Asset Identification
Adam Montville, amontville@tripwire.com

URL: http://tools.ietf.org/html/draft-montville-mile-enum-reference-format-00

Abstract:

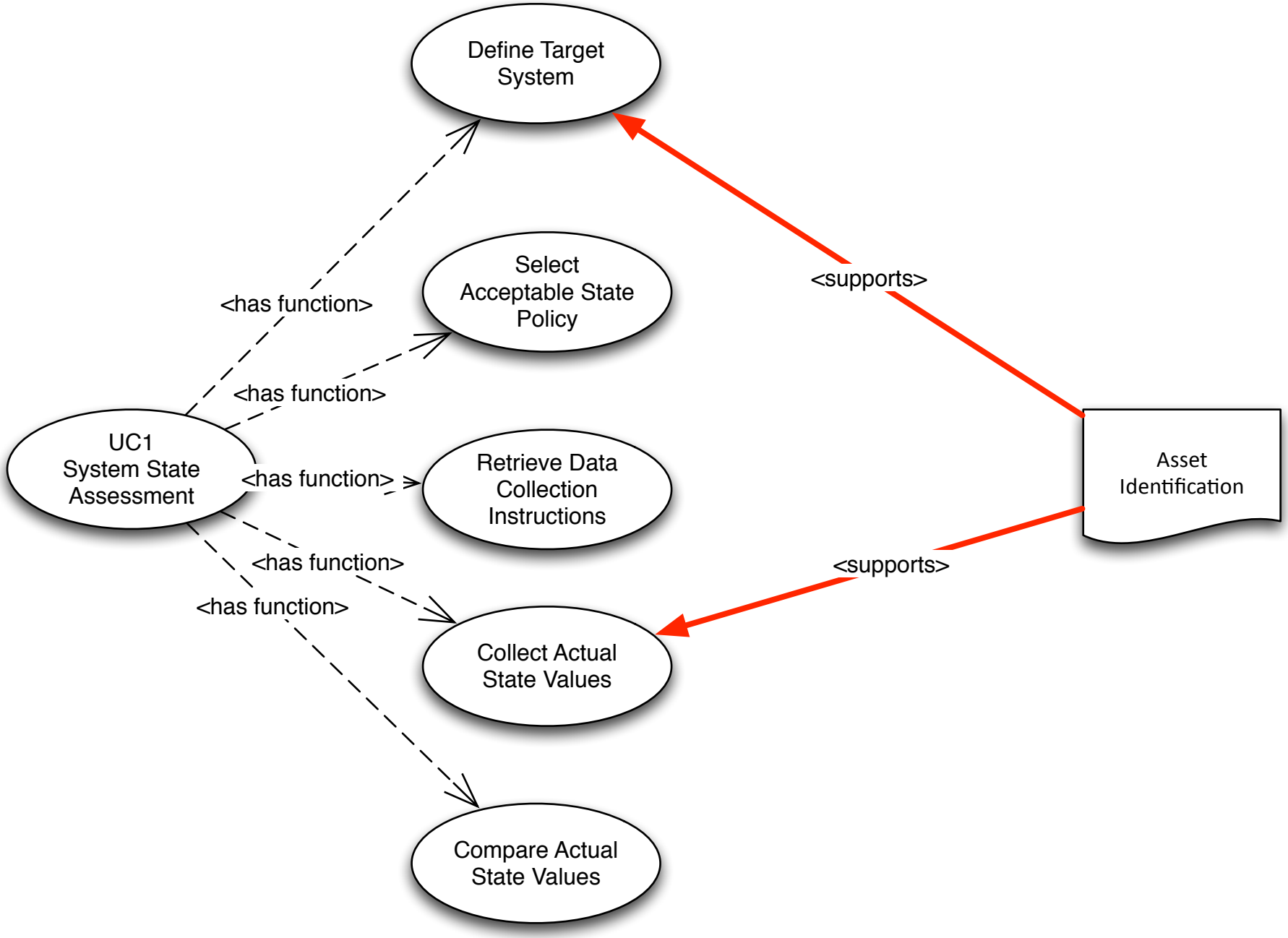
Some standards, such as the Incident Object Description Exchange Format, provide classes used to reference external entities (such as enumeration identifiers). At the time of standardization, however, needed references may not be known, and the method of external entity identification is often left unstructured. This document describes, using IODEF as an example, a method to provide structure after the fact.

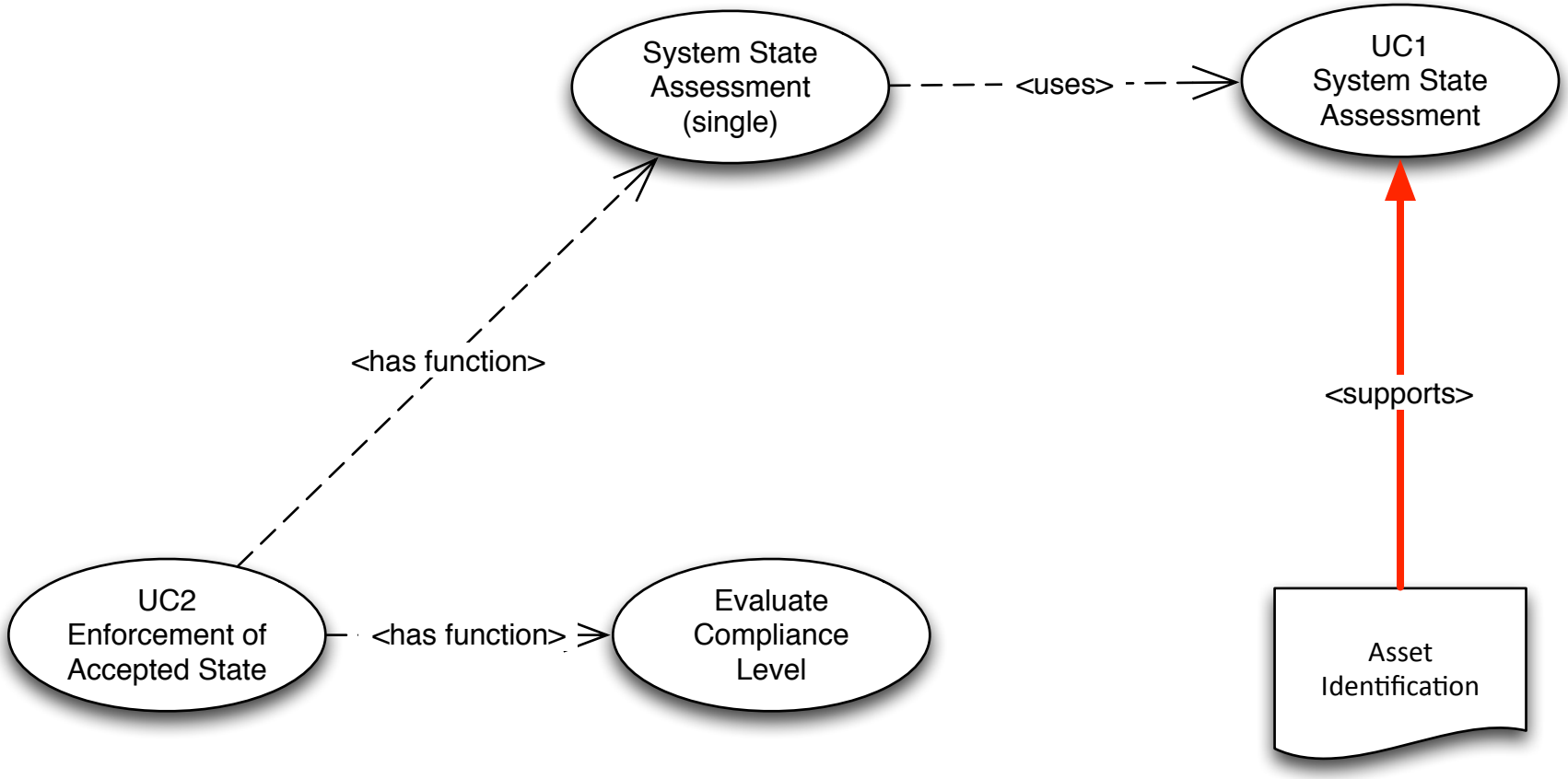
This Asset Identification specification describes a framework for how asset management processes and other specifications may identify assets using some set of information known or generated about the asset.

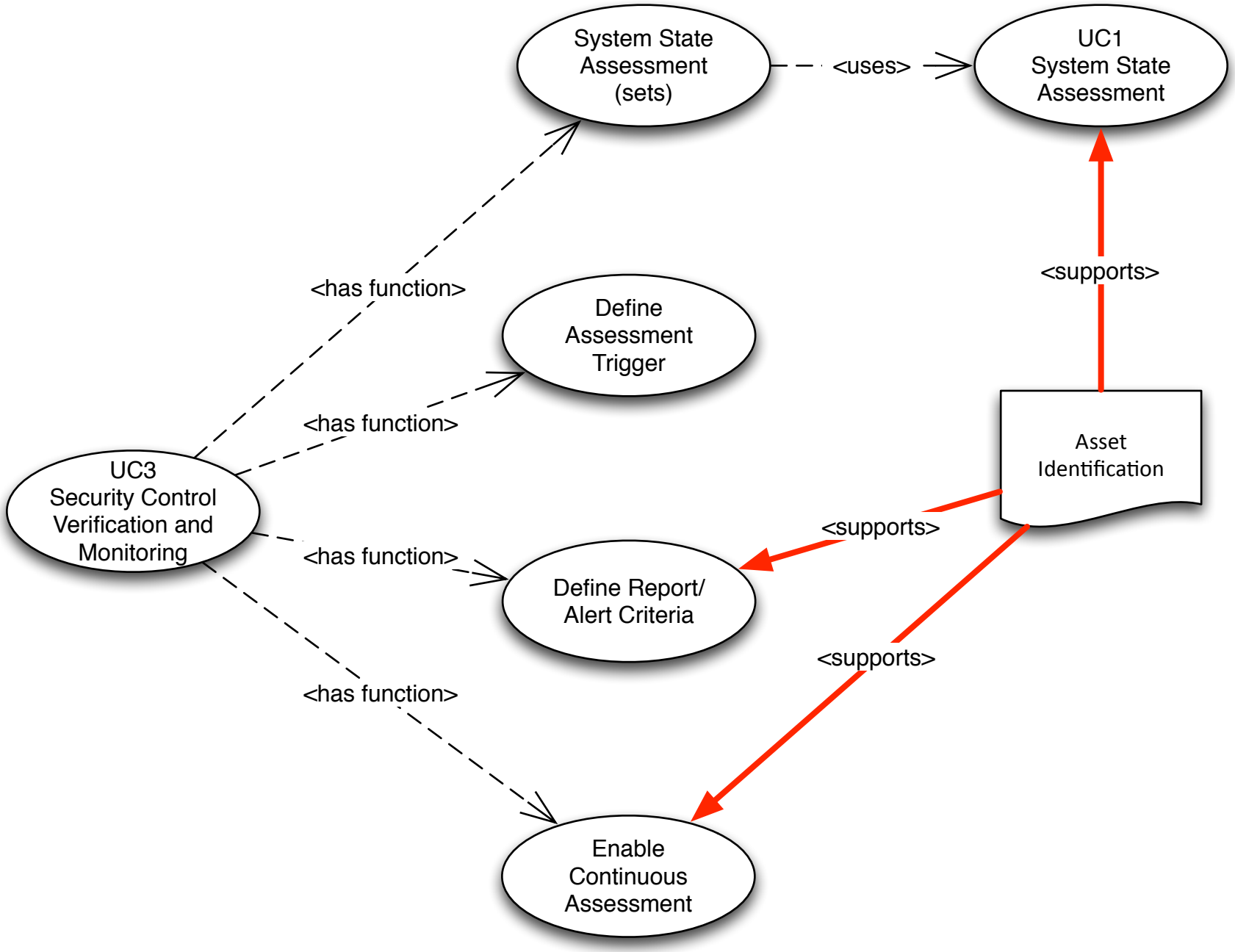
This specification was developed to support the immediate needs of the security automation community.

For the purposes of this specification, an asset is considered to be anything that has value to an organization.

It is expected that other standards, data formats, tools, processes, and organizations will reference this specification to describe how to represent asset identification information.


Define Target System
Select Acceptable State Policy
Retrieve Data Collection Instructions
Collect Actual State Values
Compare Actual State Values
UC1 System State Assessment
Asset Identification
<has function>
<has function>
<has function>
<has function>
<has function>
<supports>
<supports>

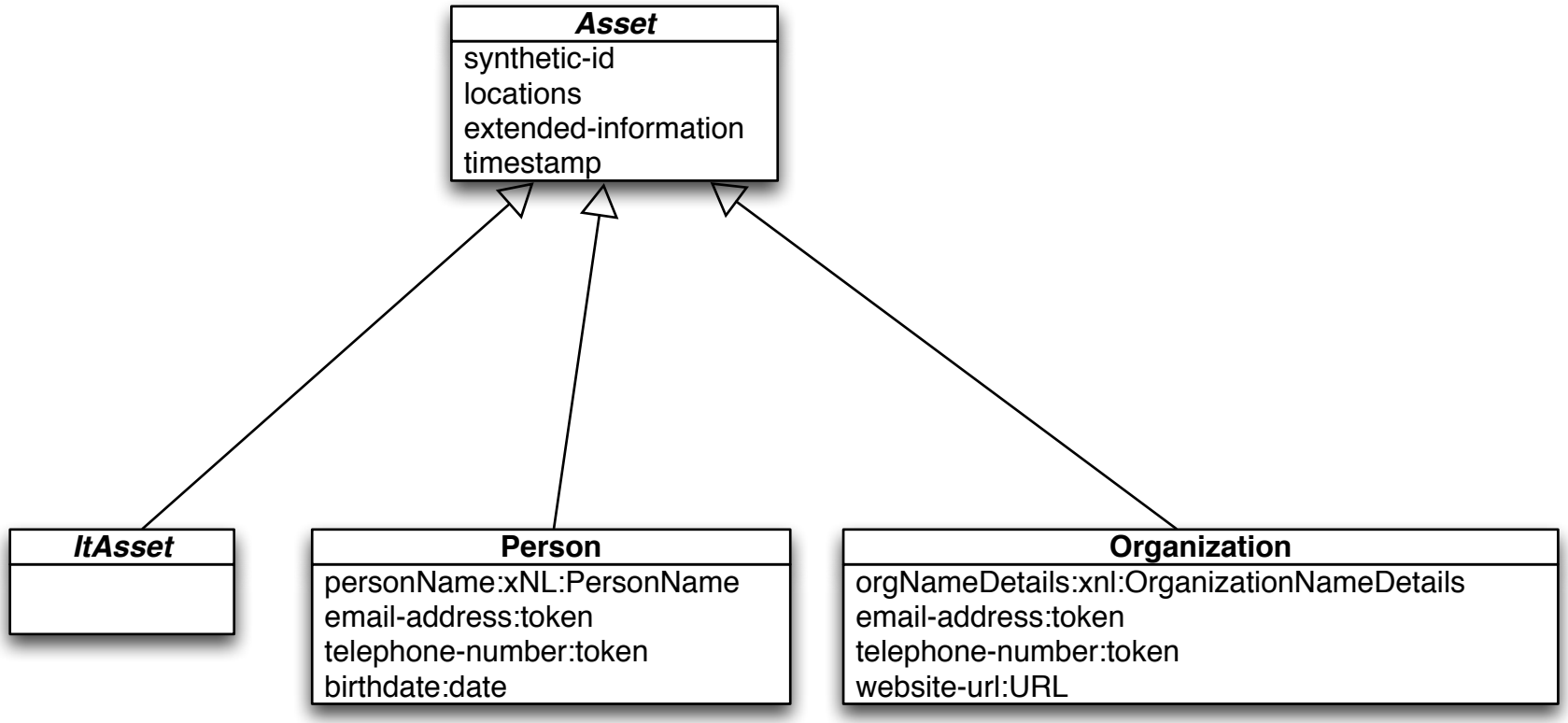

System State Assessment (single)
<uses>
UC1 System State Assessment
<has function>
<supports>
UC2 Enforcement of Accepted State
<has function>
Evaluate Compliance Level
Asset Identification

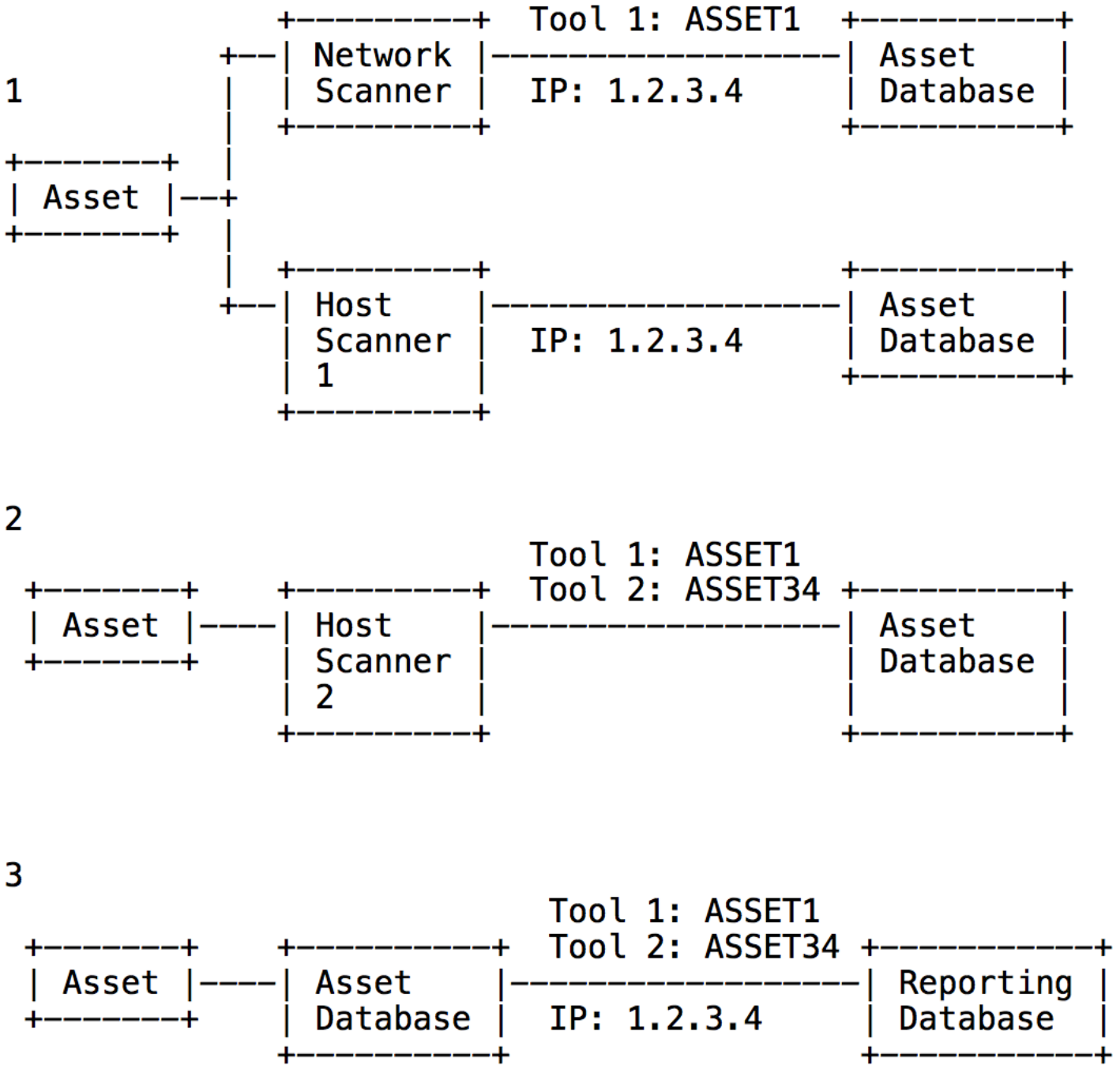

System State Assessment (sets)
<uses>
UC1 System State Assessment
<has function>
Define Assessment Trigger
<supports>
<has function>
Asset Identification
UC3 Security Control Verification and Monitoring
<has function>
<supports>
Define Report/ Alert Criteria
<supports>
<has function>
Enable Continuous Assessment

Does the Community find this work relevant?

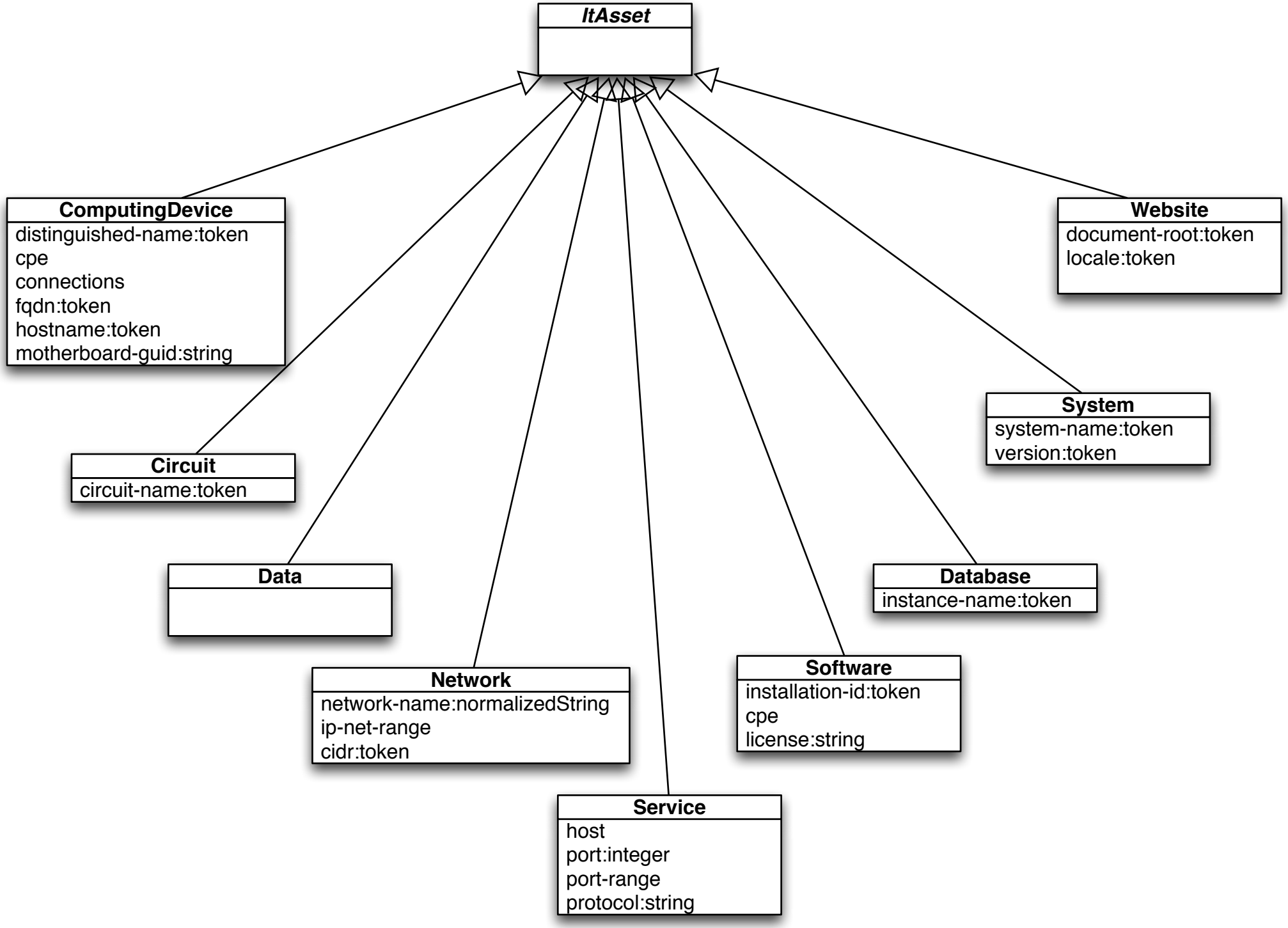
Are there willing Authors/Editors?

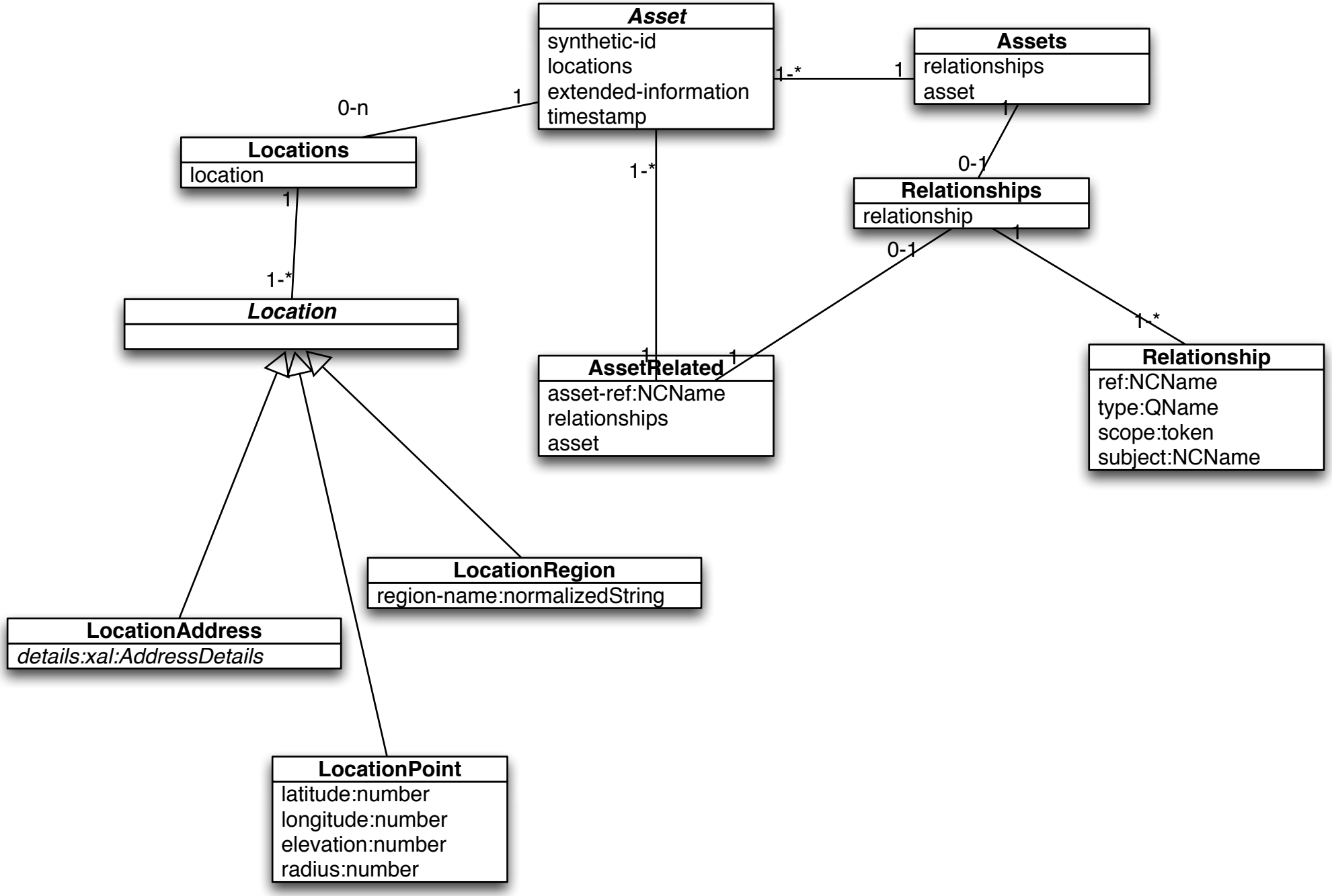
Backup Slides / Technical Details


Asset
synthetic-id
locations
extended-information
timestamp
ItAsset
Person
personName:xNL:PersonName
email-address:token
telephone-number:token
birthdate:date
Organization
orgNameDetails:xnl:OrganizationNameDetails
email-address:token
telephone-number:token
website-url:URL



Sample Correlation Workflow


ItAsset
ComputingDevice
distinguished-name:token
cpe
connections
fqdn:token
hostname:token
motherboard-guid:string
Website
document-root:token
locale:token
Circuit
circuit-name:token
System
system-name:token
version:token
Data
Database
instance-name:token
Network
network-name:normalizedString
ip-net-range
cidr:token
Software
installation-id:token
cpe
license:string
Service
host
port:integer
port-range
protocol:string


Asset
synthetic-id
locations
extended-information
timestamp
Assets
relationships
asset
Locations
location
Relationships
relationship
Location
AssetRelated
asset-ref:NCName
relationships
asset
Relationship
ref:NCName
type:QName
scope:token
subject:NCName
LocationRegion
region-name:normalizedString
LocationAddress
details:xal:AddressDetails
LocationPoint
latitude:number
longitude:number
elevation:number
radius:number
1
0-n
1-*
1
1
0-1
1-*
1
1-*
0-1
1
1
1
1-*

Relation:	Domain:	Range:
hasTerminationDevice	ai:circuit	ai:computing-device
hasServiceProvider	ai:circuit	ai:organization
hasNetworkTerminationDevice	ai:circuit	ai:network
servedBy	ai:database, ai:website	ai:service
hasServiceProvider	ai:service	ai:software
installedOnDevice	ai:software	ai:computing-device
connectedToNetwork	ai:system	ai:network
isOwnerOf	ai:person, ai:organization	ai:it-asset
isAdministratorOf	ai:person	ai:computing-device, ai:system
partOf	ai:person	ai:organization
connectedTo	ai:computing-device, ai:system	ai:system

Relation:	Description:
hasTerminationDevice	The circuit is terminated by the device.
hasServiceProvider	The circuit is owner/operated by the organization.
hasNetworkTerminationDevice	The circuit ends at the network.
servedBy	The database or website is served up by the service.
hasServiceProvider	The service is provided by the software.
installedOnDevice	The software is installed on the computing device.
connectedToNetwork	The system is connected to the network.
isOwnerOf	The person or organization owns the IT asset.
isAdministratorOf	The person is the system administrator of the computing device or system.
partOf	The person is in some way a part of the organization.
connectedTo	The computing device or system is connected to the system.

Possible Improvements

+ Consider using Asset Identification beyond Identification

+ Specify use of IANA registry for asset type addition

+ Specify use of IANA registry for asset type extension

+ Specify use of IANA registry for relationship addition

+ Augment for internationalization