Handling of EDXL-DE messages for emergency information distribution with JIXEL Share
Presentation outline

• Introduction to Intelligence for Environment & Security Solutions (IES Solutions)

• **EDXL-DE** introduction and purposes

• IES Solutions’s product **JIXEL Share**

• Routing of information with JIXEL Share
  • handling of EDXL-DE messages in JIXEL Share
IES Solutions

• Intelligence for Environment & Security
  • Software development and System Integration since 2004
  • Cloud based solutions for the security of citizens and for the environment
  • Located in Rome, Catania (Italy) and Oxford (England)

• We strongly believe in the concept of interoperability, for improving the communication between citizens and authorities

• We develop projects funded by the European Commission (17 until today):
  • our projects have been mainly focussed to the emergency management sector (REACT, REACH112, IDIRA, ESENet, EmerGent, EPISECC, I_HeERO, ALPDIRIS)
EDXL-DE

• EDXL-Distribution Element (EDXL-DE) is the XML format developed by OASIS for Standardized Routing of information

• It provides the envelope within which different type of payloads can be carried for distribution purposes

• EDXL-DE payload examples:
  • Emergency Messages represented in one of the other EDXL standards, like CAP, EDXL-SitRep, EDXL-RM, and so on
  • Any other XML and non XML message content
  • Other digital resources, like images, audio and video files
Our Products

<table>
<thead>
<tr>
<th>ALERTER</th>
<th>AGGREGATOR</th>
<th>MANAGER</th>
<th>SHARE</th>
</tr>
</thead>
</table>

![JiXel Logo](image1)

![JiXel Logo](image2)

![JiXel Logo](image3)

![JiXel Logo](image4)
JIXEL Share #1

• JIXEL Share offers tools and functionalities for data sharing and data exchange between Authorities, Emergency Services, crisis management actors and critical infrastructures owners

• It’s a set of web-based software services that can be either provided as Cloud services, or deployed on premises

• Easily configurable and highly customizable, it allows the user:
  • to define password protected web feeds for publishing information for specific recipients
  • to define custom distribution rules
  • to create user profiles and segmentation patterns for tailoring the amount of information shared with any specific recipient
JIXEL Share #2

• Main software elements:
  • REST or Web Service API to accept inbound messages (CAP, EDXL-DE, other EDXL formats)
  • Internal services and libraries for:
    • standard messages validation according to the specs (e.g. CAP v1.2, EDXL-DE v2.0)
    • check and application of specific routing and masking rules for incoming messages addressing
  • Outbound interfaces for distributing messages to the intended recipients
    • Supporting ATOM Feeds
    • Supporting MESSAGE BUS
JIXEL Share #3

• A typical scenario
  • different information types and formats are received
  • they are handled internally and then shared with the intended recipients according to pre-defined addressing rules
THE ROUTING MECHANISM

- ATOM Header
- CAP Message
- ATOM Closing

Recipient 1
Recipient 2
Recipient n

Dedicated, encrypted FEED

Message bus topic
EDXL-DE Envelope
Recipient 1
Recipient 2
Recipient n

Message bus topic
EDXL-RM
EDXL-DE Envelope

Recipients parsing Profile application Distribution rules
Routing with JIXEL Share

• Two different Scenarios
  • Scenario #1 - incoming information in EDXL-DE format with any payload
    • distribution information (rules) are retrieved by looking at the EDXL-DE envelope
  • Scenario #2 - incoming information are in other EDXL (e.g. CAP) or non EDXL formats
    • existing pre-configured distribution rules to be applied for a given sender and according to the information type, are either retrieved by looking at the JIXEL Share configuration ...
    • ... or derived from the incoming message content. For example, in case of private CAP messages, the intended recipients will be available in the alert.addresses field
EDXL-DE in JIXEL Share: Scenario #1

• an EDXL-DE message is received
• lookup of the relevant EDXL-DE fields and cross-check of configured routing rules, to understand how the information should be distributed (e.g. list of recipients)
• for messages which should be shared with external systems:
  • either the payload is extracted (in case of CAP messages payload) and published as ATOM feed entries in dedicated and password protected feed channels for each recipient ...
  • ... and/or the full EDXL-DE message is published in dedicated message bus topics to be consumed by the recipients’ systems (for any other type of payload)...
• for messages addressed to the same system where the JIXEL Share is running:
  • the payload is extracted and stored for internal handling
EDXL-DE in JIXEL Share: working case #2

- the information is received in **non EDXL-DE format** (it can be either CAP, or another EDXL or non EDXL resource)

- for messages which should be shared with external systems:
  - in case of CAP messages
    a) the message is validated and read to check for the sender and the recipients
    b) existing filters (profiles) and routing rules for each given sender / recipient pair are verified
    c) then new EDXL-DE messages are created (one for each sender / recipient profile found) and **published in dedicated message bus topics** to be consumed by the recipients’ systems
  - in case of different resources types
    a) existing filters and routing rules are verified for the given sender and according to the incoming message type
    b) new EDXL-DE messages are created (one for each sender / recipient profile found) and **published in dedicated message bus topics** to be consumed by the recipients’ systems

- for messages addressed to the same system where the JIXEL Share is running:
  - the message is stored for internal handling
Share IS

• A single, one stop shop, service for interoperability
• We support EDXL family of standards
• We use ATOM and Message BUS
• We can import any kind of existing messages and use it in our SW