

External Alert 2.0

GJXDM Information Exchange Package
Documentation
Generated: July 27, 2006

Table of Contents

<u>TABLE OF CONTENTS</u>	2
<u>1. PURPOSE AND SCOPE</u>	4
1.1. Scope.....	4
1.2. Purpose:.....	4
<u>2. LIST OF ARTIFACTS</u>	4
<u>3. XML SCHEMAS</u>	4
<u>4. ADDITIONAL IEP PROVISIONS</u>	4
<u>4.1. Additional Property Definitions</u>	5
Document.....	5
Document Sections	5
Components	5
Elements	6
Document Local XML Types	9
Document Local XML Elements.....	9
<u>4.2. Minimal Properties Set</u>	10
<u>4.3. Additional Business Rules</u>	10
4.3.1. Description.....	10
4.3.2. Data Exchanges	11
<u>5. SAMPLES</u>	13
<u>6. DEVELOPMENT</u>	13
6.1. Participants	13
6.2. Process:.....	13
6.3. Development Artifacts:	14
6.3.1. Data Model Diagram	14
6.3.2. Source Documents	15
6.3.3. Revision History:.....	15
<u>7. TESTING AND CONFORMANCE</u>	15

8. FEEDBACK..... 15

1. Purpose and Scope

1.1. Scope

National

1.2. Purpose:

2. List of Artifacts

1. GJXDM Subschema
2. Extension Schema
3. Document Schema
4. XML Document Instance
5. Data Model Diagram
6. XMI Export
7. XML Mappings
8. GIEP Description

3. XML Schemas

GJXDM Version: 3.0.3

Schema Type	File Name
Subset Schema	External Alert 2.0 Schema Package\jxdm\3.0.3\jxdm.xsd
Extension Schema	External Alert 2.0 Schema Package\lt.xsd
Document Schema	External Alert 2.0 Schema Package\External Alert 2.0.xsd

4. Additional IEP Provisions

4.1. Additional Property Definitions

Document

Name	Description
External Alert 2.0	<p>This document supports exchange from an external source (i.e. alarm company system or other sensor) into a CAD system where a message may be for informational purposes or may be to request an emergency response.</p> <p>There are two primary parties in the communication exchange, the dispatch requesting agency (typically an alarm central station) or requestor and the responding agency (typically a police or fire department or central dispatch point) responder.</p>

Document Sections

Name	Description
Alert	Alert/alarm being reported.
Contact Information	Generally for confirmed responders.

External Alert 2.0 Information Exchange Package Definition

Name	Description
	dispatch in response to an alarm.
Registration	Registration information for any form of conveyance. This would include airplanes, boats, automobiles, etc.
Site Contact	
Vehicle Identification	

Elements

Name	Description
Address Type	Block address, common place or intersection.
Alarm Audible Indicator	Whether the alarm is audible (Y).
Alarm Confirmation Text	Mechanism used to confirm the validity of the alarm. e.g., observed video, live audio, guard verified, call to premises etc.
Alert Event Type Code	The type of the event. Some of the possible values include: <ul style="list-style-type: none"> · BURG - Burglary · Holdup - Holdup / Duress · FIRE - Fire based on smoke detector, heat detector etc · Medical - Medical Alarm · Defibrillator Alarm Activation · Comm - Communication Failure · Environmental Sensor · Fire Trouble - indicates potential equipment problem
Altitude	The altitude measure of the location.
Altitude Reference Point	e.g. ground level, sea level.
Altitude Unit of Measure	The units of measure for the altitude (e.g. feet, miles, meters)
Area Code	Number Plan Area
Attachment Data	Additional information in binary/base64 etc
Attachment Description	
Attachment Name	e.g., file name + extension.
Attachment Size	
Building Designation	The name or number of a building.
Building Usage Text	Describes the usage of the building, e.g. Gun Shop, Nuclear Power Plant
CMV Weight	
CS Event Number	Event identifier, assigned by the alarm company.
CS Receive Date	The date the monitoring Station received the event based on the time zone of the site.
CS Receive Time	The time the monitoring Station received the event based on the time zone of the site.
CS Registration Number	A unique number assigned to Central Station Monitoring Companies
Callback Number	The number of the requestor.
Cell ID	Text that specifically identifies a particular cell tower.

External Alert 2.0 Information Exchange Package Definition

Name	Description
Cell Sector ID	Text that specifically identifies a particular cell sector.
Comment	Comments added to a call for service.
Commercial Identifier	
Commercial Identifier Type	
Coordinate Date	Date that the coordinates were recorded by the device in UTC.
Coordinate Time	Time that the coordinates were recorded by the device in UTC.
Country Code	
County Code	
Cross Street	The address of the site.
Datum	<p>Indicates the Lat/Long system, UTM and projection year. Need to research what NENA standard specifies for preferred Coordinate System to use.</p> <p>Specifies the map projection and coordinate system recommended for the display of longitude and latitude coordinates.</p>
E-Mail	
Encoding Type	base64, mime, hex etc
Event Details Text	Additional details about the event. e.g., indicating the specific location of an alarm, mechanism that potentially triggered the alarm (such as keypad).
Expiration Date	
First Name	
Floor Identifier	
Full Address Text	Unparsed address in full.
Full Name	
General Directions	Directions to the site.
Last Name	
Latitude Degree	
Latitude Minute	
Latitude Second	
Longitude Degree	
Longitude Minute	
Longitude Second	
Make Code	
Message Code	A code identifying the type of message. e.g., Supplemental Information, Initial Notification, Address Verification, Heartbeat, Notification Only etc.
Message Id	Message Identifier that is assigned by the sender.
Middle Name	
Model Code	
Model Year	
Municipality Name	
Name	The name of the site.

External Alert 2.0 Information Exchange Package Definition

Name	Description
Name Prefix	
Name Suffix	
Operator ID	May be name, employee id, initials, or terminal id etc.
Organization Name	<p>The name of the dispatch requesting agency (typically an alarm central station) or the responding agency (typically a police or fire department or central dispatch point) or responder.</p> <p>Organization Name has to be unique across all requestors and responders if we want to use it as an identifier. Otherwise a separate Organization Id will have to be used.</p>
P.O. Box	
PSAP Incident Number	Number assigned by PSAP to uniquely identify an incident.
PSAP Registration Number	
Permit Number	The permit number for the site.
Permit Type	The type of permit.
Plate Issuing Authority	
Plate Number	May be complete or partial
Plate Type	e.g. temporary plates, manufacturer, tail number, dealer plates, hull number.
Postal Code	
Primary Color Description Text	
Property ID	Alphanumeric unique identifier
Property ID Type Code	Indicates the property id type. e.g. Serial Number, Owner applied number
Property Type Code	<p>A commercial or residential event. Values can be 'C' or 'R'.</p> <p>May need to be expanded in future to include other property types such as apartment building.</p>
Room Number Text	Free form text field describing a location e.g. apartment 218, Suite 312.
Site Information	Necessary information about the site. Alert information that may be provided to the responder. e.g., electrified fence, dogs on property, loft apartment, multi-storied building, multiple warehouses on site, hazardous material etc.
Speed	Speed that the coordinates recording device was moving.
Speed Unit Of Measure	miles/hour km/hour ft/sec knots
State Code	
Status Code	Invalid address, Incomplete data, Closed in CAD, Will not respond, Cancel Notification, Reviewed by Dispatcher, Units Dispatched.
Status Description	Format-free text describing the current status

Name	Description
	of an incident.
Street Name	The address of the site.
Street Number	
Street Post Directional	
Street Pre Directional	
Street Type	e.g. Ave., St., Blvd.
Subscriber ID	Last 4 digits of a phone number.
Telephone City Code	
Telephone Country Code	
Telephone Number Extension	
Telephone Number Type	Cell Phone, Fax, Land Line etc
Telephone Prefix	AKA NXX Refers to the exchange which is the three digits following the area code
Test Message Indicator	Set to yes if message is for test purposes only.
Uncertainty Distance	A confidence measure derived from the number of cell sites, distance of the coordinates recorded from the cell site, accuracy of measurement of the coordinates and is typically expressed in meters.
Vehicle Classification	
Vehicle Description	This may indicate the type of vehicle (e.g. airplane, truck, car, boat).
Vehicle Identification Number	
Vehicle Ownership Text	
Vehicle Secondary Color Code	
Vehicle Style Code	

Document Local XML Types

Name	Description
AlarmEventType (ActivityType)	A structure describing an alarm event.
CellLocationServiceType (SuperType)	
EMContactRoleCodeSimpleType	
PermitType	A structure describing a permit.
ResourceComponentCapabilityTypeCodeSimpleType	

Document Local XML Elements

Name	Description
AlarmAudibleIndicator	True if an audible alarm is sounding; false if the alarm is inaudible.
AlarmConfirmationDescriptionText (TextType)	Mechanism used to confirm the validity of the alarm. e.g., observed video, live audio, guard verified, call to premises etc.
AlarmEvent (AlarmEventType)	An alarm event.
AlarmEventDetailsText (TextType)	Additional details about the alarm event.
AlarmEventLocation (LocationType)	The location of the site of the alarm event.
AlarmEventLocationTypeCode (TextType)	A code identifying the kind of location at which an alarm event occurs.
AlarmEventPermit (PermitType)	A permit for the alarm event site.

Name	Description
Attachment (DocumentType)	
CSEventNumber (TextType)	Event identifier, assigned by the alarm company.
CellID (IDType)	
CellLocationService (CellLocationServiceType)	Provides information about the location of a cellular phone.
CellSectorID (IDType)	Identifies the sector of a cellular network
MonitoringStation (OrganizationType)	Represents an organization, such as a private alarm company, that has the responsibility for responding to a premises or other hazard alarm.
PSAPIncidentNumber (TextType)	Number assigned by PSAP to uniquely identify an incident.
PermitID (IDType)	A permit number.
PermitTypeText (TextType)	A type of permit.
PublicServiceAccessPoint (OrganizationType)	Represents a centralized dispatch organization.
RecordedSpeedRate (RateType)	The speed rate of the target as measured by the GPS.
TestMessageIndicator	Set to yes if message is for test purposes only.

4.2. Minimal Properties Set

4.3. Additional Business Rules

4.3.1. Description

1. The working team shall utilize the following performance measures to focus project goals and to measure implementation success.
 - a. Reduce number of calls to from central stations to PSAPS
 - b. Reduce overall response time for alarm-based calls-for-service
 - c. Decrease errors in delivery of alarm and calls-for-service by eliminating voice delivery and PSAP call taker CAD re-entry
 - d. Progress toward a standard for interfaces between monitoring stations and PSAPs to reduce cross-agency and cross-vendor data exchange development time and cost
2. Alarms and requests-for-service will be transmitted to PSAPs per normal procedures even when a catastrophic event (e.g. hurricane) or mass alarming event (e.g. wind or electrical storm) makes the PSAP choose not to respond. This places the PSAPs in control of filtering requests and provides for historical information in their CAD or front-end processing engine.
3. Fusion Center and or other Department of Homeland Security information needs will be met via the CAD and or PSAP systems and processes and will not be met directly by creating exchanges between the monitoring stations and these DHS systems.
4. The need for an authentication, security, message broker engine is being managed by Bill Cade and Pam Petrow where possible NLETS support is being negotiated. This

?messaging? component of monitoring station-to-PSAP exchanges is not considered within scope of this project.

5. Monitoring stations will not take ownership of denoting ?high risk? locations in their alert or ?request-for-information? exchanges since no standard definition of high risk criteria currently exists. It is thought that most PSAPS and CADS provide such functionality and ownership and asking the monitoring stations to add this information could cause a conflict-of-interest and would likely create confusion.

6. Many PSAPS will likely phase in functionality associated with automated monitoring station exchanges into their CAD or front-end interface. For instance, the PSAP may initially wish to review every exchange and force call-taker ?acceptance? before CAD downloading and then begin to support automatic acceptance for certain types of alarms over time as trust and comfort builds.

7. NENA standards will be utilized for addressing since these standards are typically utilized by PSAPS and CADS.

8. An implementation guide should be created to accompany these IEPs which minimally includes;

a. Suggestions about how and when to validate and reconcile subscriber addresses across monitoring station and CAD/PSAP systems (e.g. registry server).

b. Recommendations about ways to secure security between systems and to minimize spamming threats.

c. Explanations about the possible ?phasing? of automatic alarms into a CAD.

9. The following alarm or request-for-service exchange rejection reasons shall be utilized;

a. Closed in CAD (for supplemental exchanges)

b. Invalid address (where address data does not reconcile between systems)

c. Invalid data (exchange does not contain required field elements)

d. Incorrect jurisdiction (customer/location not covered by receiving PSAP)

e. Unauthorized customer (for situations where location has exceeded false alarms)

f. Diverted (where PSAP is not accepting certain alarm types, locations, etc? due to catastrophic event or other PSAP driven reason)

10. Alarms triggered based on RFID data elements will require additional definition and research not considered within scope of this 2.0 IEP release attachment reference path or location.

11. Data elements such as ?patient name? or ?incarcerated person name? will be included in free-text notes section versus having a pre-define field since RFID and Defibrillator Alarms are still evolving.

12. Telematics data transmission is not supported by this schema definition.

4.3.2. Data Exchanges

1. During the In-process state, at the Alarm Activation event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a

notification is required the Monitoring Station sends the External Alert 2.0 to the PSAP for the Evaluate Event event in the In-process state.

2. During the In-process state, at the Evaluate Event event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If PSAP takes ownership of the notification alert the PSAP sends the External Alert 2.0 to the Monitoring Station for the Update Call Record event in the In-process state.

3. During the In-process state, at the Evaluate Event event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If PSAP rejects ownership of the notification alert the PSAP sends the External Alert 2.0 to the Monitoring Station for the Update Call Record event in the In-process state.

4. During the In-process state, at the Evaluate Event event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If PSAP takes ownership of the notification alert & If the PSAP changes the status the PSAP sends the External Alert 2.0 to the Monitoring Station for the Update Call Record event in the In-process state.

5. During the In-process state, at the Update Call Record event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If PSAP takes ownership of the notification alert & If the PSAP changes the status & If update is acknowledged the Monitoring Station sends the External Alert 2.0 to the PSAP for the Update Call Record event in the In-process state.

6. During the In-process state, at the Update Call Record event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If PSAP takes ownership of the notification alert & If Monitoring Station changes the status the Monitoring Station sends the External Alert 2.0 to the PSAP for the Update Call Record event in the In-process state.

7. During the In-process state, at the Update Call Record event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If PSAP takes ownership of the notification alert & If Monitoring Station changes the status & If update is acknowledged the PSAP sends the External Alert 2.0 to the Monitoring Station for the Update Call Record event in the In-process state.

8. During the In-process state, at the Sensor Activation event, If CSAA 1.0 messaging protocol is not implemented & If an environmental sensor is triggered the Environmental Sensor sends the External Alert 2.0 to the PSAP for the Evaluate Event event in the In-process state.

9. During the In-process state, at the Request Alert Information event, If CSAA 1.0 messaging protocol is not implemented & If the Monitoring Station determines a notification is required & If Monitoring Station is authorized the Monitoring Station sends the External Alert 2.0 to the PSAP for the Evaluate Event event in the In-process state.

5. Samples

6. Development

6.1. Participants

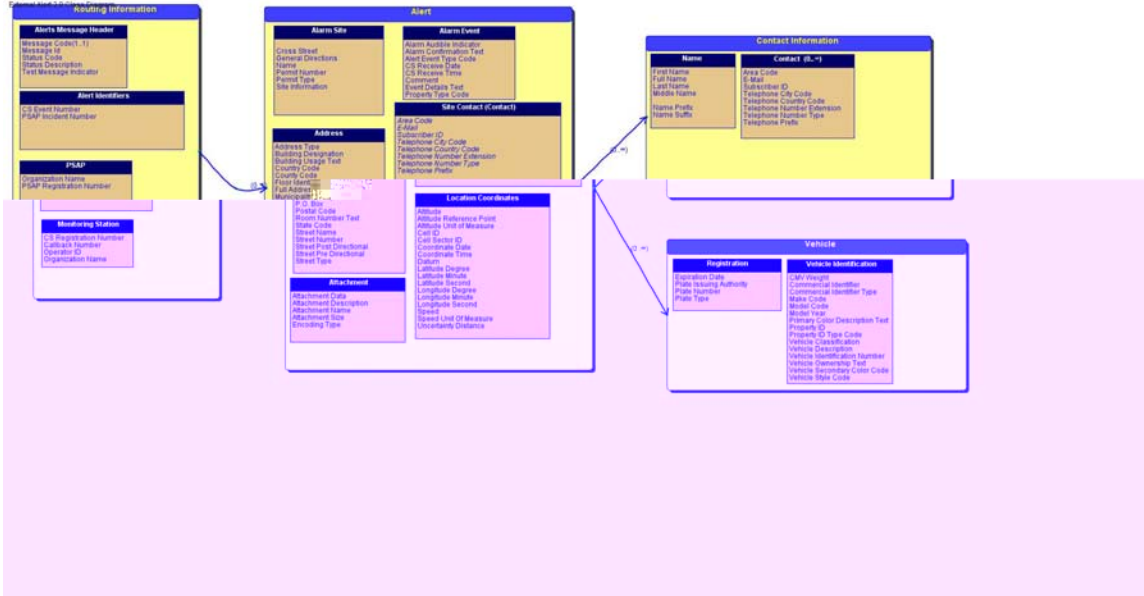
Holly Barkwell-Holland: Fire Monitoring Technologies
Jerry Cowser: Vector Security
Pamela Petrow: Vector Security
Bruce Weissman: GE Monitoring Automation Systems
Adam Eurich: Dice Corp
Bill Cade: APCO/Office 911 Service
Martin Moody: APCO/Office 911 Service
Alan Harker: Spillman Technologies
Randy Syth: Sungard HTE
Aaron Gorell: URL Integration
Vivek Misra: URL Integration
Suzette McLeod: IJIS Institute
Neil Kurlander: Asynchronous Solutions
Heather Ruzbasan: IACP/LEITSC
Matt Snyder: IACP
Tom Steele: Delaware DHS
Alan Komenski: Bellevue, WA
Stephen Wisely: Onondaga Co 911
Jim Cox: Port Orange Public Safety
David Wagner:

6.2. Process:

The Alerts Working Team met in Daytona Beach, Florida on February 21st, 22nd, and 23rd of 2006 to begin Information Exchange Package Document (IEPD) development. This working team was formed by the IJIS Public Safety Technical Standards Committee (IPSTSC) to create external alerts and requests-for-service IEPDs. Twenty of the twenty-three invited participants attended and were successful in accomplishing all meeting objectives.

6.3. Development Artifacts:

6.3.1. Data Model Diagram



6.3.2. Source Documents

6.3.3. Revision History:

7. Testing and Conformance

8. Feedback