Security and Confidentiality in Interconnected Networks

Aljoša Jerman Blažič
SETCCE
Ljubljana, Slovenia
aljosa@setcce.si

Svetlana Šaljić
SETCCE
Ljubljana, Slovenia
svetlana.saljic@setcce.si

***Abstract*— With the rapid development of interconnected environments many technical and organizational aspects are being addressed in relation to atomized services operating across networked domains. Some of those aspects still need further examination and evaluation also from security perspective. Data may traverse several organizational, security or information domains in order to be processed and results delivered. This calls for proper technical and organizational design approaches, which include means for secure data exchange. Various aspects of secure information exchange are already being addressed by different business, administration, defense and other professional initiatives. The aim of this paper is to present results of the ongoing activities for development and deployment of secure interconnected networks and to demonstrate a framework that shows the relations between relevant security requirements and security mechanisms that can be applied to fulfill the requirements of interconnected domains. The scope of security requirements and mechanisms spans the network, application and information layers.**

Keywords-component; seruity domains, confidentiality, secure data exchnage, security requirments, security mechanisms

I. INTRODUCTION

The importance of sharing information across organizational or technical domains is commonly recognized in many professional areas. Novel business or administration concepts supported by technical infrastructures rely on disperse data processing, with services deployed location independent across open networks. These requirements have also been moved to other fields with high security requirements and standards such as governmental or defense organizations [1], which today rely on infrastructures with limited or no connectivity. Data being pushed across network boundaries must be addressed form organizational and technical aspects [4, 5, 13, 15]. In many cases these data may carry sensitive information such as financial statements, governmental decisions or military orders.

In the vision of future networks everyone and everything is connected in order to allow for information sharing: the right information, at the right place, at the right time. Furthermore, dispersed processing power means that information can be processed simultaneously or in sequence at different locations or within different domains and results then combined. Ever increasing throughput, new (web) services based frameworks or cloud computing concepts for instance present foundations for information exchange, shared data processing and distributed storage. However, when it comes to sensitive information, e.g. personal, financial, governmental or even military, sharing requires harmonization and change of the existing capabilities and change in terms of doctrine, processes, personnel, culture and organization.

Examples of information sharing are to be found in many domains e.g. health services, which may combine several organizations exchanging information in order to provide proper and professional health support. Telemonitoring for example requires health services to reach patients across several networks and organizations. Health parameters may be collected from patients on the field by sensor and mobile services providers and then processed by e.g. public health institutions. Corresponding service response may then be delivered by specialized health service provider, which may be operated on private basis or patient’s relatives and professional health personnel in geographical proximity are informed on downgraded health status. It is obvious that in such scenarios data flows may traverse several organizational and security domains and be processed on distributed basis, which only imposes the risk of sensitive information leakage.

Another important concept in this context is Network-Enabled Capabilities (NEC) defined by defense and coalition organizations such as NATO [1, 12, 13, 15]. Defense operations may require fetching data from different organizations such as national weather system, then processed by military geographic data provider and final results on contaminated areas delivered by defense organization to public announcement system in case of e.g. chemical warfare. However, more recent military operations require cooperation of different organizations not only on national basis but on much wider scope between coalition partners. Such future networks are known by the term Network and Information Infrastructure (NII), which is in fact an ever-developing coalition-wide multinational military intranet alike network.

Better integrated networks mean that sharing relevant information will be easier and quicker and that more people will be reached than before. The technical basis for networked operations lies in a secure, robust and extensive federation of networks, a large network consisting of a number of smaller individual networks. This is the case for any area and domain, i.e. business, public administration, non-for-profit organizations and defense organizations.

ISBN: 978-1-61208-116-8

While technical concepts and mechanisms that support secure data exchange (e.g. access control, encryption, confidentiality labeling) are already well understood and a plethora of technical solutions are being widely implemented and put in practice such as [16], [17], [18], [19], [20], [21], etc., requirements of network and information connections and their functional security in the context of interconnected networks still remains unknown or poorly understood. In this paper we present the attempt to design a framework for collecting requirements, which focus on security mechanisms needed on both the network connection level and the information exchange level. The ultimate aim of the on-going work is to develop a methodology for designing high level system architectures for network and information connections and their associated security mechanisms that support a controlled exchange of information in different contexts. The work presented has background on coalition needs to deploy NII infrastructures, while results presented have much broader impact and may be used in any multi-domain scenarios with sensitive information flows. The primary focus of the paper is to describe a framework, which is supported by identifying some key security requirements and indicating how the framework could be developed and used to address the issues of secure networks interconnection.

II. Sharing Information Across Domain Boundaries

In this paper we address the problem of secure information exchange across domain borders. For this purpose we distinguish four different types of domains:

- Security domains; these domains are defined by the security requirements that apply, e.g. based on a security policy or classification level implemented by a single domain.
- Organizational domains; these domains span the collection of information, systems and infrastructure for which a single organization is responsible, e.g. a domain operated by a single organization.
- Technical domains; these are defined by a collection of technical means used to enable information processing and communication, e.g. local area network.
- Information domains; these are defined by a set of information that is used in a specific functional context by a community of interest (CoI), e.g. information related to a specific business, administration or defense process.

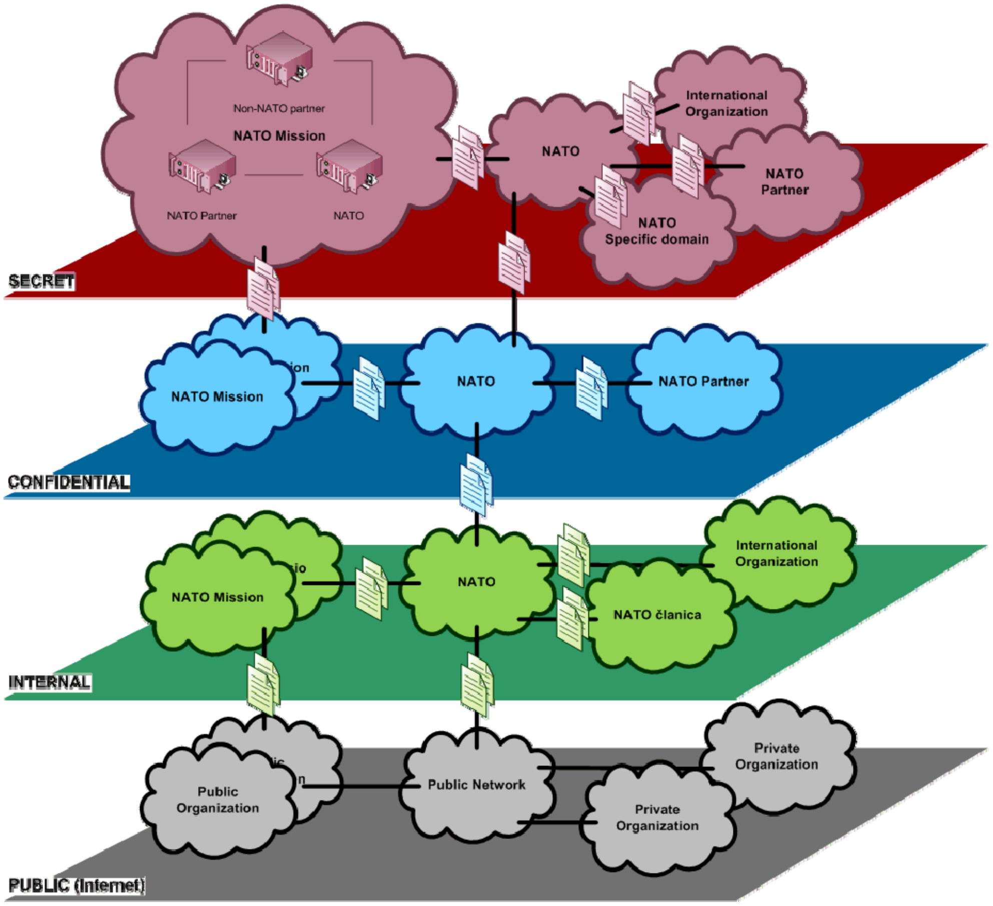

Figure 1. Information flows crossing different domain boundaries.

ISBN: 978-1-61208-116-8

These domain types provide different perspectives on an information infrastructure. A reason for distinguishing between domain types is that they pose different security requirements with respect to information exchange. When exchanging information one should be aware of which domain boundaries are crossed. Subsequently, relevant security requirements should be identified for each domain boundary individually. Figure 1 illustrates how domains can interrelate in case of coalition organization such as NATO. Information flows may cross different security or organizational domains. In order to prevent unauthorized access or interception in such conditions, data exchange is to be performed in a controlled manner using appropriate security means and organizational measures.

Secure data exchange depends on the context, which addresses crossing at least one boundary (one domain), while many scenarios exist where more than one boundary is being crossed. When multiple domains of different types are crossed an order for the resulting transition sequence must be identified. This can be interpreted by a multidimensional system, where each axis presents one domain type and points in the coordination system data origin, data final destination and data boundaries crossings. Figure 2 presents multi-domain crossing in a three way coordination system.

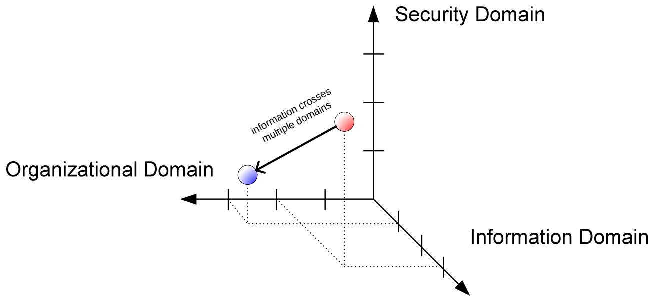

Figure 2. Interpretation of information flow domain crossing in three dimensional coordination system.

Sharing information between security domains presumes a way of determining whether a specific information object may or may not be shared. Each information object has a set of security properties that are relevant in this process.

When sharing information a number of general security requirements apply:

1. Making sure that information in a domain can be accessed (community of interest) while access to confidential information is limited according to a set policy (need to know).
2. Allowing information objects to be shared with anybody outside the security domain, while confidential information that should not be shared is protected against unintended release.
3. Managing the flow of information objects over different security domains, based on a shared security policy, e.g. mission-specific or process-specific classifications may be used to support information sharing within a mission or a process while preventing data leakage outside the mission or the process.

Setting up technical and organizational environment that supports such crossings is based on a framework of security mechanisms. Framework is a structured approach to select applicable security mechanisms which operate on different (technical) layers. For the purpose of this paper we differentiate between the network, application and information layers:

- Network layer addresses physical, (inter)network and transport protocols, such as TCP/IP;
- Application layer addresses application-specific protocols such as HTTP, MMHS but also proprietary system interfaces.
- Information layer addresses the actual information payload which may be encoded and/or encrypted.

Security mechanisms may come in various forms and may be applied in different combinations and technical implementations. Their role and function is presented by diagram showing to what layer each mechanism could be applied. It is important to understand that implementing a security mechanism on one layer may impact mechanisms working on other layers. An example is the application of network encryption, which renders application layer packet filtering useless.

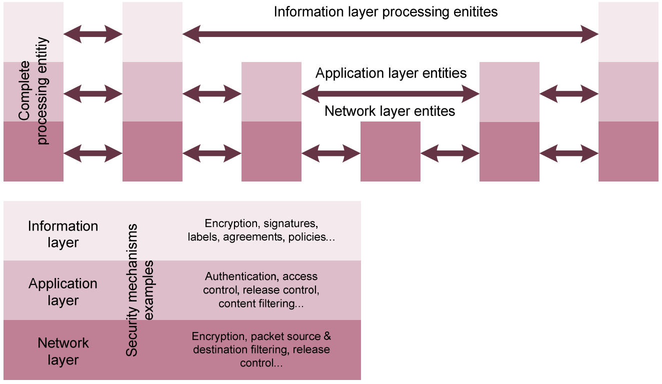
Complete processing entitiy
Information layer processing enitites
Application layer entities
Network layer entites
Information layer
Application layer
Network layer
Security mechanisms examples
Encryption, signatures, labels, agreements, policies...
Authentication, access control, release control, content filtering...
Encryption, packet source & destination filtering, release control...

Figure 3. Security mechanimsms and their application on different layers.

Figure 4 presents an example of secure information exchange between two different security domains. In this case, the following mechanisms are being used: confidentially labeling for selecting information classification level [1], XML guard as release control mechanism [1, 15] and data encryption [18] as access prevention or control mechanism. Both domains have their security policies aligned and classification categories are adjusted. Data being sent from domain A to domain B means that information flow is supported form a higher to a lower classification network. XML Guard is deployed as release control mechanism, encryption is used to support data exchange across unknown networks and classification label is used to support exchange of information on data confidentiality level.

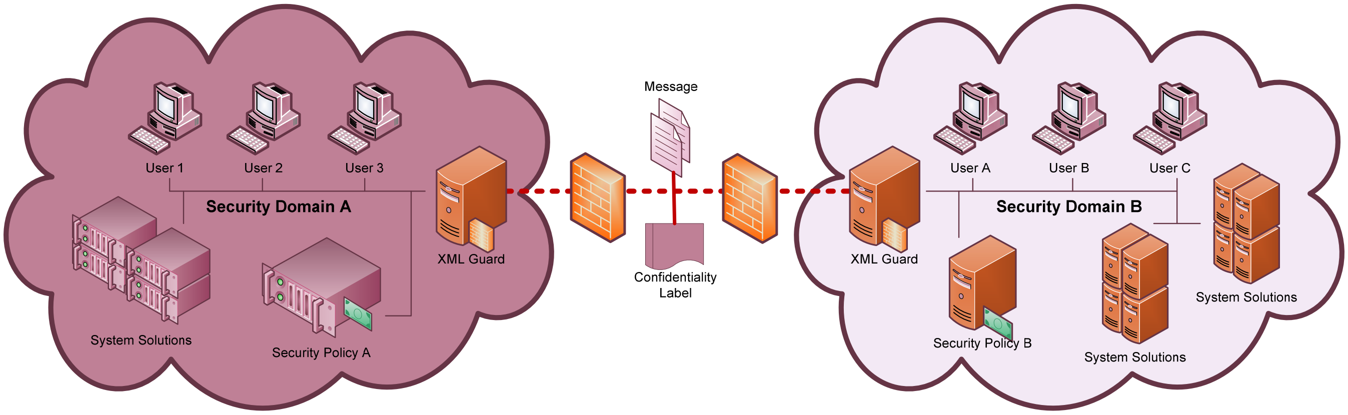

Figure 4. Secure data exchange between different security domains..

III. Security Requirements

Setting up secure environment for inter domain information exchange requires framework of organizational measures and technical means. The primary scope of this paper is to present findings on security requirements and security mechanisms related to secure data exchange, and their role within the interconnected domains. The work relates to national defense and coalition initiatives on network enabled capabilities concepts and interconnected networks.

In order to support secure information exchange across different domains data security (exchange) context has to be first defined. Data security context is associated with many scenarios and has to be addressed with for example exchange of information during defense or tactical operations. The security context includes parameters on degree of data sensitivity in terms of unauthorized access (this is usually defined with the classification category) and how classified data is to be managed. These are the basic considerations based on which security requirements are then collected.

For better understanding the following topics are not in scope for the framework. They do however need to be addressed when the framework is implemented in practical situations.

A. Policies

Policies are a set of decisions that are made on the organization level. Security requirements and related security mechanisms can be used to enforce these decisions. It is important to note the fundamental difference between a decision made by a responsible entity (i.e. to give a document a certain classification) and the enforcement of such a decision within the infrastructure (i.e. by either blocking or allowing a document to be transferred to another domain).

B. Relation to organization and management of information

With the increasing introduction of enforcement mechanisms in the infrastructure the link between infrastructure, organization and management of information becomes more interrelated. These relations can present complex and dynamics characteristics and for the purpose of the work presented relations are static and known. The actual organization and management of information and related processes are therefore outside the scope of this paper.

C. Non-security requirements

The requirements presented in this paper are limited to examples within the security scope. In order to limit the negative impacts e.g. functional and interoperability issues, additional requirements are needed.

Results presented in this paper do not have explicit intention to give a comprehensive overview of all possible security contexts. Rather it describes the basic problems of cross boundaries affection when data are exchanged across domains. In the table below key requirements for secure data exchange applicable to e.g. defense scenarios are summarized.

TABLE I. A list of identified requirments for secure information exchange across domain boundaries

No.	Requirement	Explanation
1	Information confidentiality	General requirement for data being exchanged between domains
2	Confidentiality breaches detection	Detection of unauthorized downgraded data classification
3	Change/alteration detection	Applicable for complete lifecycle of classified data
4	Information integrity	Applicable for complete lifecycle of classified data
5	(Authorized) changes propagation	Propagation (of security context changes) to relevant entities in communication
6	Trust-relation(s)	A trust-relation between parties established before exchanging information
7	Information non-repudiation	Applies for originating and receiving domain
8	Policies enforcement	Decisions on information

		exchange must not be in violation against policies
9	Policies availability	Availability of all relevant policies for an information set is ensured at all times
10	Explicit policies decisions	Information can be exchanged only when classification level is defined and adjusted
11	Deviations of policies	Deviations from policy should be possible but always detectable
12	Anonymity	Ensure anonymity of data sources (entities)
13	Limited access	Only specified subjects should have access to specified objects – need to know principle
14	Audit trail and integrity demonstration	Information actions trusted log and demonstration of information integrity

The list of collected requirements presented is in scope of defense administration, operation and decision making processes. The intention of listed requirements is not to present a comprehensive list applicable to any scenario or professional area. Other areas may need to implement additional or different requirements. However, most of the requirements are applicable to other areas, such as financial or governmental institutions, while presented collection is used primarily to demonstrate how to set up a framework for secure information exchange in defense scenarios.

IV. SECURITY MECHANISMS

Next, a set of security mechanisms that support secure information exchange in multi domain environment is collected. For each mechanism a short description is given in the table below. This is not architectural proposal but a basic collection of mechanisms needed to support secure data exchange. Conceptual and final architecture must address and include mechanisms, which are selected according to the requirements identified for specific scenario of secure data exchange.

TABLE II. A LIST OF SECURITY MECHANIMSM RELEVNT FOR SECURE INFORMATION EXCHANGE ACROSS DOMAIN BOUNDARIES

No.	Mechanism	Description
1	Authentication	Authentication of subjects for access control purposes
2	Access control	Authorized access to the information and resources (conforming to a policy)
3	Release control	Authorized released of information (conforming to a policy)
4	Security assertions for integrity	Applying additional (meta) information to demonstrate integrity of information in a form of e.g. digital signature or label.
5	Data encryption	Prevent access to information for anyone except by entities in possession of special knowledge (decryption key).
6	Hash function	Integrity demonstration.
7	Confidentiality labeling	Providing information on data classification level(s), classification marking rules and classification parameters.
8	Agreement	Establishing formal relation according to policy requirements between two or more entities.
9	Policy enforcement	Ensure that all decisions concerning secure information exchange are conforming to policy requirements.
10	Policy translation	Interpretation of different policies and establishing mutual understanding of their consequences.
11	Referencing and binding	Describe implicit or explicit relationship between resources or portions of resources.
12	Trusted binding	Support trustworthy relationships between resources or portions of resources
13	Source and destination filtering	Control of information flows based on authorized source and/or destination entities.
14	Content filtering	Excluding specific information elements form information flow based on policy requirements.
15	Segmentation	Partitioning of domains and/or entities in order contain risks of security breaches.
16	Validation	Determining or demonstrating integrity according to a predetermined set of requirements.
17	Time stamping	Process of securely applying or delivering trusted time meta data through the lifecycle of information.
18	Validity period marking	Process of securely keeping track of validity events and defining future validity in the lifecycle of information.
19	Sticky policies	Ensuring that policies are bounded to information during secure exchange.
20	Audit trails and change logs	Chronological sequence based on audit records and other relevant information.

V. FRAMEWORK COMPOSITION

Once security requirements are collected and security mechanisms selected the framework for secure information exchange in multi domain environment can be composed. This part of the process includes several steps, whose result should deliver conceptual model for deployment of proper organizational and technical infrastructure. Bellow is an example of how to define relations between security requirements and security mechanisms.

Step 1 requires determining what domains will be crossed (see chapter II). In this example we foresee a scenario crossing where security and organization domains are crossed: A NATO nation needs to send a part of a national confidential document to NATO. The document has to be filtered for non releasable information, reclassified for NATO confidential.

The next step involves selection of security requirements applicable to the foreseen scenario. In the case of NATO confidential information exchange, the requirements are R1, R2, R4, R6, R7, R8, R9, R10, R11, R13, R14.

In order to show the relation between listed security requirements and the list of security mechanisms we use the following approach: first we select a security requirement and match this to appropriate security mechanisms. Subsequently we add a requirement and matching mechanisms. Then we check if there are any conflicts in the mapping of the mechanisms to the requirements. Implementation layer of security mechanisms is finally added. Table 3 presents the output of the process.

TABLE III. AN EXAMPLE OF RELATION BETWEEN SECURITY REQUIRMENTS AND SECURITY MECHANISMS IN SCENARIOS OF CONFIDENTIAL DATA EXCHENAGE WITHIN COALITON PARTNER AND COALITION.

Mechanism	Requirement	Applicable layer		
		Information	Application	Network
M1	R1, R8, R13		●	
M2	R1, R8, R13		●	●
M3	R1, R8, R13		●	●
M4	R4, R6, R7, R14	●	●	
M5	R1, R8		●	●
M7	R1	●	●	
M8	R6, R8, R9	●		
M9	R8	●	●	
M10	R8, R9, R10		●	●
M11	R1, R8, R10	●	●	
M12	R1, R8, R10	●	●	
M13	R1, R7, R8, R10, R13			●
M14	R1, R7, R8, R10, R13	●	●	
M16	R4, R14	●	●	
M20	R2, R1	●	●	●

Figure 5. An example of relation between security requirments and security mechanisms in scenarios of confidential data exchenage within coaliton partner and coalition.

The example above presents how security mechanisms can be selected and integrated in the infrastructure. The result of the exercise does not deliver a final architectural model. This is to be done in the final step, which is however not relevant for framework development.

When composing a framework, it is important to perform steps of consistency. It might happen that selected security mechanisms collide or that a combination of security mechanisms is affecting the process in a way it is non-executable or that security implications have been tampered. Systematic approach to address these issues is still to be developed.

It is important to understand that security mechanisms are not to be confused with security services or solutions implementation. Utilization of security mechanisms may happen in various combinations, where some instances can cover a significant part of the listed security mechanisms. Therefore, the methodology presented, takes into account only logical components of the final architecture. Further development should therefore among others be focus on interpreting the results and their translation to security implementations.

VI. CONCLUSIONS

The work presented does not only illustrate how to address secure data exchange in interconnected infrastructures but how to understand implications of data being exchanged across different domains. Connecting secure networks has a long history and has been around since the introduction of open systems. However, local networked environments have long ago become part of global infrastructures and the last barriers for unconnected high risk networked environments are coming down. This is aligned with the key strategy of coalition partners to utilize a single network supporting order and decision processes.

Through the research work performed on security in interconnected networks it has been proved that a single security architecture is not feasible since an appropriate architecture depends on the (security) context (scenario) to which it needs to be applied. Rather it is essential to identify security context for scenario or a collection of scenarios. This can be very demanding process and proposed example, which illustrates approach taken, only shows that a significant amount of resources are required to identify proper architectural concept for a specific scenario.

Further work lies ahead, mostly focused on development of methodologies, which will ease security context definition, security requirements and security mechanisms mapping. Another research topic should focus on security profiles, which address common scenarios, and security contexts. Profiles may also deliver predefined architecture compositions for secure data exchange based on a specific context. Similar work has already been done for the security patterns through European Commission funded 6th Framework programme integrated project SERENITY [26]. The project was focused on developing methodologies and languages for capturing security and dependability knowledge in heterogeneous and pervasive environments. The result of 3 years research was a platform for collecting security requirements and library of patterns [23, 24]. Patterns are layered through business and organization levels, workflows and processes level, devices and networks level. Specific language was developed in order to interpret patterns, which provide security properties (e.g. information confidentiality), context in which a pattern is to be used (e.g. communication over IP protocol) and one or more implementations (e.g. data encryption using IPSec).

Another important research topic is security mechanisms utilization and standardization of security solutions orchestration. In scenarios of dynamic services and concepts such as cloud computing, security requirements and supportive security mechanisms must be selected and composed in consistent services solution on the fly. This is why it is of utmost importance for future research in this field to address above issues and propose standardized methodologies for setting up frameworks for secure information exchange in interconnected environments.

REFERENCES

[1] B.J. te Paske, D. Boonstra, D.H. Hut, and H.A. Schotanus, "Cross-Domain Solutions, A conceptual model", Whitepaper, TNO, 2009.

[2] P. Hoffman, "Enhanced Security Services for S/MIME", RFC 2634, IETF, June 1999.

[3] National Institute of Standards and Technology, "Standard Security Label for Information Transfer", FIPS 188, NIST, 1994.

[4] ISO/IEC, “Information technology Portable Operating System Interface (POSIX)”, ISO/IEC 9945 and IEEE 1003-1, ISO/IEEE, 2003

[5] ISO, "Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview", ISO 10181-1, ISO, 1996.

[6] ISO, "Information Technology – Open Systems Interconnection – Security Frameworks for Open Systems: Access Control Framework", ISO 10181-3, ISO, 1996.

[7] National Security Agency, "Common Criteria Labeled Security Protection Profile", NSA, 1999.

[8] ISO/ITU, "Information Technology – Security Techniques – Security Information Objects for Access Control", ISO/IEC 15816, ITU-T X.841, ISO/ITU, 2002.

[9] W. Nicolls, "Implementing Company Classification Policy with the S/MIME Security Label", RFC 3114, May 2002.

[10] A. Thümmel and K. Eckstein, "Design and Implementation of a File Transfer and Web Services Guard Employing Crypto-graphically Secured XML Security Labels", Proceedings of the 7th IEEE Workshop on Information Assurance, U.S. Military Academy, West Point, NY, pp. 26 – 33, IEEE, 2006.

[11] OASIS, "eXtensible Access Control Markup Language v2.0", XACML, 2005.

[12] NATO, "Information Exchange Gateways Reference Architecture" March 2009

[13] NATO, "Core Enterprise Services Framework V1.2", January 2009.

[14] http://www.xmlspif.org/, "Open XML SPIF - XML Schema for Security Policy Information File". Last access November 2010.

[15] http://www.isode.com/whitepapers/isode-security-infrastructure.html, "Isode Security Policy, Security Label and Security Clearance Infrastructure", August 2008. Last access November 2010.

[16] D. Eastlake, J. Reagle, and D. Solo, "XML-Signature Syntax and Processing", RFC 3275, IETF, 2002.

[17] T. Imamura, B. Dillaway, and E. Simon, "XML Encryption Syntax and Processing", XMLEnc, W3C, 2002.

[18] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol", RFC 5246, IETF, 2008

[19] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, IETF, 1998

[20] M. Wahl, T. Howes, and S. Kille, "Lightweight Directory Access Protocol", RFC 2251, 1997

[21] R. Housley, W. Ford, W. Polk, and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, IETF, 1999

[22] J. Porekar, K. Dolinar, and A. Jerman Blažič, "Design Patterns for a Systemic Privacy Protection", Journal On Advances in Security, vol 2, no 2&3, pp. 267 – 287, IAIRA, September 2009.

[23] J. Porekar, A. Jerman Blažič, and T. Klobučar, "Towards Organizational Privacy Patterns", Proceedings of The Second International Conference on the Digital Society, pp. 15 – 19, IEEE, February 2008

[24] European Comission FP6 Intergated Project SERENITY, http://www.serenity-project.org/, accessed october 2010.