POLAND

Shared situational awareness in EU led CMO

EUROPEAN DEFENCE AGENCY

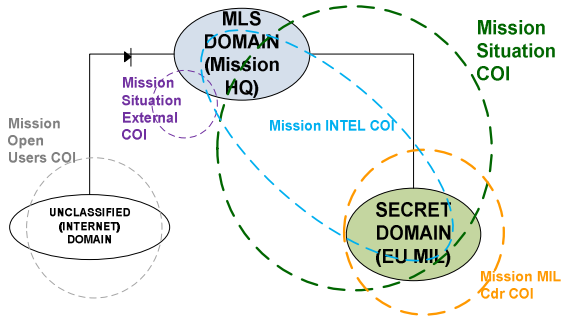
EDA project No. 13-115-CAP

Multilevel Security Services

Civil – military operations require exchange of up-to-date information among parties that are equipped with different communications systems. Those domains very often differ in levels of classification and pieces of data sent between them have various confidentiality.

Multilevel Security Services (MLSS) are designed to support cross-domain secure information exchange among independently managed trusted parties. They follow SOA paradigm and support both MLS and MILS types of domains.

MLSS are SOA core services protecting information retrieval. With MLSS access to resources is granted only to authenticated and authorized users even though they are coming from different domains.



MLSS supports creation and management of COIs. It enables creation of shared situational awareness on different levels of command in all domains operating in the federation. With the use of this approach all COIs engaged in the operation (civil and military ones) have reliable information that they need for fulfilling their tasks.

MLSS can be used in SOA-federated environment scenarios involving EU, EU nations, NATO, NATO nations, non-NATO nations, coalition forces, Non-Governmental organizations (NGOs) and other civilian and military organizations.

Multilevel Security Services

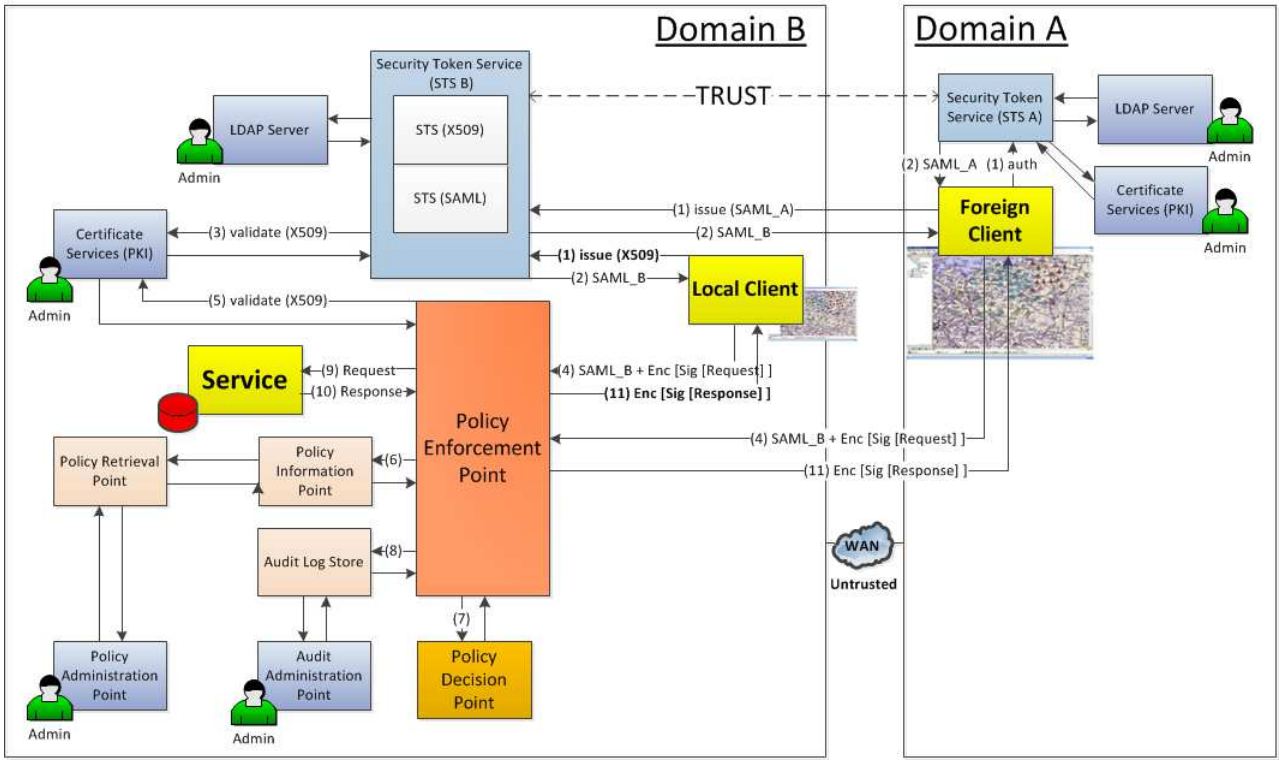
Benefits

- Ensures secure exchange of information between civil and military parties with the same or different levels of classification
- Adaptable to broad range of security requirements and policies
- Releases information only to authenticated and authorized trusted parties on the basis of security policy and data label
- Verifies credentials of users of every domain in the federation
- Supports privacy and confidentiality of information flows (encryption)
- Enables interoperability in SOA federated environment
- Ensures cross domains information sharing.

Architecture

Multilevel Security Services have been designed in accordance with the NEC/SOA concept. They are core services supporting operation of any functional service. The MLSS environment consists of the following components:

- Security Token Service (STS) (X509/SAML), LDAP Server
- Policy Enforcement Point (PEP), Policy Decision Point (PDP)
- Policy Information Point (PIP), Policy Administration Point (PAP), Audit Administration Point (AAP), Policy Retrieval Point (PRP)



Multilevel Security is based on the XACML architecture. Each request for information is augmented with so called security token that includes information about user identity confirmed by the trusted CA (Certificate Authority) and user credentials (e.g. user role in particular mission). This allows to grant access to remote resources to domain external users on the basis of trust relationship between federated domains.

Security tokens are produced by Security Token Service (STS). For local requests (within the same domain) STS confirms identity of users on the basis of their X.509 certificates (step 1). For external requests STS provides SAML tokens that confirm the identity of the local user that can be used in external trusted domains to request for information (step 2). Only with valid SAML security token the user can request for information from secured service (step 4).

Authorization service with the use of Policy Enforcement Point (PEP) provides access control to protected resources. Firstly it verifies if the token is valid and its contents did not lose integrity (step 5). Then, it checks currently valid security policy (step 6) and cooperates with Policy Decision Point (PDP) (step 7) that compares user privileges with security policy making decision about granting or denying access to resources. PEP operates as a proxy for information retrieval and encrypts service response ensuring privacy and confidentiality of information exchange (step 11).

Access will not be granted e.g. when (a) the user has invalid X.509 certificate, (b) the SAML token has expired, (c) according to valid security policy user credentials do not allow to him access requested resource.

Technology

MLSS implementation is based on commonly used standards:

- WS-Security, WS-Trust, Security Assertion Markup anguage (SAML) and eXtensible Access Control Markup Language (XACML)
- Public Key Infrastructure, X.509 certificates and CRLs, LDAP

TRL: 8.

Technology provider

Services provided by Asseco Poland S.A. and Military Communication Institute as a result of R&D project "Prototype of multilevel security system for cross-domain information exchange in the SOA environment", granted by Polish Ministry of Science and Higher Education through founds assigned for science in fiscal years 2010-2013.

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.

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.

International Organization and Security Sector Solutions Department of Asseco Poland SA specialises in designing and development of specialised military and double use software including advanced security solutions. As a member of the largest software house with Polish capital and seventh largest software house in Europe, we are proud to successfully compete with the worldwide market global companies and provide services to NATO, European agencies and other international organisations. We have successfully passed a SCAMPI-A formal appraisal which confirmed that all processes adopted by PRW were implemented on the Level 3 of CMMI-DEV.

Military University of Technology is the largest military academic facility in Poland, providing educational, research and development capabilities to Polish Armed Forces and government institutions. Cybernetics Faculty was founded in 1968 in response to the growing demand for specialists in the domain of computer systems and in particular decision support, computer simulation, cryptology, operational research and methods to assist the decision-making processes of military commanders. Scientific research has been applied in many products deployed for Polish and foreign DoDs providing software and hardware components (Military Decision Support Systems, HLA based virtual and constructive simulators, cryptographic modules, crisis management tools).

Military Communication Institute is an R&D institute supervised by Ministry Of National Defence, funded in 1951. It realizes researches and development projects inter alia in the area of cryptographic and electromagnetic protection, information assurance, cyber defence, building C4I systems' mechanisms and services, communication systems, radio-communications, reconnaissance and electronic warfare systems. Many of the MCI products are applied in practice and fielded in Polish Armed Forces. MCI has ISO and AQAP certificates, Ministry of Interior licence and 1st degree certificate of industrial safety (EU, NATO SECRET and national up to TOP SECRET).

Filbico is an engineering company which provides the Information and Communication Technology solutions for forces and uniformed services. The company supports the full life cycle of ICT systems: from research up to the maintenance. Our business areas are the air traffic control and management, cyber security, crisis response, command and control as well as fire control. Filbico's capabilities are recognized in several certificates required to successfully develop mission critical systems for military customers. Web page: www.filbico.pl.

ITTI Sp. z o.o. is a private company focused on technical consulting and applied R&D in the area of IT and telecommunications as well as on development of innovative applications and software solutions. ITTI has been working in EU Framework Programmes, PASR, EDA projects (e.g. JIP-FP) and in NATO Industrial Advisory Group studies. ITTI has been awarded the prestigious "Cristal Brussels Prize 2010" and has received an award for the high performance in R&D projects for European Defence Agency granted by Polish Ministry of Defence. ITTI is a member of the following international organisations: PSCE, IMG-S and ITIC Group.