Unified Incident Command Decision Support (UICDS)

Architecture Description Document

Version 1.5, April 15, 2011

4001 N. Fairfax Dr., Suite 250, Arlington, VA 22203

UICDS-SPEC-ADD-R01305

Architecture Description Document Approvals

The signatures below constitute approval of this specification.

Contributors

Roger Wuerfel UICDS Implementation Lead	4/15/2011	Chip Mahoney UICDS Project Manager	4/15/2011

Submitter

Roger Wuerfel, UICDS Implementation Lead	4/15/2011

Approver(s)

Gerald Mahoney UICDS Project Manager	4/15/2011	Daphne Hurrell UICDS Configuration Management Lead	4/15/2011

Revisions

Original: UICDS-SPEC-ADD-R01C00

Revision Number	Date	Description
1.0	6/6/2008	Initial submittal for PDR
1.1	9/10/2008	Extensively revised to encompass design work accomplished since PDR
1.2	11/07/08	Clarification and typographical edits
1.3	04/08/09	Submittal for SRR. Revised to encompass design work accomplished for the prototype. The following sections have been updated 1.1, 1.4, 2.1, 2.2, 2.4, 2.5, 2.6, 3.0, 4.0, 4.2.1, 4.2.2,
1.4	12/22/2009	Edit for consistency with IDD
1.5	4/15/2011	Updated for UICDS version 1.1.1.

Contents

List of Figures

List of Tables

1.0 Introduction

This document describes the architecture of the prototype for Phase II of the Unified Incident Command and Decision Support program.

1.1 Project Overview

The Department of Homeland Security (DHS) Science & Technology (S&T) Directorate has launched the Unified Incident Command and Decision Support (UICDS) program to meet the United States' need to enable government entities across the country to work together to prevent, prepare for, plan for, respond to, and recover from emergency and catastrophic situations.

While a number of systems have been in existence for decades to manage subsets of the required functions for first responder emergency operations, none to date have the innate ability to manage emergency operations at multiple levels in an integrated fashion. The UICDS solution is one that will support a multi-echelon, multi-platform, dynamically structured command structure and associated resources and processes that will enable information sharing and decision support for all individuals, teams, and organizations in order to respond to emergency situations.

Central to the UICDS solution is the doctrine set forth by the DHS:

- The National Response Framework (NRF).
- The National Incident Management System (NIMS), and
- The Incident Command System (ICS)

Within these guidelines, SAIC developed the UICDS architecture during the UICDS Phase I contract. The UICDS Phase II effort expanded upon the UICDS Phase I architecture to produce:

- UICDS Architecture Specifications that are based on open standards, allowing the UICDS solution to be propagated throughout the country, incorporating any technology that enables the specification.
- UICDS Middleware that supports interoperability, information sharing, inclusion of a wide variety of legacy systems, and sharing of common views of incident related data throughout the MACS and ICS.

The UICDS Phase II base period developed and field tested a prototype of these capabilities in the base period and a pilot of these capabilities in the option period.

The UICDS Phase III, Technology Insertion and Pilot Expansion Program extend UICDS, fielding and testing an operational UICDS prototype in a series of regional pilots.

1.2 Document Overview

This document contains the high level overview of the UICDS Architecture and should be used in conjunction with the Interface Design Description (IDD) for the entire architectural description. The IDD documents the service interfaces used by UICDS clients to interact with UICDS. It is suggested to start with this document and then proceed to the IDD to fully understand the Phase II prototype.

1.3 Applicable Documents

Reference Documents

- National Information Management System (NIMS), December, 2008
- National Response Framework (NRF), January 2008
- Universal Task List (UTL), February 2007
- Target Capabilities List (TCL), September 2007

Contract Documents

- DHS S&T BAA 06-02, Unified Incident Command and Decision Support (UICDS) Phase II dated 8 June 2007
- SAIC Proposal #01-0155-71-2007-052 in response to DHS S&T BAA 06-02
- NASA Contract NNG08CA07C (UICDS Phase II Contract) awarded 24 April 2008
- Unified Incident Command and Decision Support (UICDS) Phase II Statement of Work (SOW) dated January 18, 2008
- DHS contract HSHQDC-10-C-00030 (UICDS Phase III Contract) dated 23 June 2010

Phase I Documents

- UICDS Phase I Architecture
- UICDS Phase I Implementation Plan

Phase II Documents

- Templates for planning and technical documents are derived from SAIC's Engineering Edge Software View for Software Product Development.
- UICDS Planning documents are referenced in the UICDS Project Management Plan, UICDS-PLN-PMP-R01C01.
- UICDS Deliverables are referenced in the UICDS Project Management Plan, UICDS-PLN-PMP-R01C01.
- UICDS System/Subsystem Design Description (SSDD), UICDS-SPEC-SSDD-R01C01
- UICDS Interface Design Document (IDD), UICDS-SPEC-IDD-R01C02

Phase III Documents

- UICDS Planning documents are referenced in the UICDS Project Management Plan, UICDS-PLN-PMP-R03C01.
- UICDS Deliverables are referenced in the UICDS Project Management Plan, UICDS-PLN-PMP-R03C01.
- UICDS Interface Design Document (IDD), UICDS-SPEC-IDD-R01C06

1.4 Acronyms, Abbreviations, Notations, Naming Conventions

Table 1 presents the acronyms used in the document.

Table 1- Acronyms and Abbreviations

Acronym	Definition
CAP	Common Alerting Protocol
COTS	Commercial-off-the-shelf
DHS	Department of Homeland Security
EDXL-DE	Emergency Data Exchange Language – Distribution Element
EDXL-RM	Emergency Data Exchange Language – Resource Management
EOC	Emergency Operation Center
HSOC	Homeland Security Operation Center
ICS	Incident Command System
IDD	Interface Design Description
IEPD	Information Exchange Package document (IEPD)
IETF	Internet Engineering Task Force
IM	Instant Messaging
ISA	Information Sharing Agreement
LDAP	Lightweight Directory Access Protocol
LEITSC	Law Enforcement Information Technology Standards Council
MAA	Mutual Aid Agreement
MACS	Multi Agency Coordination System
MOU	Memorandum of Understanding
NIEM	National Information Exchange Model
NIMS	National Incident Management System
NRF	National Response Framework
OGC	Open Geospatial Consortium
PIS	Public Information System
REST	Representational state transfer
RFC	Request for Comments
S&T	Science & Technology
SA	Situational Awareness
SOA	Service Oriented Architecture

Acronym	Definition
SOAP	Protocol for exchanging XML-based messages
SOI	Sensor Observation Information
SOS	Sensor Observation Specification
SOW	Statement of Work
SSDD	System Subsystem Design Description
TCL	Target Capabilities List
TLS	Transport Layer Security
UICDS	Unified Incident Command and Decision Support
URL	Universal Resource Locator
UTL	Universal Task List
WFS	Web Feature Service
WMS	Web Map Service
WSDL	Web Services Definition Language

2.0 Summary of Architecture

The UICDS architecture is a partial mesh network of UICDS servers that allow clients to collaboratively assemble and share emergency management information about an incident using web services provided by their local UICDS server. Collaboration occurs between clients on one UICDS server transparently and between clients on different UICDS servers based on information sharing agreements. Creation or modification of shared information is communicated to clients via a role-based notification service. Clients can be directly addressed for targeted notification delivery through a combination of unique client instance and core names.

2.1 Standards-Based Service Oriented Architecture

The UICDS architecture is built on service-oriented principles using open standards. Each UICDS server, named a UICDS core, serves as a local point of integration for technology providers and agency services. UICDS cores support three varieties of services: infrastructure, domain, and external. Infrastructure services enable the sharing of information between cores and are based on existing, established industry standards. Domain services provide for the management of information specific to emergency management; such as incidents, command hierarchies, tasking, and the common operating picture. These services rely on existing and developing standards in the emergency management domain such as those from NIEM and the OASIS EM Technical Committees. Finally, in addition to the standard UICDS services provided by a core, each core provides the ability to register external services using existing, developing and future standards.

2.2 Federation of UICDS Cores

The UICDS network is a federated system of UICDS cores, with each core representing an organization, an agency or sub-organization of an agency. This concept is illustrated in Figure 3 and shows deployments at the Federal, State, County and Local levels. The topology of the federation is defined by

information sharing agreements following local Memorandums of Understanding (MOUs) and/or Mutual Aid Agreements (MAAs) that define the terms and conditions under which agencies will share information. Agreements must be mutually established prior to data sharing and enable dynamic, incident-based data sharing topologies. User authentication, integration of external systems, and participation in information sharing agreements are managed locally at each core enabling agencies to retain control of local policies and support for their users and systems.

2.3 Information Sharing

Information is shared within a UICDS deployment between UICDS-enabled clients that are connected to a UICDS core. This information is exchanged using a SOAP framework (HTTP or HTTPS) over TCP/IP. Because UICDS is middleware, information to be shared is controlled at the source – the application. Applications control what information is shared via UICDS by only including "appropriate" information in the UICDS data exchanges. Prior to accessing a UICDS core, UICDS clients are authenticated against a local Lightweight Directory Access Protocol (LDAP) database that is either supplied with a UICDS deployment or is part of the local IT infrastructure.

Information is also shared between UICDS deployments (and therefore their UICDS-enabled clients). This information is exchanged using an eXtensible Messaging and Presence Protocol (XMPP) protocol using TLS over TCP/IP. This UICDS core to core information sharing is automatic, but governed by information sharing agreements that are controlled locally. UICDS core to core information sharing can be fully enabled, fully disabled or limited by incident type.

2.3.1 Work Products

UICDS Work Products are the atomic unit of UICDS-based information sharing. All UICDS information is exchanged via UICDS work products. In the emergency management domain, a work product represents information within UICDS that can be associated with an incident. The information is managed as a typed data package containing data in one of several standard data formats as listed in Table 6. The payload of a work product often consists of National Information Exchange Model (NIEM) Information Exchange Packages (IEP), though other structured, unstructured, and binary formats are supported. UICDS cores provide services for creating, publishing, retrieving, and monitoring work products.

2.3.2 Information Sharing Agreements

Information sharing agreements (ISA) represent the terms and circumstances under which UICDS cores exchange data. These conditions are currently based on incident type, but may be expanded to include facets such as geography, time, resource type, and data-handling requirements. An instance of an information sharing agreement specifies the unique identity of the member parties, the incident types that will be shared, and the scope of the agreement. Each party to the agreement is represented by the unique identity of their core (represented by the core's XMPP identifier). The incident types are designated using the local incident typing system of the owner of the core. The scope of the agreement specifies the period of time in which the agreement is valid. Once an agreement is entered into the agreement service of each core, the cores may share incidents. When an incident is shared between UICDS cores, all work products associated with the incident will automatically be shared.

2.3.3 Role-Based Interest Management

While the routing of information between cores is dictated by information sharing agreements, the delivery of information to UICDS resources is dictated by profiles. A UICDS resource is a person, piece of equipment, team, or service which has been assigned a role in the coordination structure (ICS, MACS or other). UICDS resources that collaborate through work products are represented by UICDS web

service clients. Profiles contain information about the resource typing as well as topic expressions defining the interests of a resource. Each resource instance may have one or more resource profiles applied that describes its role and its topics of interest. Topic expressions may be based on work product type and enable the intelligent routing of work product notifications to UICDS resources.

2.3.4 Routing and Delivery

2.3.4.1 User Identification

Each core in the UICDS federation is assigned a unique identifier based on its registered domain name. Additionally, each UICDS resource (as represented by applications for individual users or systems) registered on that core is assigned a unique identifier based on the core's identifier and a resource instance unique identifier.

2.3.4.2 Emergency Data Exchange Language – Distribution Element (EDXL-DE)

UICDS uses EDXL-DE for message routing where appropriate in the system, for example routing of EDXL-RM messages. The EDXL-DE is used in UICDS to capture routing instructions for specific target UICDS resources. The EDXL-DE routing instructions and information sharing agreements determine the cores that will receive the message.

2.3.4.3 Delivery

UICDS employs two separate mechanisms for delivering messages. Core to core communications rely on an established federation of cores [previous section] and the XMPP pub/sub features to deliver information sharing messages to the proper cores. Once delivered, the message's metadata are examined to determine the proper recipients at that core. The recipient then receives a brief notification message via a specific WS-Notification endpoint for the particular resource instance.

2.3.4.4 Work Product Notifications

UICDS work products are defined as a UCore Data Information Package (DIP) which contains metadata and a structured payload. The UICDS metadata elements are the work product identification and the work product properties. Some work product types have a UCore Digest element which indicate who, what, when and where details. Metadata and digests are the elements that are delivered in a work product notification.

2.4 Resource Management

Given the great disparity in how agencies manage their local resources, the UICDS architecture does not provide resource management services for end users. However, the UCIDS system does provide a service level interface for routing EDXL-RM compliant resource messages between cores with established sharing agreements.

When UICDS receives an EDXL-RM message (wrapped in EDXL-DE as required by the OASIS specification), it extracts summary information and forwards the message to other UICDS servers in accordance with EDXL-DE routing information. Selected summary resource information of requested and committed resources is stored as a Work Product for retrieval by UICDS clients.

2.5 In-Band vs. Out-of-Band Data

The UICDS architecture is designed to distribute information among large groups of cores and their users at incident-time. To accomplish this, UICDS relies on XMPP for core-to-core communications. This protocol is ideal for small to moderately sized data packages at moderate per-client frequencies (on the

order of seconds). Data transfer occurring in this manner is referred to as "in-band". However, some data formats and applications do not lend well to the XMPP protocol. Examples include data distributed via streaming and real-time protocols and very large sets of data (of the magnitude megabytes). UICDS manages these kinds of transfer as "out-of-band" – meaning that the data is not transferred from core to core, but is managed by an external content provider or service. A core's clients are notified of the availability of out-of-band data via a notification containing a reference to the data (such as map context or URL).

2.5.1 GIS Information

UICDS clients are the source for raw GIS data and provide filtered views of this data to the UICDS core as UICDS Map Work Products. Client applications that receive this information then provide interactive mapping and rendering capabilities of the shared, focused data.

The UICDS architecture provides operations for sharing data both in-band and out-of-band GIS information. Clients may create and distribute point features, such as the location of an incident or command post, as in-band data. These point features are contained in the resulting work product that is shared between cores (via XMPP) and made available to remote UICDS clients as XML data.

To manage large, complex, or frequently updated datasets, an agency first publishes the data to an internal Map server that is OGC compliant and then submits links to this information to UICDS as a Map Work Product. UICDS then allows clients to publish and share a context document (based on the OGC's Web Map Context) referencing the specific data layers on the map server. Clients on remote cores receiving the context document (as a work product) can then retrieve the feature overlays directly from the map server (i.e. out of band).

2.5.2 Streaming Data

The same technique that applied to large, complex mapping data is also used for streaming data such as audio and video. Streaming data cannot be passed from core to core via XMPP, so a reference to the data stream is passed via a context document. Generally, a reference to streaming data is a URL. The context document may then be an EDXL-DE document or CAP message depending on the application.

2.5.3 Sensor Utilization

In addition to map servers and streaming data, agencies or organizations may have external sensor suites available to provide situational awareness of anomalies. The UICDS architecture allows these agencies to register their OGC Sensor Observation Specification (SOS) sensors suites with the UICDS core server. Specific sensors that are of interest to an incident can be published as a Sensor Work Product allowing clients on remote cores to discover the sensor and to request a specific observation directly from the OGC SOS compliant sensor service. Because of the potential size and frequency, the observation requests occur out-of-band.

3.0 Operational View

The UICDS architecture enables users to:

- Discover and capture critical incident information
- Analyze captured information
- Effectively disseminate critical information to emergency responders
- Coordinate the efforts of emergency responders
- Store relevant information for future analysis

The UICDS architecture provides an information exchange infrastructure in compliance with the NRF and NIMS doctrines. UICDS is designed to support all phases of emergency response (planning, protection, response and recovery) over the full spectrum of natural, technological, and terrorist events, from small accidents to major catastrophes, from daily incidents to large events. As shown in Figure 2, UICDS supports the three primary systems of the NIMS, beginning with the ICS that is responsible for control of the immediate incident scene. UICDS facilitates the interface between ICS and the cognizant jurisdiction's Emergency Operation Center (EOC), thus providing the critical information link to the MACS (the second major system in NIMS) that extends from local to state to federal and tribal organizations. The result of interconnecting the ICS with the MACS is an exchange of information, requests, and decisions that results in an improved situational awareness from the ICS to MACS and improved incident support from MACS. Situational awareness and incident support begins at the local level with immediately available resources and mutual aid resources; continues with the addition of tribal or state resources, including the National Guard; and extends to the Federal level for large scale incidents.

The third of the major systems in NIMS, Public Information is integrated with both the ICS and MACS. Using the UICDS role base interest management, the situation awareness contained in UICDS provides the public information officer timely, accurate and accessible information about an incident.

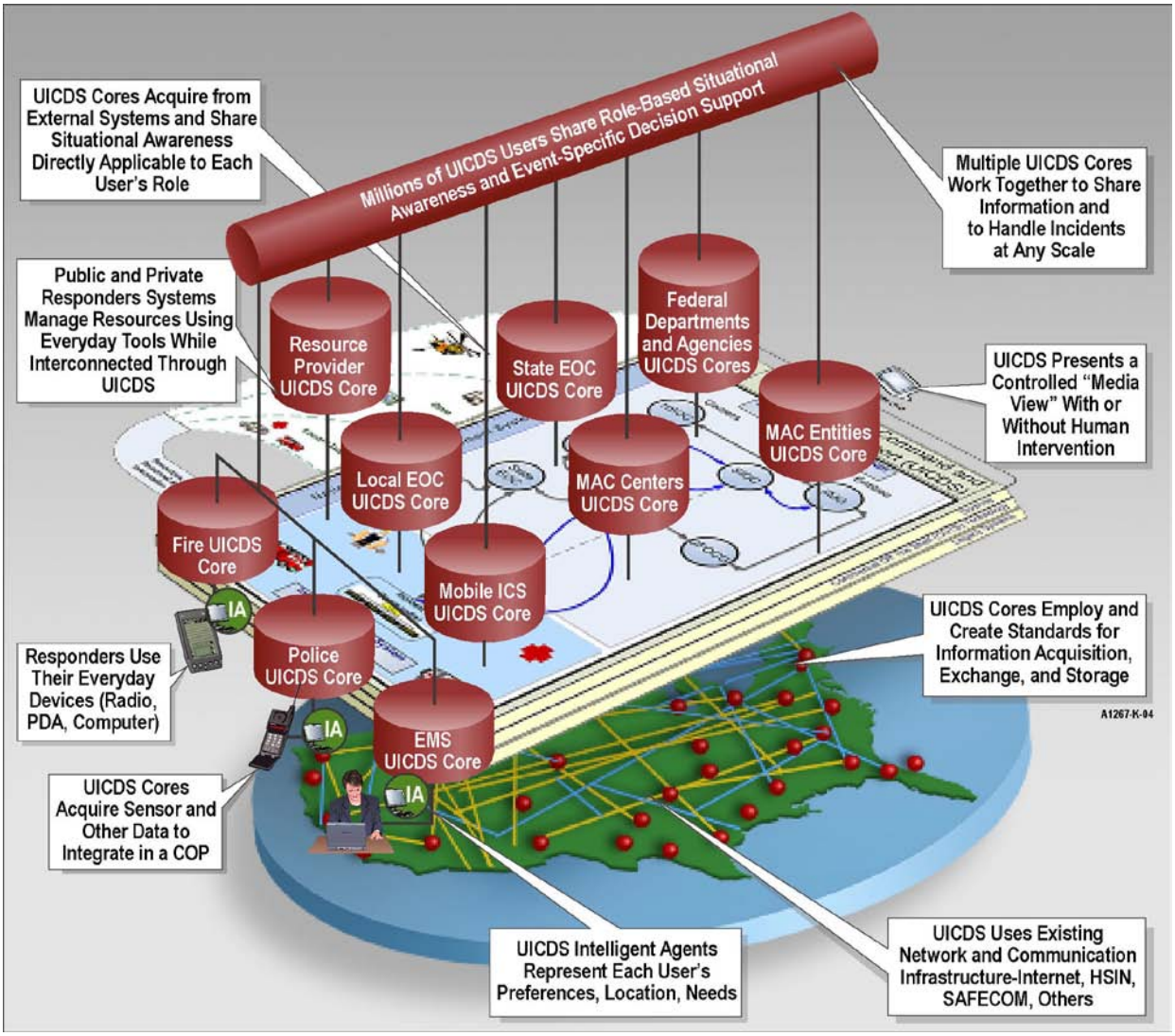


Figure 1 - UICDS Conceptual Architecture

The UICDS architecture was formulated in Phase I of the project and refined in the current Phase II to encompass the basic Emergency Management functions and capabilities defined in the NIMS, NRF, National Planning Scenarios, Target Capabilities List and the Universal Task List.

Figure 3 shows some of the various entities that could be involved in a UICDS deployment. Such a deployment would consist of a collection of UICDS cores representing organizational or political enterprises and agencies. UICDS users interact with UICDS via external UICDS enabled applications and devices that exchange data with UICDS cores. UICDS Cores are interconnected at incident time in accordance with applicable information sharing agreements (MOUs, MAAs, etc) to enable a collaborative planning and response environment for all personnel involved.

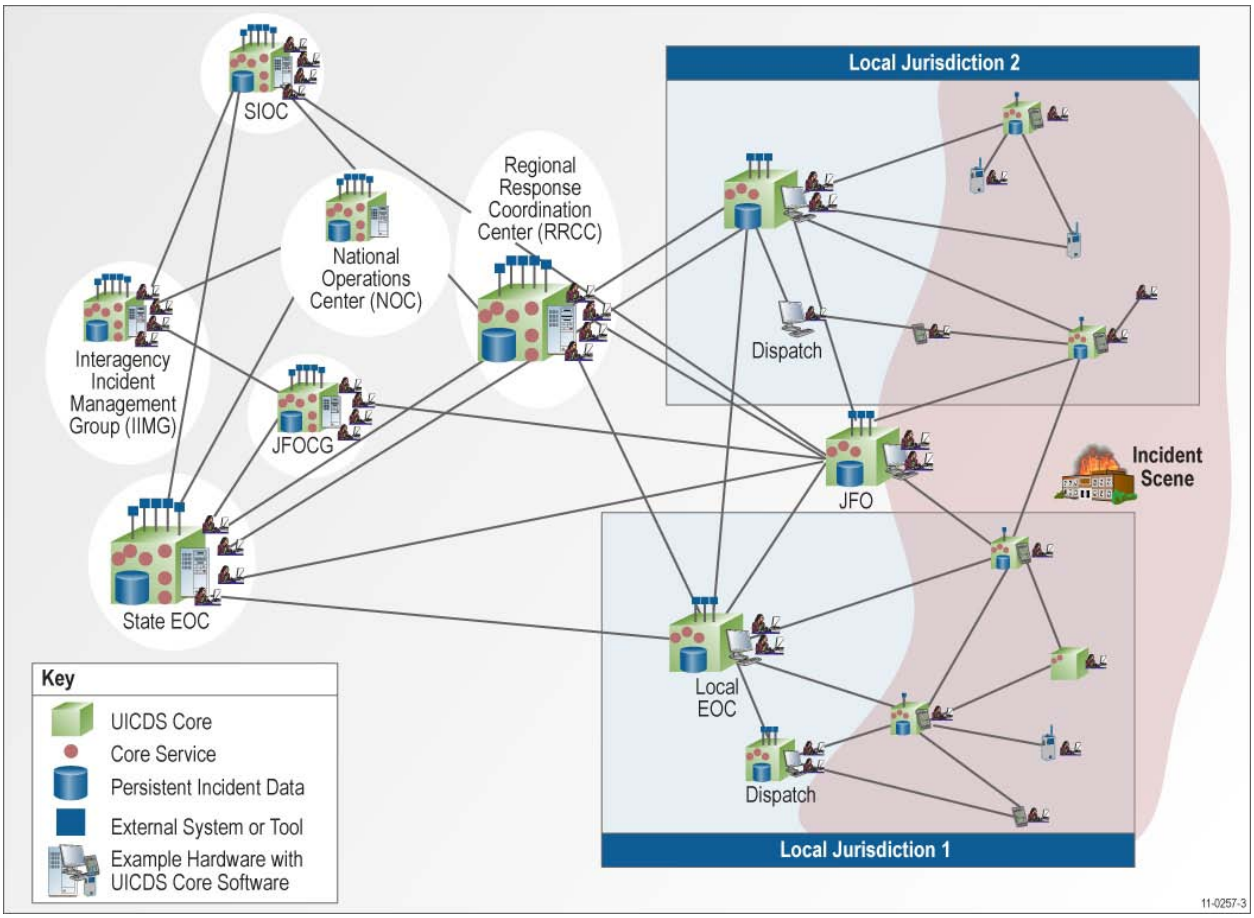


Figure 2 - UICDS Deployment Diagram

4.0 System View

4.1 System Architecture

UICDS uses a combination of cores (servers) and user clients to address the complex information sharing and collaboration needs of the ICS during emergencies. UICDS accommodates multiple agencies (such as police, fire, and emergency medical service) across multiple jurisdictions at multiple levels (e.g., local, state and national) by enabling their individual responder systems to communicate with each other.

UICDS cores serve the personnel and agencies represented in the ICS, EOCs, and MACS Centers and Entities. They interconnect relevant jurisdictions to provide critical information links, extending from local, state, and tribal organizations' centers to federal centers and entities.

Figure 4 depicts the UICDS system architecture. UICDS services can be categorized into two functional areas. UICDS Infrastructure Services form the backbone of UICDS information sharing and provide the fundamental UICDS capabilities such as work product management, information sharing agreements, external notifications, UICDS resource management and event/error logging. UICDS Domain Services then overlay on this infrastructure to provide specific UICDS capabilities geared to emergency responders and emergency managers. UICDS Domain Services provide the interfaces to external applications and enable the exchange of UICDS Work Products specific to the domain. These web service interfaces support the exchange of standards based UICDS Work Products as listed in Table 6.

UICDS Work Products are persisted in an XML database (eXist), but only for the duration of the incident. Once the incident is identified by a UICDS client as closed or inactive, the incident, and all of its Work Products, is removed from UICDS.

All UICDS clients (UICDS Cores, client applications and people) are authenticated against a Lightweight Directory Access Protocol (LDAP) database. This database is managed locally to ensure that local end users control all who have access to their information and all with whom they share their information.

Each deployed UICDS core interacts with client applications via standard UICDS web services. UICDS core to core interactions are enabled via an XMPP connection to other cores with which it has a locally managed information sharing agreement. Then, when a new UICDS Work Product is created (or a current Work Product is modified), this information is shared with all other UICDS cores in accordance with these local information sharing agreements.

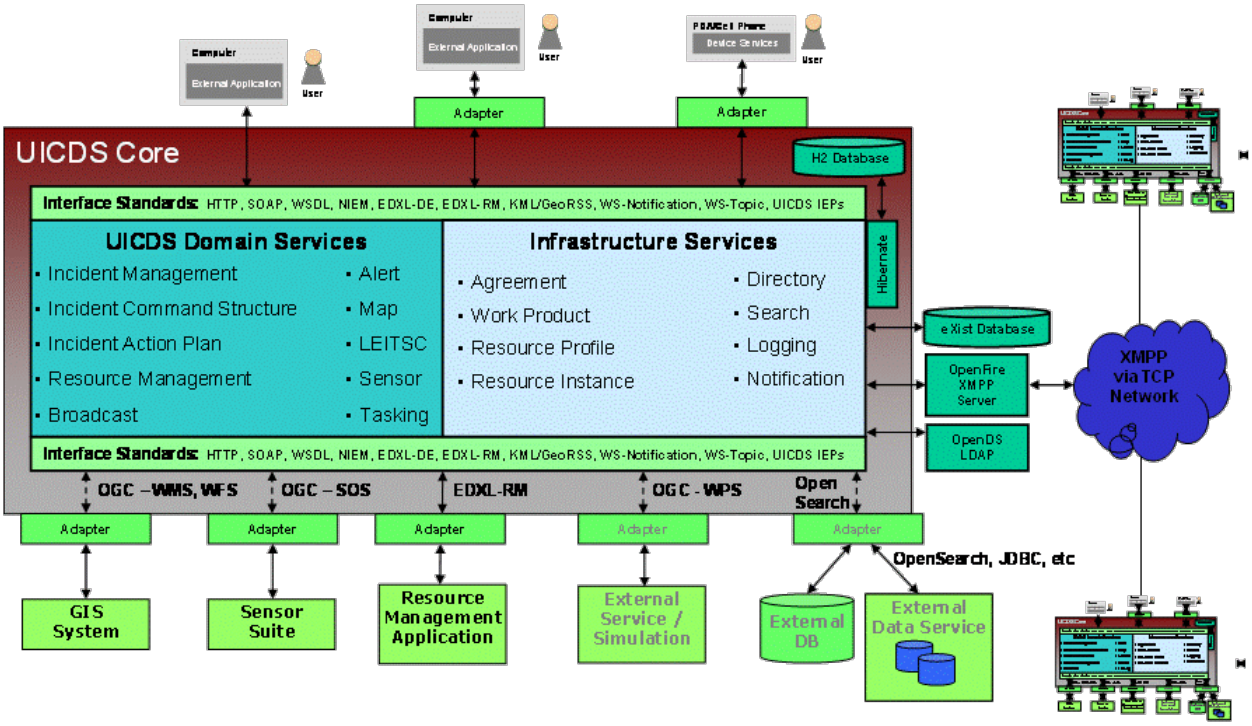


Figure 3 - UICDS System Architecture

4.2 UICDS Core Software Components

The main software components of the UICDS Core are shown in Figure 5. UICDS Web Services are deployed in an instance of Tomcat and are supported by the other components. The embedded H2 database provides internal storage of non-work product data such as data mappings, resource profiles, and resource instances. OpenDS provides bind-based authentication and user management to control access to the UICDS web services. The Openfire XMPP Server provides the core to core messaging

infrastructure. The eXist database provides native XML storage and query for the UICDS Work Products.

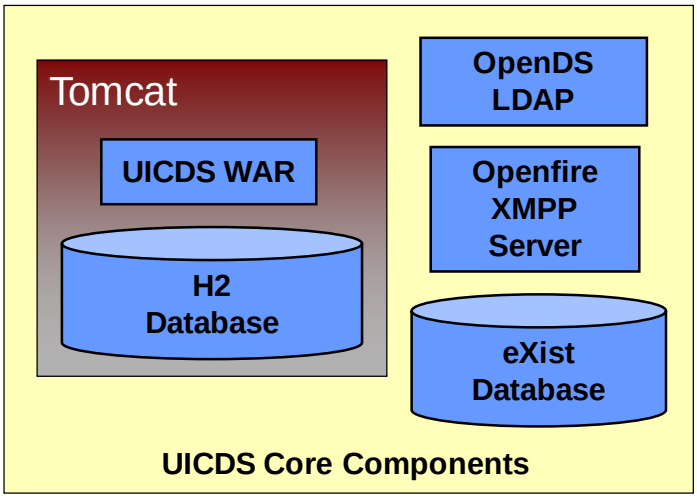


Figure 4 - UICDS Core Server Components

4.3 Services

The following sections describe Service Oriented Architecture (SOA) Groups and the services that comprise these groups.

4.3.1 Infrastructure Services

The UICDS Infrastructure Services provide the APIs for managing the sharing of information among UICDS Cores.

Table 2 - Infrastructure Services

UICDS Infrastructure Service	Description
Agreement Service	Provides a means to establish and define relationships between UICDS Cores. The Agreement service allows relationships based on Mutual Aid Agreements, Memorandums of Agreements, Memorandums of Understanding, and other contractual documents.
Notification Service	Provides a WS-Notification compliant service interface to provide push and pull based notifications to UICDS clients.
Work Product Service	Interacts with all the work product providers, such as Alert Service, Incident Management Service, and Map Service to persist and retrieve their work products.
Directory Service	Allows UICDS users or software modules to retrieve information on the following: • UICDS cores • Available services • Available external tools

UICDS Infrastructure Service	Description
	• Available external data sources • Available sensors • Active incidents
Logging Service	Provides Apache log4j functionality to allow the client to log any type of information into the log file. This web service is configured based on the configure file (log4j.properties).
Resource Profile	The UICDS Resource Profile service provides a means to create, discover and update information about UICDS Resource Profiles. Resource Profiles represent a role that a potential resource instance will fulfill with respect to a particular Interest Group (i.e. incident)
Resource Instance	The UICDS Resource Instance service provides a means to create, discover and update information about UICDS resource instances. A UICDS resource instance represents a resource that is capable of receiving Notification Service messages.
Search	The Search service provides UICDS clients with services to discover and access work products using OpenSearch enabled fields. The Search service also provides various types of feeds of data such has a GeoRSS feed of incidents.

4.3.2 Domain Services

The UICDS Domain Services provide APIs for managing Emergency Management specific constructs within UICDS such as incident summaries, command hierarchy, and mapping.

Table 3 - Domain Services

UICDS Domain Service	Description
Incident Management Service	Allows clients to create an incident, update information about an incident, and share the incident with other UICDS cores.
Incident Command Service	Allows clients to create and modify command structures for incidents and MACS and associate people to organizational roles.
Alert Service	Allows UICDS compatible clients to send, update, cancel, and subscribe to Common Alerting Protocol (CAP) alerts that conform to the CAP version 1.1 specification.
Broadcast Service	Provides a mechanism to send EDXL-DE 1.0 messages to selected UICDS users.
Map Service	Provides an abstract specification for interacting with an

UICDS Domain Service	Description
	UICDS core to manage map related resources.
Tasking Service	Allows a client to create and update a list of tasks for a resource.
Resource Management Service	Provide clients with services to communicate with other external Resource Management Application using EDXL-RM messages.
Incident Action Plan Service	Provides operations to create or retrieve an IAP, create ICS Forms, and mark an IAP as approved for an operational period.
Sensor	Provides the ability for UICDS users to create, update, and delete a Sensor Observation Information (SOI) work product for a given incident.
LEITSC	The Law Enforcement Information Technology Standards Council (LEITSC) service allows clients to create, update, close and archive UICDS incidents based on LEITSC Detailed Call For Service messages.

4.4 Security Architecture

4.4.1 UICDS Communications Overview

UICDS allows for Core to Client and Core to Core Communications as shown in the following figure. Core to Client communications authenticate via a Directory Server. UICDS may either be deployed with a standalone LDAP directory server or integrated with an existing directory server. The WSDL for each service describe the UICDS core to client communications. The UICDS web services are deployed with the Apache Tomcat web server. The UICDS Communication Component, implemented by a XMPP Server, enables UICDS core to core interfaces.

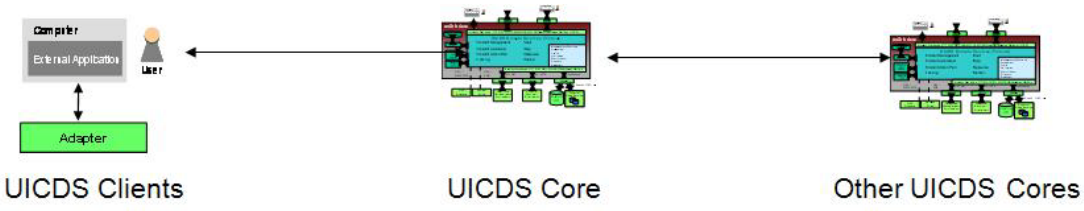


Figure 5 - Typical UICDS Core to Core Communications

4.4.2 Access Control

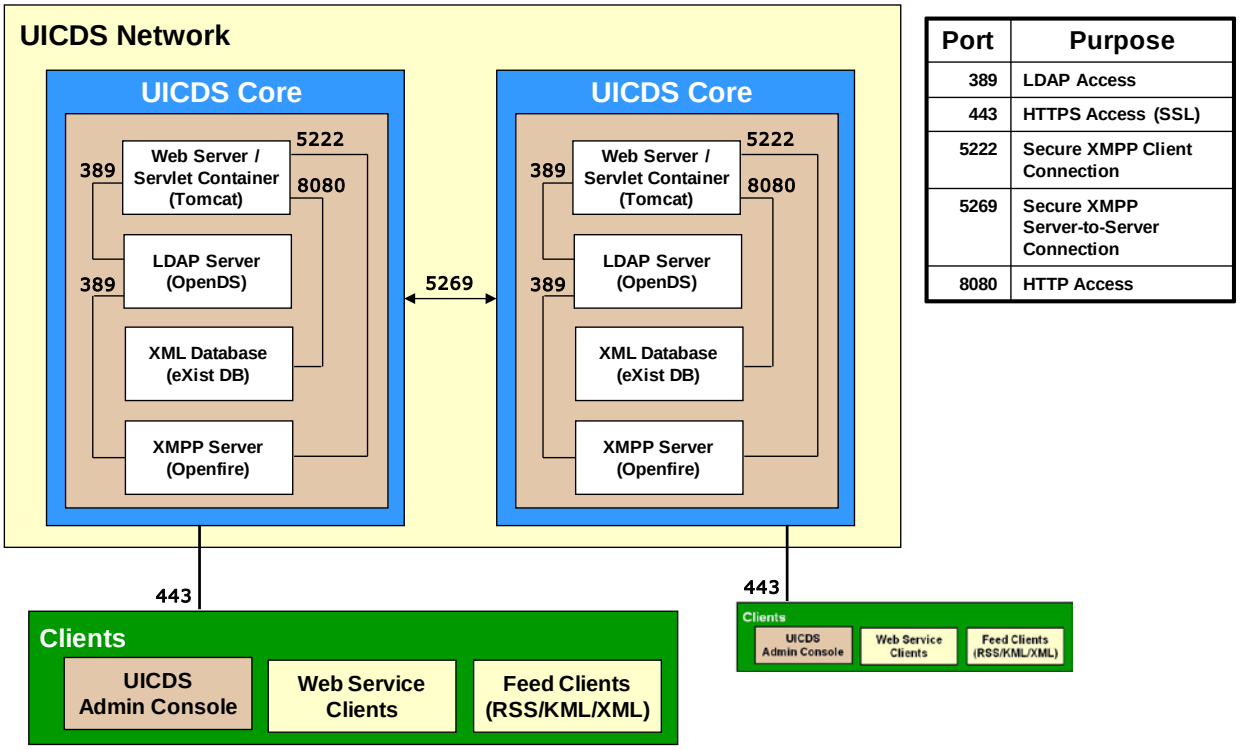
UICDS access control is managed at the local agency level and according to their policies. All client access to web services is controlled by using HTTP basic authentication via HTTPS on port 443. All clients are authenticated against a UICDS LDAP server.

4.4.3 Core to Core Communications

UICDS core to core communications are governed by information sharing agreements that are managed at the local level. All core to core communication is XMPP messaging over port 5269 and is secured using TLS.

4.4.4 Required Ports

The UICDS software components rely on ports as shown in Figure 7.



Port	Purpose
389	LDAP Access
443	HTTPS Access (SSL)
5222	Secure XMPP Client Connection
5269	Secure XMPP Server-to-Server Connection
8080	HTTP Access

Figure 6 - UICDS Required Ports

4.5 UICDS Data Model

The following diagram shows the UICDS conceptual data model. This data model identifies the project's high-level data structure based on desired overall functionality for the project. The detailed data model for each service is captured in the IDD. It is represented there as class diagrams in each service section and as WSDLs in the IDD Appendix A and XML schema in the IDD Appendix B.

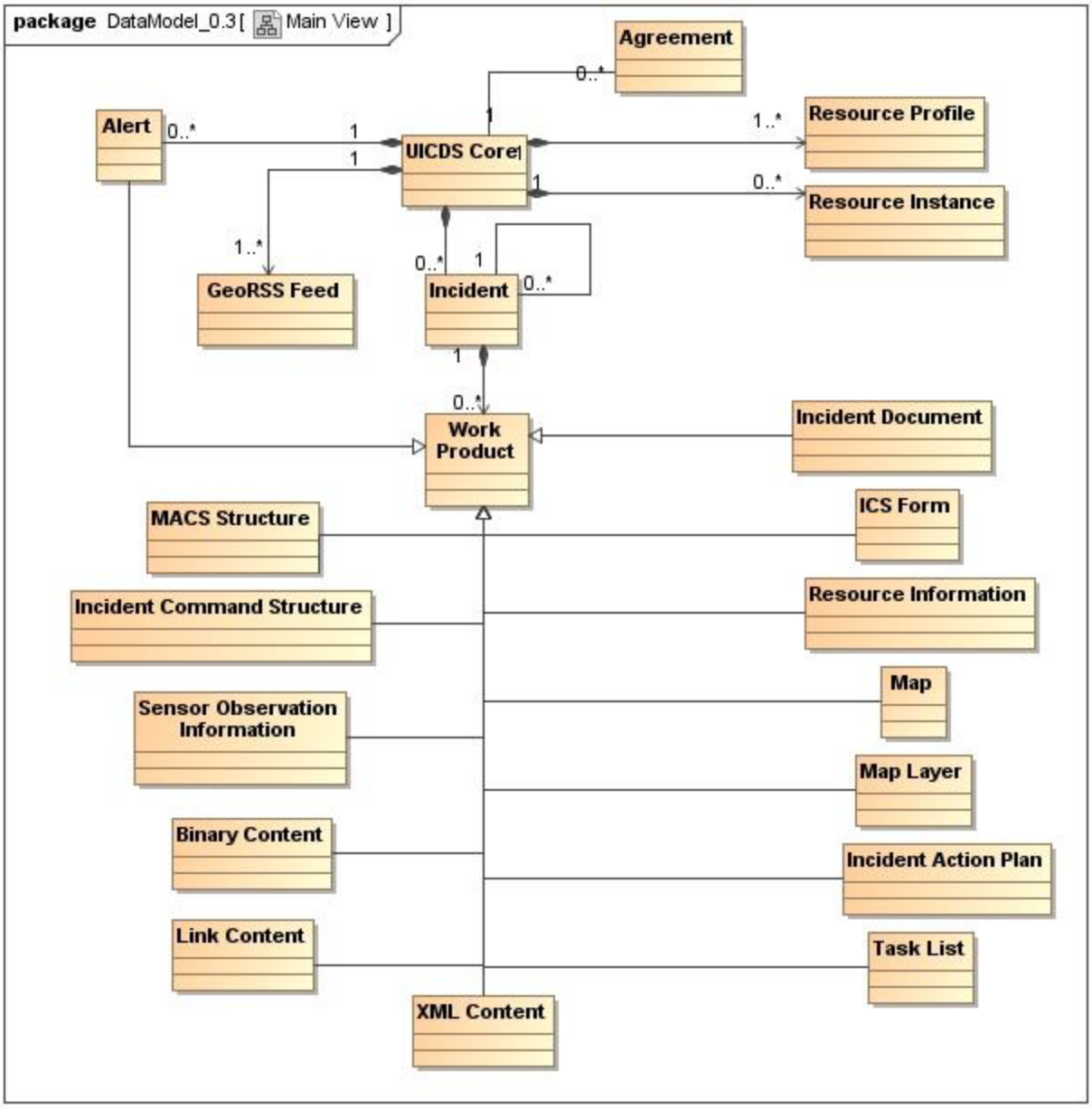


Figure 7 - UICDS Conceptual Data Model

4.6 UICDS Client Use Cases

The following is a UICDS client use case to describe how a UICDS client interacts with the services on the cores and share incident data:

- A UICDS Resource Profile establishes a set of Work Product types about which a UICDS client should be notified. Resource Profiles can represent roles such as those in the ICS.
- Each UICDS client/user must be represented by a Resource Instance. A Resource Instance is a specific representation of a Resource Profile. There may be multiple Resource Instances

associated with a Resource Profile. A Resource Instance may be an application or a person (and that person can be assigned to a role).

- Once a client is assigned a role in an incident, they begin receiving work product notifications. The types of work products they receive notifications for is the union of the types specified by the resource profiles applied to their resource instance.
- As work products are published to a core, the work product types are evaluated against the resource profiles. When a work product matches a resource profile's declared interest, a notification is placed in the resource instance's notification queue. The notification is then delivered to the client via the notification service.
- Notifications are retrieved from the notification service by the client. The notification includes the work product identification, work product properties, and digest of the work product which precipitated the notification. Using the work product identification, the client may then request the full work product from the UICDS core.

5.0 Technical View

5.1 Work Products Overview

UICDS Work Products are the atomic unit of UICDS information sharing. A Work Product is the versioned artifact of a UICDS process and may be generated by UICDS services or by UICDS clients.

A UICDS Work Product consists of:

- Work Product Metadata – ULex derived metadata components to capture Identification and Property elements required for the UICDS infrastructure.
- Work Product Digest – UCore Digest element (Who, What, Where, and When)
- Work Product Payload – XML, Binary, or Link content

Data from a client is augmented by metadata and a digest, and then assembled into a UICDS Work Product for core-to-core communications. Notifications of new and updated UICDS Work Products are sent to clients as UICDS Work Product Summaries which include digest information and the metadata necessary for retrieving the full UICDS Work Product.

5.2 Work Products Description

The following are work products that are managed by the UICDS services.

5.2.1 Incident

UICDS Incident work product is derived from the NIEM Incident Type and extended with elements to represent UICDS specific items.

5.2.2 Alert

UICDS Alert work product conforms to CAP version 1.1 specifications.

5.2.3 Map

There are two types of UICDS Map work products:

- Map View Context (OGC View Context)
- Layer View Context (OGC Layer)

5.2.4 The model is based on OGC Web Map Context specification. Sensor

UICDS Sensor work product contains the information required to retrieve sensor observations that are associated to the incident. UICDS Sensor Observation Information conforms to Open Geospatial Consortium Sensor Observation Specification (OGC-SOS).

5.2.5 Incident Command Structure

UICDS Incident Command Structure work product represents the organization structure for an incident and the resources that have been assigned to the incident.

5.2.6 Incident Action Plan

UICDS Incident Action Plan work product contains other work products that are part of the action plan. Examples of these work products are maps, image files, task list, and ICS forms.

5.2.7 Resource Management

There are two types of Resource Management work products:

- Requested Resources
- Commit Resources

The Request and Commit Resource message are used within UICDS to create the work products and their digest so that these data can be searched.

5.3 Standards

All messages that are exchanged from a UICDS client to a UICDS service are fully defined in the UICDS WSDL so they are not obscured. The IDD defines the services, operations and message schemas for the UICDS system. The standards used in the implementation of the services are listed in the following tables. All of the services utilize the SOAP version 1.1. All Services utilize HTTP 1.1.

All services and web-addressable resources are protected using HTTP Basic Authentication as specified in IETF RFC 2617 and HTTPS.

5.3.1 Infrastructure Services

Table 5 presents the standards observed by each UICDS infrastructure service.

Table 4 - Infrastructure Service Standards

UICDS Service	Standards
Agreement Service	NIEM 2.0
Notification Service	WS-BaseNotification 1.3, WS-Topics 1.3
Work Product Service	UCore 2.0
Directory Service	N/A
Logging Service	N/A
Resource Profile	WS-BaseNotification 1.3, WS-Topics 1.3
Resource Instance	WS-Addressing 2005-08
Search	OpenSearch 1.1, KML 2.2, RSS 2.0 with W3C Basic Geo

UICDS Service	Standards
	extensions, UCore 2.0

5.3.2 Domain Services

Table 6 presents the standards observed by each UICDS domain service.

Table 5 - Domain Service Standards

UICDS Service	Standards
Incident Management Service	NIEM 2.0
Incident Command Service	NIEM 2.0
Alert Service	CAP version 1.1 specification
Broadcast Service	Emergency Data Exchange Language Distribution Element (EDXL-DE) Version 1.0
Map Service	OGC WMS, WFS
Tasking Service	NIEM 2.0
Resource Management Service	Emergency Data Exchange Language Resource Messaging (EDXL-RM) 1.0
Incident Action Plan Service	NIEM 2.0
Sensor	OGC Sensor Observation Service (SOS) 1.0.0
LEITSC	LEITSC Information Exchange Package document (IEPD)