Physical Security Interoperability Alliance

Core PSI Model

Specification Version 1.0
Revision 0.7
15 December 2008

Revision History	Description	Date	By
Version 1.0 Rev 0.1	Initial Draft	June 17, 2008	Frank Yeh
Version 1.0 Rev 0.2	Updates as agreed at June 20 F2F	July 11, 2008	Frank Yeh
Version 1.0 Rev 0.3	Updated with IP Video Use Case Details	August 8, 2008	Frank Yeh
Version 1.0 Rev 0.4	Updated for IP Video Use Case 002	August 30, 2008	Frank Yeh
Version 1.0 Rev 0.5	Added section for Standards Bodies & Organizations, Protocols section to Use Case Template	November 12, 2008	Frank Yeh
Version 1.0 Rev 0.6	Expanded Bindings and Statuses entries in Glossary	December 5, 2008	Frank Yeh
Version 1.0 Rev 0.7	Added Entities Diagram	December 15, 2008	Frank Yeh

Disclaimer
THIS SPECIFICATION IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Without limitation, PSIA disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification and to the implementation of this specification, and PSIA disclaims all liability for cost of procurement of substitute goods or services, lost profits, loss of use, loss of data or any incidental, consequential, direct, indirect, or special damages, whether under contract, tort, warranty or otherwise, arising in any way out of use or reliance upon this specification or any information herein.
No license, express or implied, by estoppel or otherwise, to any PSIA or PSIA member intellectual property rights is granted herein.
Except that a license is hereby granted by PSIA to copy and reproduce this specification for internal use only.

Contact the Physical Security Interoperability Aliance at <insert email> for information on specification licensing through membership agreements.

Any marks and brands contained herein are the property of their respective owners.

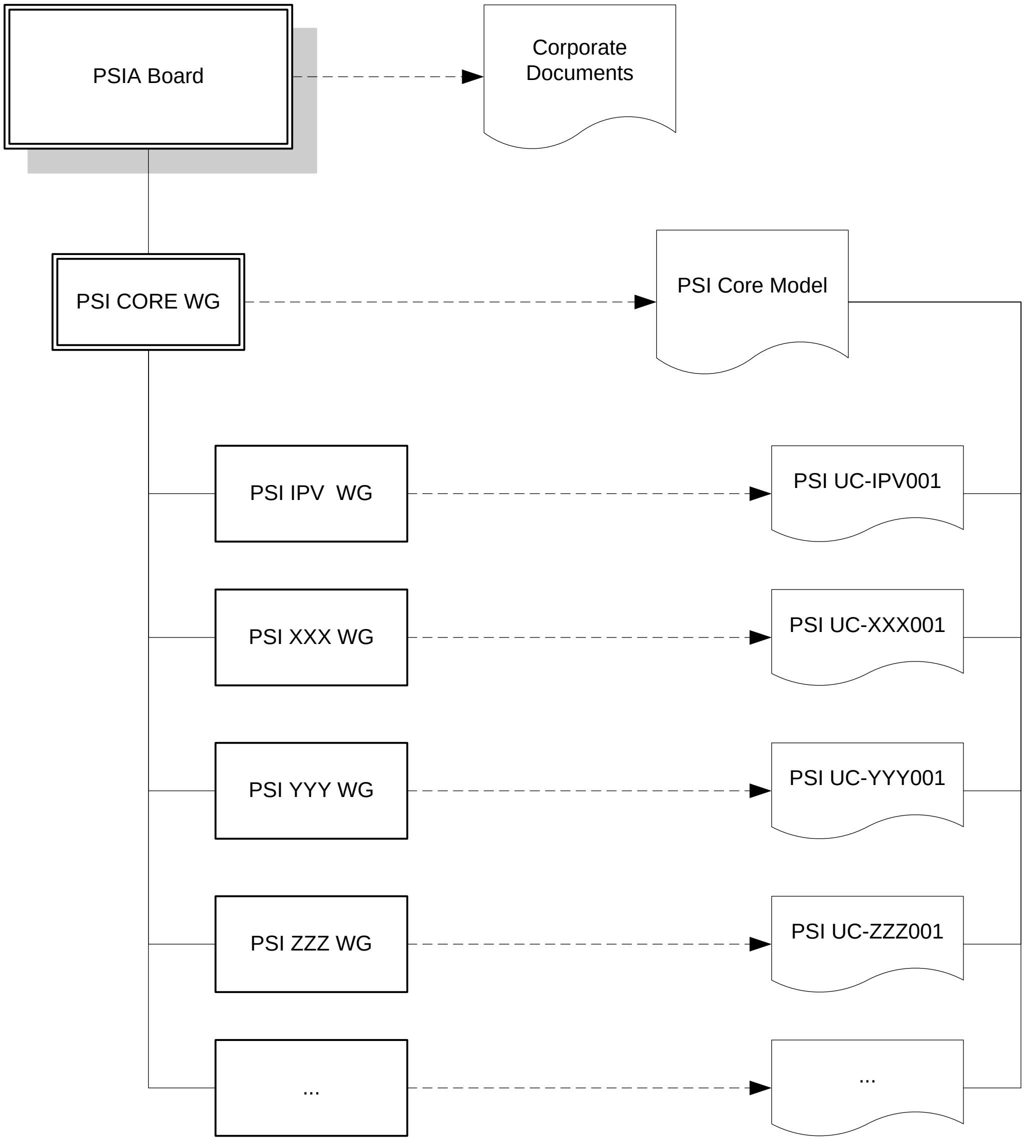


Figure 1: PSIA Document Roadmap

1 Scope and Audience

The Physical Security Interoperability Alliance is working to define and promote an open model that enables vendors, consortiums, and standards bodies to position their particular specifications and protocols within a broad architecture designed to describe Physical Security offerings enabled by Internetworking and Information Technologies.

Architects, designers, developers and technologists who are interested in the development, deployment, and interoperation of such Physical Security systems may find this document helpful in understanding the Model and Architecture defined by the PSIA to support interoperation of the available specifications and protocols.

2 Introduction

The PSI Model focuses on the integration of complex solutions in which technology from various vendors representing different markets is combined using modern networking and information technologies. While each of the various offerings and market spaces typically have their own set of protocols (standard or proprietary), the use of any of these protocols within a hybrid solution must be performed so that it can interoperate or at least peacefully co-exist with the other protocols in the solution. The market is starting to demand interoperability within these solutions. As demonstrated by the internetworking and information technologies, strong and open standards are crucial to developing and deploying such solutions cost-effectively and with a low total cost of ownership.

2.1 Physical Security Interoperability: Background

The growth of the Internet IP infrastructure in the last decade has introduced new technologies, new opportunities, and new challenges. The traditional physical security market was characterized by proprietary protocols, vendor lock-in strategies, and stovepipe solutions. In contrast, the internetworking and information technology markets have experienced phenomenal growth enabled by open standards and implicit guarantees of interoperability. Recent trends show that the physical security market is experiencing a wave of migrations to digital, information, networking technologies to leverage many of the cost of ownership advantages created by this new culture. This migration has created a culture clash between the open standards camp and the proprietary protocols camp.

While there are some advantages to proprietary protocols, most of them are vendor-specific and do nothing towards the growth of the market as a whole. The desire of vendors, customers and integrators to make the physical security market more of an information market demonstrates that the total cost of ownership will be lower for all if this market embraces open standards and interoperability.

2.2 Aim and Purposes

The aim of the PSI Model is to provide a framework within which usage of specifications can be described from the perspective of the architect or integrator. Readers of the model should be able to quickly identify the functions that they wish to implement, the Use Cases that describe the desired implementation, a Sequence of Events which the use cases execute, and a description of the relevant protocols for each Event.

3 The PSI Model

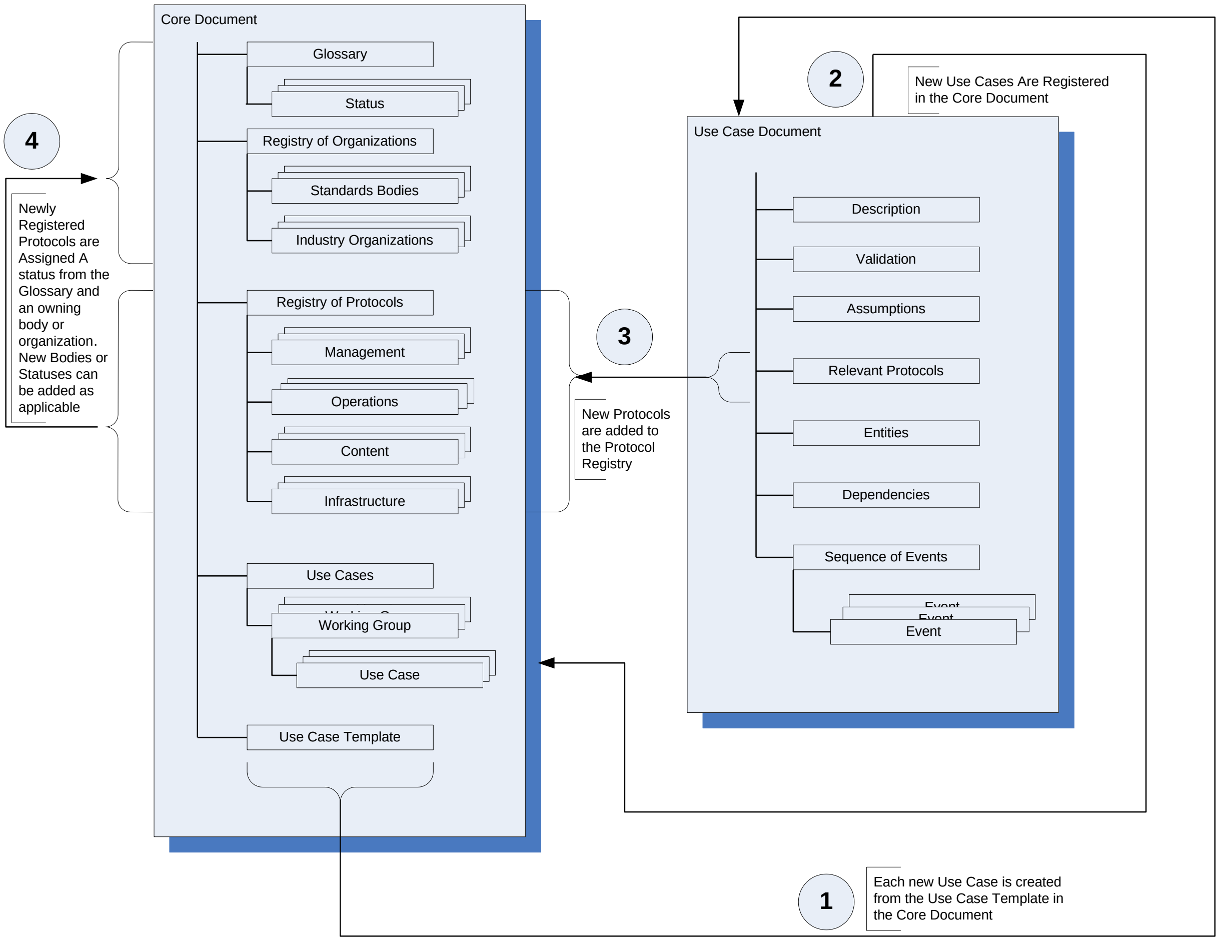
The PSI Model is described at two separate levels_ the Core Model, and the Use Cases. The Core Model includes subsections for a Glossary of Terminology, a Registry of Protocols and Specifications, and a Use Case Template to expedite the creation of new use cases.

Each Use Case will contain a functional summary or description of the use case, a list and description of the Entities involved in the use case, and a Sequence of Events that describes the chronology in which the various bindings are established or terminated.

As indicated in Figure 1 above, the Document Hierarchy of the PSIA will closely reflect the organizational structure as each organizational unit of the PSIA will own and maintain a specific set of documents. The PSIA Board will create, own, and maintain the corporate documents. The PSIA Core Working Group will create, own and maintain the PSI Core Model. As various functional areas come into focus, expert working groups will be formed to create Use Case documents for their specific Use Case.

Each PSIA Document will be assigned a life cycle state that reflects its maturity and status. As the document reaches maturity, it will transition between these states. These life cycles states are described in the Use case Section of this document but it should be noted that they also apply to this document.

3.1 PSI Core Document Model



Core Document
Glossary
Status
Registry of Organizations
Standards Bodies
Industry Organizations
Registry of Protocols
Management
Operations
Content
Infrastructure
Use Cases
Working Group
Use Case
Use Case Template
4
Newly Registered Protocols are Assigned A status from the Glossary and an owning body or organization. New Bodies or Statuses can be added as applicable
3
New Protocols are added to the Protocol Registry
2
New Use Cases Are Registered in the Core Document
Use Case Document
Description
Validation
Assumptions
Relevant Protocols
Entities
Dependencies
Sequence of Events
Event
Event
Event
1
Each new Use Case is created from the Use Case Template in the Core Document

Figure 2: PSIA Core Document Model

The PSI Core model describes the structure of the PSI Use Cases, defines Functional Categories, and provides a header document that can be updated to include the various Use Cases as they are developed.

The PSI Document Model defines the following entities and relationships.

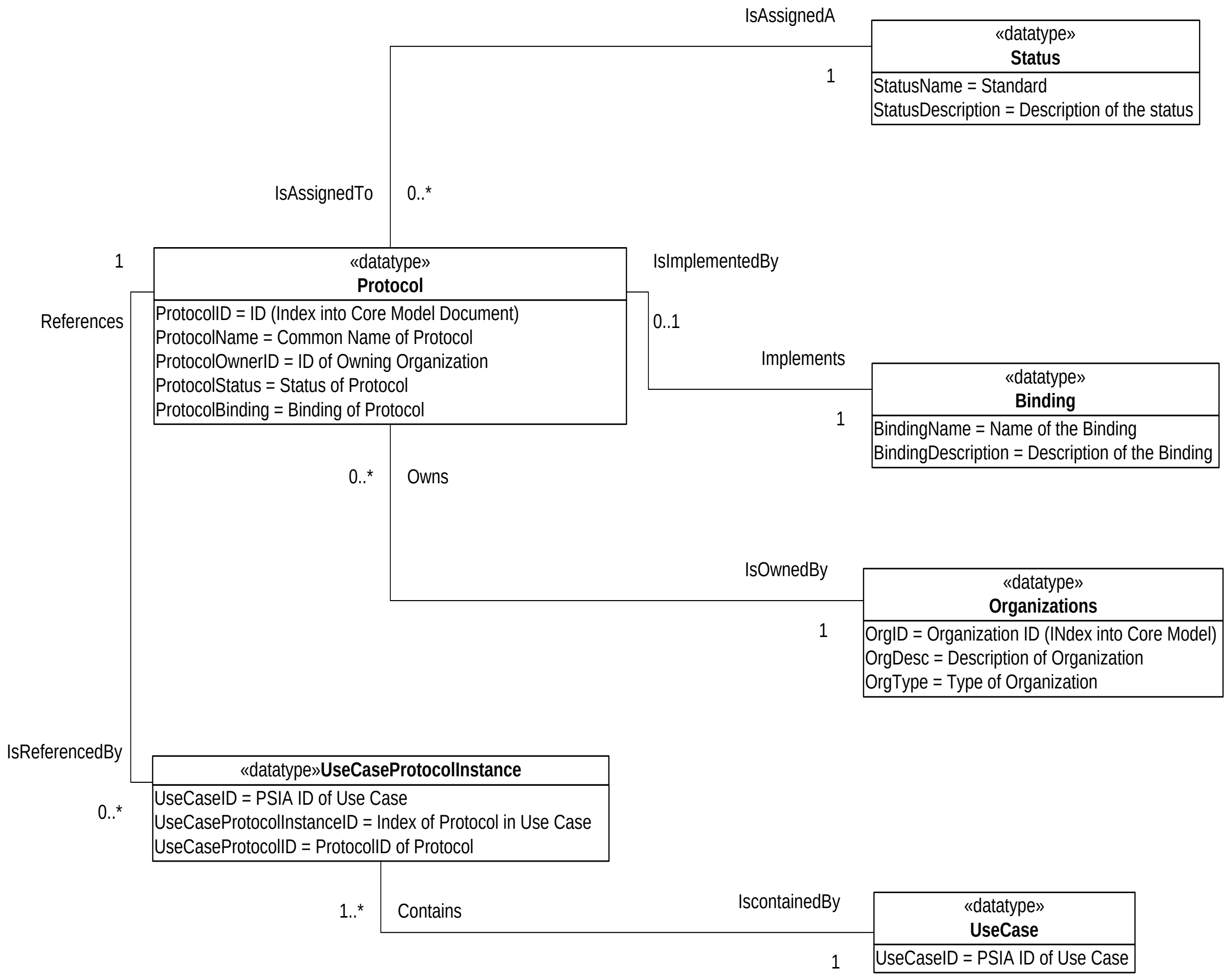

IsAssignedA
«datatype»
Status
1
StatusName = Standard
StatusDescription = Description of the status
IsAssignedTo
0..*
1
«datatype»
Protocol
IsImplementedBy
References
ProtocolID = ID (Index into Core Model Document)
ProtocolName = Common Name of Protocol
ProtocolOwnerID = ID of Owning Organization
ProtocolStatus = Status of Protocol
ProtocolBinding = Binding of Protocol
0..1
Implements
«datatype»
Binding
1
BindingName = Name of the Binding
BindingDescription = Description of the Binding
0..*
Owns
IsOwnedBy
«datatype»
Organizations
1
OrgID = Organization ID (INdex into Core Model)
OrgDesc = Description of Organization
OrgType = Type of Organization
IsReferencedBy
«datatype»UseCaseProtocolInstance
0..*
UseCaseID = PSIA ID of Use Case
UseCaseProtocolInstanceID = Index of Protocol in Use Case
UseCaseProtocolID = ProtocolID of Protocol
1..*
Contains
IscontainedBy
«datatype»
UseCase
1
UseCaseID = PSIA ID of Use Case

Figure 3: Core Model Entities & Relationships

3.1.1 Glossary

3.1.1.1 Protocol

In computing, a protocol is a convention or standard that controls or enables the connection, communication, and data transfer between two computing endpoints. In its simplest form, a protocol can be defined as the rules governing the syntax, semantics, and synchronization of communication. Protocols may be implemented by hardware, software, or a combination of the two. At the lowest level, a protocol defines the behavior of a hardware connection.

3.1.1.2 Binding

A Binding describes the application of a protocol as a connection between two endpoints. In the context of interoperability standards, bindings have been a major point of contention. In essence, any protocol may be broken down into the schema portion, which defines the content and structure of the data to be exchanged, and the binding portion, which sets certain expectations as to how endpoints will encapsulate the data for transport over the network. The receiver of the encapsulated data must understand the binding in order to de-encapsulate the data.

Major Bindings of interest today include REST, SOAP, XML-RPC, and MIME.

3.1.1.3 Standard

A standard is a protocol that has been published by an acknowledged standard body (EG IETF, IEEE, ISO, IEC, NIST, and others) and is openly accessible to anyone without a fee. Standards fall into several categories such as Open Standards, De-Facto Standards, and Industry Standards.

3.1.1.4 Specification

A specification is the actual technical definition for a protocol. It contains all of the technical information for someone to actually implement a protocol.

3.1.1.5 Status

Each Protocol is assigned a status that describes its state in the protocol life cycle. Current status definitions are:

Proposed	Someone has stated the need for a standard
Draft	Someone has started writing up a protocol
Private Review	Closed team of SME's is reviewing protocol
Public Review	Review period open to public
Pre-Standard	Endorsed by Reviewers but not yet a standard

3.1.1.6 Proof Point

Each PSIA Use Case must include a definitive sequence of events. Included within this sequence may be bindings or user actions that must be completed in order to progress through the sequence. Proof points will be provided as methods to test individual bindings or actions as successful within the entire sequence. Proof Points are provided as a pseudo-checklist for deployments and as a debugging and troubleshooting aid.

3.1.1.7 Conversion

Conversion protocols are used to convert content between analog and digital states. Conversion is used to capture the state of various physical inputs such as video, audio, and electrical impulses as digital information that can be stored or transported and subsequently converted back to analog form, thus reproducing the original captured state.

3.1.1.8 Transcoding

Transcoding includes both encoding and decoding of digital content between various formats. Transcoding supports compression, time correction, and other application-specific functions.

3.1.1.9 Encapsulation

Encapsulation is the use of one protocol to transport another. Within today's complex internetworking environments, application content is typically encapsulated using various protocols to support differentiation between content types on an endpoint, different endpoints on a subnet, different subnets in a domain, and different domains on the internet.

3.1.2 Registry of Organizations

The Registry of Organizations is subdivided into an enumeration of recognized standards bodies and one of organizations that are performing work relevant to physical security interoperability

Each organization listed herein is either a recognized standards body capable of publishing true open standards with global scope, or an entity that is involved in developing specifications/protocols that are relevant to physical security and referenced in one of the PSI Use Cases.

In addition to providing a description of the organization as to its scope and purpose, the relevance of the organization to specific PSIA Working Groups should be noted.

3.1.2.1 Standards Bodies

3.1.2.1.1 Internet Engineering Task Force (IETF)

www.ietf.org

The Internet Engineering Task Force (IETF) develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standard bodies and dealing in particular with standards of the TCP/IP and Internet protocol suite. It is an open standards organization, with no formal membership or membership requirements. All participants and leaders are volunteers.

The IETF model for developing specifications is the fundamental to the PSIA's processes. Since the PSIA's mission is to promote and accelerate standards, the IETF is one body that could become the eventual publisher of work supported by PSIA.

3.1.2.1.2 IEEE

www.ieee.org

The IEEE name was originally an acronym for the Institute of Electrical and Electronics Engineers, Inc. Today, the organization's scope of interest has expanded into so many related fields, that it is simply referred to by the letters I-E-E-E

The IEEE Standards Association (IEEE-SA) is a leading developer of industry standards in a broad-range of industries. Globally recognized, the IEEE-SA has strategic relationships with the IEC, ISO, and the ITU and satisfies all SDO requirements set by the World Trade Organization, offering more paths to international standardization.

3.1.2.1.3 American National Standards Institute (ANSI)

www.ansi.org

ANSI facilitates the development of American National Standards (ANS) by accrediting the procedures of standards developing organizations (SDOs). These groups work cooperatively to develop voluntary national consensus standards.

Accreditation by ANSI signifies that the procedures used by the standards body in connection with the development of American National Standards meet the Institute's essential requirements for openness, balance, consensus and due process.

3.1.2.1.4 International Organization for Standardization (ISO)

www.iso.org

ISO, the world's largest developer and publisher of International Standards, is a network of the national standards institutes of 157 countries, one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system.

3.1.2.1.5 International Telecommunication Union (ITU)

http://www.itu.int/ITU-T/

ITU's role as creator of the world's most universally-recognized infocommunications standards dates back as far as the organization itself. Since its inception in 1865, the Union has been brokering industry consensus on the technologies and services that form the backbone of the world's largest, most interconnected man-made system. In 2007 alone, ITU's Telecommunication Standardization Sector (ITU-T) produced over 160 new and revised standards (ITU-T Recommendations), covering everything from core network functionality and broadband to next-generation services like IPTV.

3.1.2.2 Organizations

3.1.2.2.1 Joint Photographic Experts Group (JPEG)

http://www.jpeg.org/committee.html

This group is actually a working group established by ISO and ITU-T. Its focus is in defining specifications used in the compression of still images.

The Motion JPEG (MJPEG)and JPEG2000 protocols developed by JPEG are used extensively to compress digital video. These specifications are relevant to the IP Video Working Group

3.1.2.2.2 Moving Picture Experts Group (MPEG)

http://www.chiariglione.org/mpeg/

MPEG is a working group of ISO/IEC charged with the development of video and audio encoding standards.

MPEG-4 is the most commonly used MPEG specification for transporting digital video

These specifications are relevant to the IP Video Working Group

3.1.2.2.3 Security Industry Association (SIA)

https://www.siaonline.org/index.html

SIA is a nonprofit international trade association representing electronic and physical security product manufacturers, specifiers, and service providers.

SIA promotes growth and professionalism within the security industry by providing education, research, technical standards and representation and defense of its members' interests.

SIA is an ANSI-approved Standards Development Organization. As such, SIA leads the development of systems integration and equipment performance standards. Standards staff also serves in an external liaison capacity, partnering with federal agencies, law enforcement, and other related associations to develop and advance standards.

3.1.2.2.4 Organization for the Advancement of Structured Information Standards (OASIS)

http://www.oasis-open.org/home/index.php

OASIS is a not-for-profit consortium that drives the development, convergence and adoption of open standards for the global information society. The consortium produces more Web services standards than any other organization along with standards for security, e-business, and standardization efforts in the public sector and for application-specific markets.

OASIS is distinguished by its transparent governance and operating procedures. Members themselves set the OASIS technical agenda, using a lightweight process expressly designed to promote industry consensus and unite disparate efforts. Consortium leadership is based on individual merit and is not tied to financial contribution, corporate standing, or special appointment.

3.1.2.2.5 Association for Retail Technology Standards (ARTS)

http://www.nrf-arts.org/

The Association for Retail Technology Standards (ARTS) of the National Retail Federation is a retailer-driven membership organization dedicated to creating an open environment where both retailers and technology vendors work together to create international retail technology standards.

ARTS is a separate council within the NRF governed by a council of retailers and technology solution providers.

These specifications are relevant to the Video Analytics Working Group

3.1.2.2.6 Open Network Video Interface Forum (ONVIF)

http://www.onvif.org/

ONVIF is an open industry forum for the development of a global standard for the interface of network video products.

ONVIF was established in 2008 by Sony, Axis and Bosch, who jointly represent a large segment of the IP Video camera market segment.

ONVIF has created and demonstrated a specification for interoperability of IP Video cameras and the three founding members delivered an interoperability at the Essen Show in October 2008.

ONVIF's first open meeting is scheduled for December 3-4 2008 and on the agenda are a presentation of the technical specification and a walkthrough of the architecture, web services, and tools.

ONVIF has posted version 1.0 of their IP Video specification and stated that they will accept suggestions to the specification. At this time the process for review of suggestions and possible incorporation into the spec is unclear.

The ONVIF specification is expected to relate to the work of the PSIA IP Video Working Group.

3.1.3 Registry of Protocols

Protocols are described within one of four functional categories_ Management, Operations, Content, and Infrastructure. Each of these categories is further desctribed in its own section below.

This Registry will not describe the protocols in extreme detail as most of the required knowledge is already published by the respective standards groups of the respective technologies. Rather, the protocol will be described with regards to standards (EG IETF or IEE Standard, Industry Standard, Open Specification, Proprietary, etc) and standards bodies, and ownership. Hyperlinks to information or entities related to each protocol should also be included in the Registry.

3.1.3.1 Management Protocols

This functional category includes any operations that set or modify a device configuration. Typical actions to be performed in this category are device registration, device configuration, software or firmware updates, and Device query.

3.1.3.1.1	**Simple Network Management Protocol (SNMP)**	SNMP is used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. It consists of a set of standards for network management, including an Application Layer protocol, a database schema, and a set of data objects. SNMP exposes management data in the form of variables on the managed systems, which describe the system configuration. These variables can then be queried (and sometimes set) by managing applications.
Status	**Ownership**	IETF
Standard	**Specification**	RFC 3411–RFC 3418
	Links	http://tools.ietf.org/html/rfc3411

3.1.3.1.2	**IP Media Device API**	IPMDAPI is a pre-standard protocol contributed to the public domain by Cisco Systems. It is currently under review by the PSIA's IP Video Expert Working Group
Status	**Ownership**	While in Public Review, the working document is maintained by the PSIA IP Video Working Group.
Pre Standard	**Specification**	IPMDAPI v1.0
	Links	www.psialliance.org

3.1.3.1.3	ZeroConf	Zero Configuration Networking is a working group of the IETF that was formed to simplify the attachment of devices to a network. The group identified four main requirements: • Allocate addresses without a DHCP server (IPv4 Link-Local Addressing) • Translate between names and IP addresses without a DNS server (Multicast DNS) • Find services, like printers, without a directory server (DNS Service Discovery) • Allocate IP Multicast addresses without a MADCAP server (future work) The first spec, Dynamic Configuration of IPV4 Link Local Addresses was published as RFC 3927. While Zeroconf delivers several similar functions to UPnP and Bonjour, it is preferred by many to avoid licensing and brand implications that can be issues when dealing with UPnP or Bonjour.
Status	**Ownership**	IETF Zeroconf Working Group
Standard	**Specification**	See Links
	Links	http://www.zeroconf.org/

3.1.3.1.4	Universal Plug & Play (UPnP)	The UPnP™ Forum is an industry initiative designed to enable simple and robust connectivity among consumer electronics, intelligent appliances and mobile devices from many different vendors. Major functional areas of the UPnP Device Architecture include addressing, Discovery, Description, Control, and Eventing.
Status	**Ownership**	UPnP Forum
Industry Standard	**Specification**	See Links
	Links	http://www.upnp.org/standardizeddcps/default.asp

3.1.3.1.5	**Bonjour**	Bonjour is considered by many to be Apple’s implementation of Zero Configuration Networking. Apple’s Web Site says: “Bonjour, also known as zero-configuration networking, enables automatic discovery of computers, devices, and services on IP networks. Bonjour uses industry standard IP protocols to allow devices to automatically discover each other without the need to enter IP addresses or configure DNS servers. Specifically, Bonjour enables automatic IP address assignment without a DHCP server, name to address translation without a DNS server, and service discovery without a directory server. Bonjour is an open protocol which Apple has submitted to the IETF as part of the ongoing standards-creation process.” This description is extremely similar to the description of ZeroConf which can cause some confusion. For most purposes, Bonjour and Zeroconf can be used interchangeably. The major differentiation is that Bonjour implementations tend to display an Apple logo during startup, which is unacceptable to some other vendors.
Status	**Ownership**	Apple
Industry Standard	**Specification**	See Links
	Links	http://developer.apple.com/networking/bonjour/specs.html

3.1.3.2 Operational Protocols

This functional category involves (near) real-time user or automated operational control of devices. Typical actions include Pan/Tilt/Zoom control of cameras and on demand data requests from sensors or telemetry devices.

3.1.3.2.1	**Real Time Streaming Protocol (RTSP)**	RTSP is a protocol for use in streaming media systems which allows a client to remotely control a streaming media server, issuing VCR-like commands such as "play" and "pause", and allowing time-based access to files on a server. The sending of streaming data itself is not part of the RTSP protocol.
Status	**Ownership**	IETF
Standard	**Specification**	RFC 2326

	Links	http://tools.ietf.org/html/rfc2326

3.1.3.3 Content Protocols

This functional category is how the actual content that is interesting to the user or application is encoded and transferred over the network.

3.1.3.3.1	**Real-time Transport Protocol (RTP)**	RTP defines a standardized packet format for delivering audio and video over the Internet.
Status	**Ownership**	IETF
Standard	**Specification**	RFC 1889
	Links	http://tools.ietf.org/html/rfc2326

3.1.3.3.2	**Motion JPEG (MJPEG)**	MJPEG is an informal name for multimedia formats where each video frame or interlaced field of a digital video sequence is separately compressed as a JPEG image. The name "JPEG" stands for Joint Photographic Experts Group, the name of the committee that created the standard.
Status	**Ownership**	JPEG
Standard	**Specification**	ISO 10918-1
	Links	http://en.wikipedia.org/wiki/Motion_JPEG

3.1.3.3.3	**MPEG4**	MPEG-4 is a collection of methods defining compression of audio and visual (AV) digital data. It was introduced in late 1998 and designated a standard for a group of audio and video coding formats and related technology.
Status	**Ownership**	ISO/IEC Moving Picture Experts Group (MPEG)
Standard	**Specification**	ISO/IEC 14496
	Links	http://en.wikipedia.org/wiki/Mpeg-4

3.1.3.3.4	**HTTP Push**	Actually describes part of the HTTP Protocol. A special MIME type (multipart/x-mixed-replace) was added to describe documents with changing content. Using this type, browsers will expect the server to continue to push updates to the document with each update overwriting the previous. The key is that the connection is left open,

		which makes the transmission of content much more efficient. HTTP Push has the advantage of being a TCP protocol (where RTP is a UDP protocol) which means that it is less sensitive to network problems, etc. In contexts where the video is being recorded (as opposed to being viewed in real time) retransmission of dropped packets can be accommodated without losing the time index of the frame with respect to the entire video. In realtime viewing scenarios, once a frame has been dropped, it is not retransmitted but simply ignored. This is more appropriate for a UDP protocol.
Status	**Ownership**	ISO/IEC Moving Picture Experts Group (MPEG)

3.1.3.4 Infrastructure Protocols

This functional category involves any interoperation with the supporting infrastructure (EG Computers, Networks, Databases) by the solution.

3.1.3.4.1	**Session Initiation Protocol (SIP)**	SIP is a signalling protocol, widely used for setting up and tearing down multimedia communication sessions such as voice and video calls over the Internet. Other feasible application examples include video conferencing, streaming multimedia distribution, instant messaging, presence information and online games. In November 2000, SIP was accepted as a 3GPP signaling protocol and permanent element of the IMS architecture for IP based streaming multimedia services in cellular systems. The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions consisting of one or several media streams. The modification can involve changing addresses or ports, inviting more participants, adding or deleting media streams, etc.
Status	**Ownership**	IETF

Standard	**Specification**	RFC 3261
	Links	http://tools.ietf.org/html/rfc3261

3.2 PSI Use Cases

Each PSI Use Case will have a Working Group assigned to create and maintain it. Use Cases MUST contain each of the following sections:

3.2.1 Use Case Entities

Any entity that participates in a Use Case should be enumerated in this section. In addition to a basic identifier, a description of the entity should be provided.

3.2.2 Use Case Sequence of Events

All of the steps within the Use Case should be described in chronological order in this section. Each event in the sequence should describe a binding and the entities at the endpoints of the binding.

3.2.3 Use Case Life Cycle

The following states should be assigned to every PSIA document. In addition to a description of the maturity of the document, the life cycle state also has relevance as to who is allowed to view, comment, or contribute to a document.

The document numbering convention for documents will require that documents that are not yet in the Public Review state have a 0.x version number. Once the document has passed internal review, it will be posted for public review as version 1.0. Subsequent changes to the document based on public feedback will be numbered in the 1.x range.

State	Description
Requested	PSIA Members have voted to create a document but the initial draft has not been created yet. While in this state, the working group to create the document must be formed or identified and the initial author(s) assigned to create the first draft.
Draft	A draft version of the document has been posted for review by the authors.
Internal Review	The relevant PSIA Working Group can access the document and submit additions, changes, or deletions.
Public Review	Anyone registered with PSIA can read the document and submit comments to the PSIA working group.
Pre-Standard	Waiting to be published by an acknowledged standards body

3.2.4 Use Cases

Category	Description	Document ID	Status
IP Video	Basic	PSI-UC-IPV001	Public Review

4 Use Case Template

This section is a template to be used in the creation of new Use Case Documents

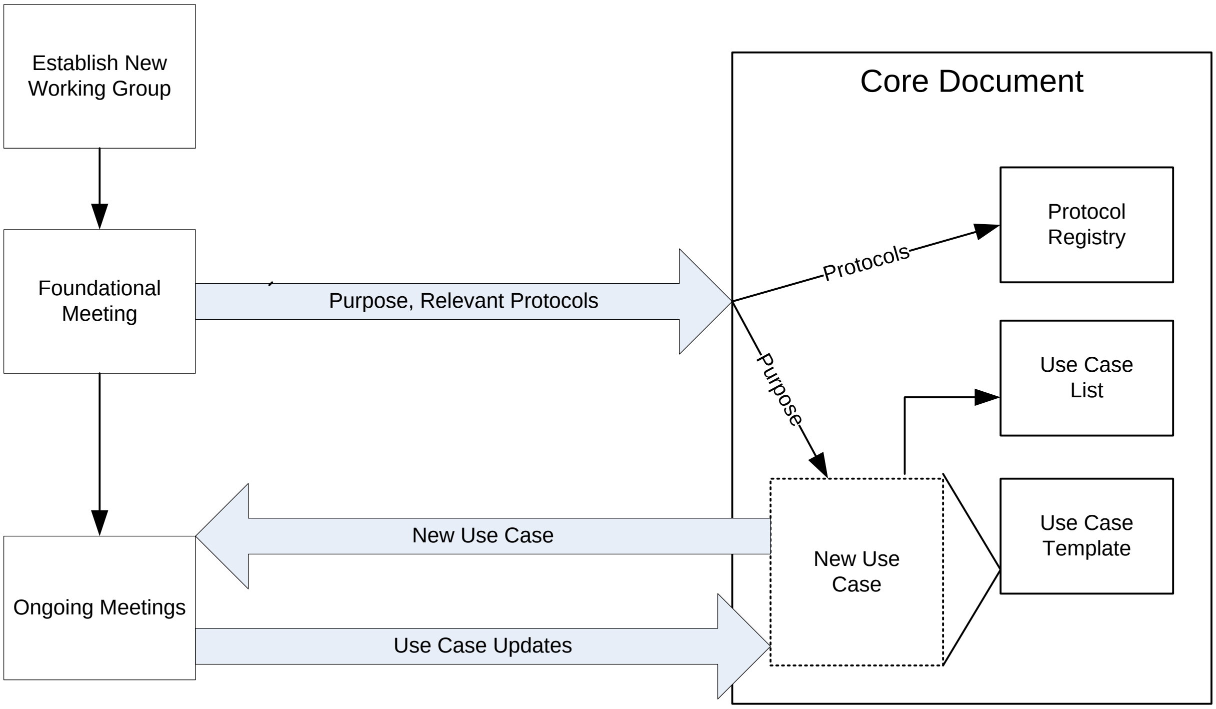


Figure 4: Creating a new Use Case

1. Description

Provide a description of the use case and the fundamental value it provides to the user.

EG: The IP Video Use case applies to any device that provides streaming digital video over an IP network. The use case applies to all events necessary to connect to such devices over the network, request streaming content from these devices, and view the requested content. This use case applies to the simplest scenario, and should be useful in lab and demonstration scenarios.

2. Validation

Provide a Validation for the use case. This validation provides a description of the functional application of the use case.

EG: The IP Video Use Case is validated when a user can request and view streaming video from an IP Camera over a local network or the internet.

3. Assumptions

Note any assumptions the Use Case makes.

3.1. Assumption 1

3.2. Assumption 2

3.3. Assumption 3

4. Protocols, Statuses and Standards Bodies

This section should be used to list any relevant protocols that might be relevant to the use case. The intent is to give the reader an awareness of options that currently exist or might emerge in the near future. Each listed protocol should be described as to function, but status and ownership of the protocol are to be assigned in the core document. This model will allow multiple Use Cases to reference the same protocols without having to alter the use cases for changes to protocol status.

4.1. Protocol 1

4.2. Protocol 2

5. Entity Enumeration

The following entities participate in this use case:

5.1. Entity 1

5.2. Entity 2

5.3. Entity 3

6. Functional Dependencies

The Functional Dependencies should illustrate why the various protocols are applied in the order of the Sequence of Events. This illustration should be from the application perspective.

7. Sequence of Events

7.1. Step 1 (EG Address Resolution)

Description, Purpose and Proof Point of Step (EG - Registration of device IP Addresses to support application access. Proof Point is to test IP connectivity with the device. PING is a nominal test of connectivity.)

7.1.1. Manual Options (EG - Manual IP Address Registration)

Description of Manual options (EG - Camera IP Addresses are entered manually into applications.)

7.1.2. Automated Sequence (EG - Automatic Device Discovery)

7.1.2.1. Event 1 (EG - User requests Device Discovery at Application)

7.1.2.2. Event 2 (EG - Application discovers IP Cameras using☺

7.1.2.2.1. Protocol 1 (EG - Proprietary Protocol 1)

7.1.2.2.1.1. IP Details (EG TCP or UDP)

7.1.2.2.1.2. Entity 1

7.1.2.2.1.3. Entity 2

7.1.2.2.1.4. Function

7.1.2.3. Event 3 (EG - Device responds to address discovery request)

7.1.2.3.1. Protocol 2 (EG – Proprietary Protocol 2)

7.1.2.3.1.1. IP Details (EG TCP or UDP)

7.1.2.3.1.2. Entity 1

7.1.2.3.1.3. Entity 2

7.1.2.3.1.4. Function

7.2. Step 2 (EG - Device Configuration and Capabilities)

Description, Purpose and Proof Point of Step (EG - Allow applications to understand what camera can support [frame rate, resolution, codec, etc.]. Proof Point is when camera management application has cameras registered with device capabilities and configuration)

7.2.1. Manual Options (EG – Manual entry)

Description of Manual Options (EG - Camera Configuration entered manually into application)

7.2.2. Automated Options (EG - Configuration and Capabilities

discovery)

7.2.2.1. Event 1 (EG - User requests Device Configuration at Application)

7.2.2.2. Event 2 (EG - Application Requests information from camera using)

7.2.2.2.1. Protocol 3 (EG - Proprietary Protocol 3)

7.2.2.2.1.1. IP Details (EG TCP or UDP)

7.2.2.2.1.2. Entity 1

7.2.2.2.1.3. Entity 2

7.2.2.2.1.4. Function

7.2.2.3. Event 3 (EG - Device responds to information request)

7.2.2.3.1. Protocol 4 (EG - Proprietary Protocol 4)

7.2.2.3.1.1. IP Details (EG TCP or UDP)

7.2.2.3.1.2. Entity 1

7.2.2.3.1.3. Entity 2

7.2.2.3.1.4. Function

7.3. Step 3 (EG – Client Request Video Stream)

Description, Purpose and Proof Point of Step (EG – Allow client to request a Video Stream from the Camera. Proof Point is when user requests a video stream and application acknowledges same. Testing that the client has an RTSP connection to the Source is also a proof point.)

7.3.1. Manual Options (EG – Manual request)

Description of Manual Options (EG – button on camera is pressed)

7.3.2. Automated Options

Description of Automatic Option (EG – Play button on Client is pressed)

7.3.2.1. Event 1 (EG – User clicks Play button in Client)

7.3.2.2. Event 2 (EG – Application Requests Video Stream from Camera)

7.3.2.2.1. Protocol 3 (EG - RTSP)

7.3.2.2.1.1. IP Details (EG TCP or UDP)

7.3.2.2.1.2. Entity 1

7.3.2.2.1.3. Entity 2

7.3.2.2.1.4. Function

7.4. Step 4 (EG – Video is Streamed to Client)

Description, Purpose and Proof Point of Step (EG – Client displays video from Server. Proof Point is when user Can actually see video on the client)

7.4.1. Manual Options (EG – None)

None

7.4.2. Automated Options

Description of Automatic Option (EG – Video is Streamed to Client)

7.4.2.1. Event 1 (EG – Server Establishes Stream back to Client)

7.4.2.1.1. Protocol 3 (EG - SIP)

7.4.2.1.1.1. IP Details (EG TCP or UDP)

7.4.2.1.1.2. Entity 1

7.4.2.1.1.3. Entity 2

7.4.2.1.1.4. Function

7.4.2.2. Event 2 (EG – Server Encodes video to selected codec)

7.4.2.2.1. Protocol 3 (EG - MJPEG)

7.4.2.2.1.1. IP Details (EG TCP or UDP)

7.4.2.2.1.2. Entity 1

7.4.2.2.1.3. Entity 2

7.4.2.2.1.4. Function

7.4.2.3. Event 3 (EG – Server Streams Encoded Video)

7.4.2.3.1. Protocol 3 (EG - RTP)

7.4.2.3.1.1. IP Details (EG TCP or UDP)

7.4.2.3.1.2. Entity 1

7.4.2.3.1.3. Entity 2

7.4.2.3.1.4. Function

7.4.2.4. Event 4 (EG – Client Decodes and displays Video)

7.4.2.4.1. Protocol 3 (EG - MJPEG)

7.4.2.4.1.1. IP Details (EG TCP or UDP)

7.4.2.4.1.2. Entity 1

7.4.2.4.1.3. Entity 2

7.4.2.4.1.4. Function