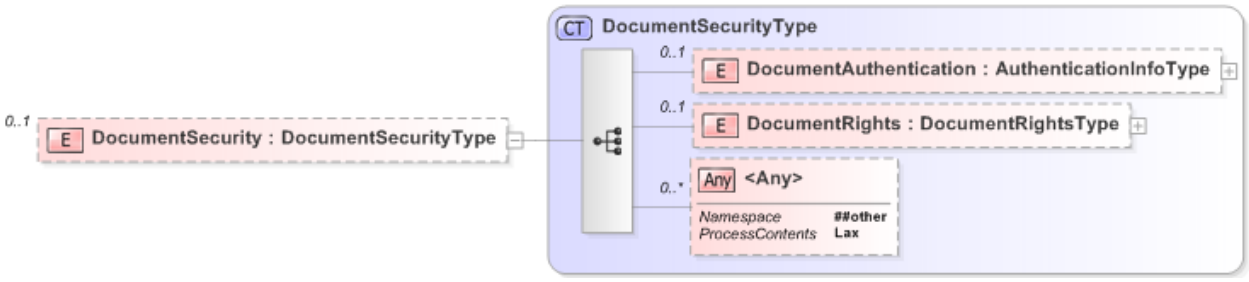


Figure 9: Document Security

DocumentSecurity includes elements to provide information for the Authentication and Authorization (Access Rights) of the document.

5.2.6.1 Document Authentication

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. It may also contain information to verify that the Document was provide by a trusted User, Client or Imaging Service.

5.2.6.2 Document Rights

The DocumentRights element contains the access and usage rights for the user, device or service for a document provided in a document operation such as the UserGroups allowed to print a document

6. Security Operations

It is necessary to facilitate the creation and population of Security Elements and values in a PWG Security Ticket, to be able to determine which Elements and attributes are supported by a particular Actor. The PWG IDS Security Model defines a small set of System level operations to access IDS Security Elements.

6.1 GetServiceElements (SecurityElements)

The GetSecurityElements operation allows a client to obtain a list of available security elements for a specified Actor. GetSecurityElements is a transactional operation and consists of a transaction request and a corresponding transaction response.

The response will contain the current security elements for the requested security identifies and types.

6.1.1 GetSecurityElementsRequest

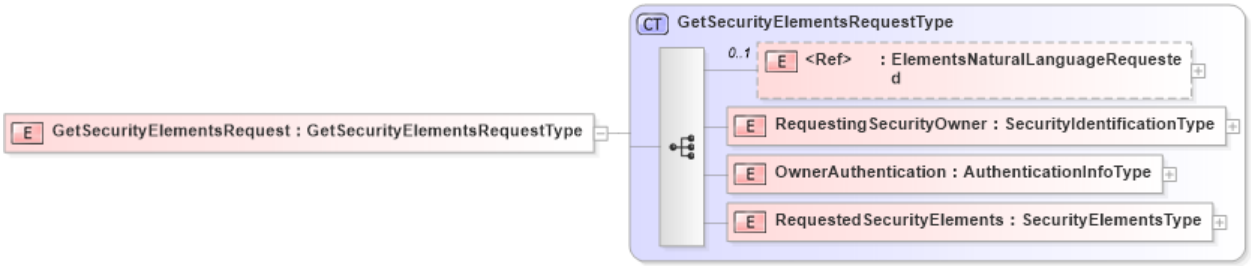


Figure 10: GetSecurityElement Request

The GetSecurityElementsRequest is issued by an Actor to obtain the security element values supported by another Actor.

6.1.1.1 ElementsNaturalLanguageRequested

Specifies the language, where appropriate, that the response values should be provide in

6.1.1.2 RequestingSecurityOwner

This element contains the Identification information for the Actor making the request.

6.1.1.3 RequestingSecurityOwnerAuthentication

This element contains the corresponding authentication information for the Actor making the request.

6.1.1.4 RequestedSecurityElements

Providing a RequestedSecurityElements element allows a requesting Actor to specify which SecurityElements (i.e. UserAuthentication, DeviceSecurity, etc.) it wishes to receive information about…

The request MUST provide at least one SecurityElement containing a valid security identification element, such as UserIdentification, DeviceIdentification or ServiceIdentification, in order to specify the Actor from which additional security information is being requested.
Additional SecurityElements, such as UserAuthentication or UserAuthorization, can be provided in the request to specifiy which information about the Actor is being requested. If no additional Security Elements are provided, that the responding Actor will provide all information on all applicable SecurityElements. The security elements that can be requested vary depending on the Actor to which the request is directed.

6.1.1.4.1 UserSecurity

6.1.1.4.2 DeviceSecurity

6.1.1.4.3 ClientSecurity

6.1.1.4.4 ServiceSecurity

6.1.1.4.5 JobSecurity

6.1.1.4.6 DocumentSecurity

6.1.2 GetSecurityElementsResponse

A GetSecurityElementsResponse is issued by an Actor in response to a GetSecurityElementRequest from another Actor.

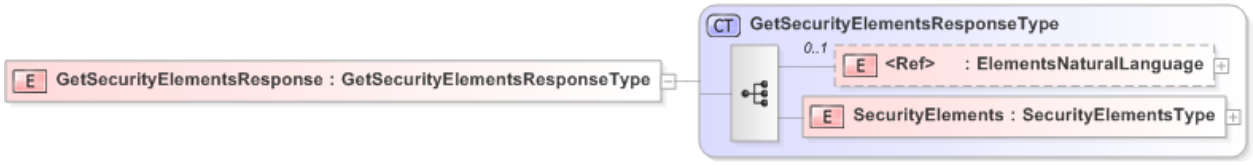


Figure 11: GetSecurityElement Response

6.1.2.1 ElementsNaturalLanguage

Identifies the language, where appropriate, that the response values are provide in

6.1.2.2 SecurityElements

This element contains the security elements and values that are returned by the response. The contents are dependent on which elements are requested, and the Actor to which the requested was directed, and the requesting actor

6.1.2.2.1 UserSecurity

6.1.2.2.2 DeviceSecurity

6.1.2.2.3 ClientSecurity

6.1.2.2.4 ServiceSecurity

6.1.2.2.5 JobSecurity

6.1.2.2.6 DocumentSecurity

6.1.3 GetSecurityElements Operations

Figure 12 : GetSecurityElements Sequence Diagram

7. Alerts and Notifications

In order to keep administrators and security monitoring tools informed, an Imaging System or service MUST be able to provide security and status alerts. In addition to the alerts and messages defined in PWG 5107.3-2012: Printer MIB and IPP MFD Alerts [PWG5107.3] and PWG 5110.3-2013 - PWG Common Log Format [PWG5110.3], Imaging System SHOULD support the alerts listed in the following sections.

7.1 Security Alerts

NOTE: Need to get final values and send registration to IANA

Security Alert	PrtAlertCodeTC Value
securityUserIdentificationError	550
securityUserAuthenticationError	551
securityUserAuthorizationError	552
securityDeviceIdentificationError	560
securityDeviceAuthenticationError	561
securityDeviceAuthorizationError	562
securityServiceIdentificationError	570
securityServiceAuthenticationError	571
securityServiceAuthorizationError	572
securityUnknownEntity	580
securityInvalidAuthenticationService	581
securityInvalidAuthorizationService	582

Table 6: Security Alert Codes

8. Conformance Requirements

Any binding must conform to the PWG Security Schema and must meet the design requirements outlined in 3.4.

9. Conformance Recommendations

9.1 IEEE2600-2008 Conformance

The IEEE2600-2008 standard [IEEE2600] defines security requirements for manufacturers, users, and others in the selection, installation, configuration, and usage of hardcopy devices including Imaging Systems. Imaging Systems SHOULD support the IEEE 2600-2008 standard.

9.2 Imaging System health and network access

In order to support health assurance on such controlled networks, Imaging Systems SHOULD support the Imaging System Security Health Attributes [PWG5110.1] and corresponding Network Access Control protocol bindings such as Network Access Protocol (NAP) [PWG5110.2] and Trusted Network Connection (TNC) [IDS-TNC].

9.3 Audit Log Generation and Availability

Generating audit log records and making them available for review and analysis by Administrators or Auditors are the most basic common security requirements for all Imaging System operational environments. To support the auditing of imaging operations, Imaging Systems SHOULD support the logging requirements as described in PWG Common Log Format [PWG5110.3].

10. 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].

11. Security Considerations

Although security considerations specific to each Imaging Service may be discussed in the specification for the Service Model, the following considerations are generally applicable.

11.1 Protection of End User's Data

An Imaging System receives, creates, and processes a User's Job and Document according to the User's intent configured in their Job and Document tickets. The Job and Document and their associated ticket information may contain sensitive data such as a Document that is classified as top secret, and where the Job and Document is to be routed or stored after completion according to a local security policy. In addition to routing a completed User's Job and Document over the network, User's sensitive Job and Document data may be received over the network from a remote PC or client station. In order to protect User's data stored in an Imaging System or in-transit against disclosure or modification, security measures can be implemented by an Imaging System according to a local site's security policy.

Additionally, an Imaging System SHOULD provide:

- Access Control for on-device Data storage: Any user data stored by the Imaging System, on internal storage or external storage controlled by the Imaging System, can be protected by a minimum of User-level access control.

- Protection of data at rest: Any user data stored by the Imaging System, on internal storage or external storage controlled by a Imaging System, can be encrypted while stored.

- Protection of data in transit: Provide confidentiality of data in transit using an protected end-to-end data path, such as provided by TLS encryption [RFC5246] or by encrypting the data prior to transport.

- Protection of data in use. Decrypted data that is stored in memory but not being actively used is protected.

12. IANA and PWG Considerations

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

Printer MIB alert coded and corresponding state reason in IPP – see 5107.3 for examples

13. References

13.1 Normative References

[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

[RFC2817] R.Khare, S. Lawrence, "Upgrading to TLS Within HTTP/1.1", RFC 2817, May 2000, http://www.ietf.org/rfc/rfc2817.txt

[RFC2911] T. Hastings, R. Herriot, R. deBry, S. Isaacson, P. Powell, "Internet Printing Protocol/1.1: Model and Semantics", RFC 2911, September 2000, http://www.ietf.org/rfc/rfc2911.txt

[RFC3995] T. Hastings, R. Herriot, "Internet Printing Protocol: Event Notifications and Subscriptions ", RFC 3995, March 2005, http://www.ietf.org/rfc/rfc3995.txt

[RFC3805] R. Bergman, H. Lewis, I, McDonald "Printer MIB v2", RFC 3805, March 1997, http://www.ietf.org/rfc/rfc3805.txt

[RFC5246] T.Dierks, E. Rescorla, "Transport Layer Security 1.2", RFC 5246, August 2008, http://www.ietf.org/rfc/rfc5246.txt

[PWG5100.12] R. Bergman, H. Lewis, I. McDonald, M. Sweet, "IPP/2.0 Second Edition", PWG 5100.12-2011, February 2011, ftp://www.pwg.org/pub/pwg/candidates/cs-ipp20-20110214-5100.12.pdf

[PWG5100.14] M. Sweet, I. McDonald, "IPP Everywhere", PWG 5100.14-2013, January 2013, ftp://ftp.pwg.org/pub/pwg/candidates/cs-ippeve10-20130128-5100.14.pdf

[PWG5108.1] W. Wagner, P. Zehler, "MFD Model and Common Semantics", PWG1304 5108.1-2011, April 2011, ftp://ftp.pwg.org/pub/pwg/candidates/cs-sm20-mfdmodel10-20110415-5108.1.pdf

[PWG-CLOUD] W. Wagner, "PWG Cloud Imaging Requirements and Model ", April 2014, http://ftp.pwg.org/pub/pwg/cloud/wd/wd-cloudimagingmodel10-20140418.pdf

[PWG5110.1] J. Murdock, J. Thrasher, PWG 5110.3-2013, "PWG Hardcopy Device Health Assessment Attributes", May, 2014, ftp://ftp.pwg.org/pub/pwg/candidates/cs-idsattributes11-20140529-5110.1.pdf

[PWG5110.2] B. Smithson, J. Murdock, R. Bergman, J. Thrasher, PWG 5110.3-2013, "PWG Hardcopy Device Health Assessment Network Access Protection Protocol Binding", April 2013, ftp://ftp.pwg.org/pub/pwg/candidates/cs-ids-napsoh10-20130401-5110.2.pdf

[PWG5110.3] M. Sweet, PWG 5110.3-2013, "PWG Common Log Format", April 2013, ftp://ftp.pwg.org/pub/pwg/candidates/cs-ids-log10-20130401-5110.3.pdf

[IDS-IAA] J. Murdock, “IDS Identification, Authentication and Authorization specification”, August 2014, ftp://ftp.pwg.org/home/pwg/pub/pwg/ids/wd/wd-ids-iaa10-current.pdf

[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

13.2 Informative References

[RFC4559] K. Jaganathan, L. Zhu, J. Brezak, "SPNEGO-based Kerberos and NTLM HTTP Authentication in Microsoft Windows", RFC 4559, June 2006, http://www.ietf.org/rfc/rfc4559.txt

[OASIS-SOA] OASIS Standard, “OASIS Reference Model for Service Oriented Architecture 1.0”, Oct. 12, 2006, http://docs.oasis-open.org/soa-rm/v1.0/soa-rm.pdf

[OASIS-XACML] eXtensible Access Control Markup Language (XACML) Version 3.0, January 2013, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.pdf

[JAVVIN] Dong, Jielin, “Network Dictionary”, ISBN: 978-1-60267-000-6, March, 2007, http://www.javvin.com/networkdictionary.html

[ECMATR46] ECMA TR/46, “Security in Open Systems – A Security Framework”, July 1988, http://www.ecma-international.org/publications/files/ECMA-TR/TR-046.pdf

[PWG5107.3] PWG 5107.3-2012, "Printer MIB and IPP MFD Alerts", June 2012, ftp://ftp.pwg.org/pub/pwg/candidates/cs-pmpmfdalerts10-20120629-5107.3.pdf

[IEEE2600] IEEE 2600-2008 IEEE Standard for Information Technology: Hardcopy Device and System Security

[IEEE2600.1-2009] IEEE 2600.1-2009 IEEE Standard for a Protection Profile in Operational Environment

[RFC3275] D. Eastlake, J.Reagle, D. Solo, “XML-Signature Syntax and Processing”, RFC3275, March 2002, http://www.ietf.org/rfc/rfc3275.txt

14. 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 - Okidata
Michael Sweet - Apple
Ira McDonald - High North
Bill Wagner - TIC

15. Change History

April 2, 2011

Initial revision.

829 **May 24, 2011**

830 Added Roles, Alerts.

831 Added security considerations, etc.

832 **October 5, 2011**

833 Include Security Alerts from MFD Alerts

834 **April 25, 2012**

835 Updated Use Cases

836 Reformatted Roles and Alerts tables

837 **June 5, 2012**

838 Updated User Roles

839 **August 3, 2012**

840 Editorial Updates

841 Updated missing entries from change history

842 Add terminology and section on visibility

843 Removed Web Services Binding section

844 **October 20, 2013**

845 Rewrote section on visibility

846 Added proposed values for organization, device and service role definitions

847 **February 5, 2014**

848 Converted to new PWG template

849 **February 28, 2014**

850 Simplified document objective and moved IAA details to IAA document

851 **April 10, 2014**

852 Made changes requested from last review. Cleaned up and reorganized.

853 **May 10, 2014**

Made changes requested from last review. Added Client actor. Added Device as an object. Added new Types section. Updated all schema diagrams to match latest schema changes. Removed old Security Consideration section and moved parts into Conformance Requirements. Added missing Normative references. Added JobSecurity element

July 10, 2014

Made changes requested from last review. Updated schema diagrams to match latest schema changes. Change SecurityId to SecurityOwner in the SecurtyTicket

July 28, 2014

Made changes requested from conference call review.

August 04, 2014

- Made changes requested from conference call review.
- Added Security operations
- Added Document security section
- Moved Identification detail back to the IAA specification
- Updated all schema diagrams to match latest schema changes.
- Added missing normative references.
- Filled in text description in several sections

November 1, 2014

- Made changes requested from F2F review.
- Merged Service Roles into Service Type and updated schema to match
- Updated all schema diagrams to ones generated by Liquid XML for consistencey with PWG specifications.
- Filled in text description in several sections
- Added references to RFC3995, RFC3275 and PWG Schema

February 02, 2015

- Reorganized Terminology section in alphabetical order
- Address F2F review comments

881 **April 26, 2015**

882 • Address F2F review comments

