COLLABORATION SERVICES

Chat Service

Chat Service

Collaboration among parties taking part in an operation is crucial for the success of the mission. Users need to exchange orders, tasks and reports making sure that all entities have common understanding of both the situation and the mission goal.

The solution to support collaboration among mission participants is the use of chat service. It allows to create COIs interested in particular subjects (e.g. situational reports and alarms) as well as bidirectional information relations targeted to the exchange of orders and reports.

Chat service assures privacy and confidentiality of conversations among different COIs. The access is protected by the authentication service. Each message is augmented with the security label which makes it possible to be released by border security guards (e.g. XML guard).

Chat service allows to transfer both structured and unstructured messages. It strongly supports collaboration with the use of instant messaging. With the use of COIs on different levels of classification it is possible to provide direct contact between cooperating civil and military units.

Benefits

- Supports creation of COIs and collaboration among mission participants.
- Provides possibility to send structured messages (e.g. reports, orders) and unstructured messages (free text, alarms, warnings).
- Supports presence context handling.
- Provides instant messaging among mission participants (Single Room Chat) and information distribution to subscribed users (Multi Room Chat).
- Multi Room Chat can be used to create information channels on particular topic to subscribed users (e.g. weather information, video sensors URLs, etc.).
- Supports border protection with the use of security labels.
- Supports creation of ad-hoc communication channels.

Architecture

- Chat service is one of the SOA collaboration services. It provides instant messaging on the basis of publish-subscribe architecture. The architecture of the solution is based on XMPP protocol, originally designed to be extensible. This makes it also useful to provide e.g. file transfer, Internet of Things applications such as the smart grid, and social networking services.
Demonstration of Shared situational awareness in EU led Crisis Management Operation was delivered by a consortium led by Asseco Poland SA (Poland) and comprised of Military Communication Institute (Poland), Military University of Technology (Poland), ITTI Ltd (Poland), Filbico Ltd (Poland) under the European Defence Agency project No. 13-115-CAP.

The solution is based on distributed client-server architecture. Each chat server provides the possibility to subscribe to multiple topics created in the form of chat rooms. The topics are targeted to exchange particular types of information, e.g. intel reports, tasks and orders, alarms and warnings. Different chat rooms are created also based on confidentiality of the data granting access only to users with appropriate credentials.

Chat service is based on the following standards and solutions:

- Asynchronous statefull communications
- User presence context handling
- Extensible Messaging and Presence Protocol (XMPP) based on XML
- SASL or TLS encryption

TRL: 6.

**Technology provider**

Service provided by Military Communication Institute.
UE NEC Demonstration - PT NEC initiative for a collaborative project between EDA and pMS to host a practical demonstration of operational relevance of NEC started in late 2010. Out of 7 pMS proposals, Polish consortium was selected with "Shared Situational Awareness in EU-led CMO" demonstration. Project started in January 2013 with the demonstration planned for 27/28 November 2013 in Warsaw.

The demonstration scope included: Presentation of CSDP driven EU-led CMO scenario; Presentation of capabilities prepared by Polish consortium members to form a distributed CIS/C2 environment, as a configuration of their selected IT assets (PL NEC). These capabilities included inter alia situational information presentation (pictures and portals), knowledge management, information assurance and cyber threat identification & assessment; simulation of three operational episodes: Civ/mil response to IED incident, Ad-hoc civ/mil collaboration and Terrorist threat identification and response; Demonstration of PL NEC architecture, services and tools.

NEC Demonstration was provided by a consortium led by Asseco Poland S.A. with partners: Military Communication Institute, Military University of Technology, ITTi Ltd. and Filbico Ltd.