Trust architecture applied in document management

Laura Danilescu [1]

Abstract: Document management involves, in addition to classification and archiving, application of additional elements to ensure confidentiality of the information contained therein. These additions are trust policies. For these policies, we define categories of documents and categories of users, actions and rules of which interaction results trust architecture.

Keywords: Document management, trust policies, information

1. Introduction

Document management systems allows employees to access necessary information - rights-based authorization - clarifies relations between documents (eg through systematic records of contracts and invoices, e-mail registration, etc.) and facilitates rapid and efficient communication between colleagues in different departments (eg finance, HR, administrative, etc.) and subsidiaries, contributing to a more transparent workflow.

2. The document built on the concept of "privacy and trust"

This concept arose because of observations on the need for information both intra and inter-organization, namely access to various documents for all their members.
Thus, in the EPAL policy, the person who needed to be informed, made a query over access rights to documents and EPAL policy answer "allow" or "deny".
XACML, like EPAL, allow or disallow access to a document.
From the first observation one can see that how to access a document is quite simple ('allow' or 'deny'), which can lead to a lack of information for users wishing to access a document, but the fact that the document contains information prohibited for this, it can not access any information that is entitled to access. But inside documents there are both public information and data and information that are subject to various degrees of confidence based on the trust that enjoys the person having access to them.
Also, to access data and information through the two previous methods, the user must be connected to the corporate network and can see them only on-line, while the new solution proposed here allows the document can be consulted both on-line and off-line.
Suppose that in the organization is made a report to be circulated to all staff, shareholders and business partners.
Each of these categories and category members are in different relationships of "trusting" with the organization. Therefore, each person has access to the public

[1] Lecturer, PhD. Danubius University of Galati, Address: Galati, Romania, telephone no +40.372.361.102, fax no +40.372.361.290, corresponding author: ldanilescu@univ-danubius.ro

part of the document and also each of them has access to certain confidential information under the policy of "trusting" of the organization.
Therefore, if the organization has 1000 employees, 10 shareholders and 25 partners, should be made a minimum of 1035 different documents to enable everyone to have access to both document and data customized according to the "trusting" policy.
The new document creation system allows to create a single document, which is processed by each employee, according to the "trusting" policy, and to reveal him only the information that has the access right.
Thus, each department will create his part of the document which will be part of the whole. Then, it apply the "trusting" policy on his part of the document and submit the document with the "trusting" policy applied, which will make that confidential data can not be seen by those who are not eligible. Then the document will be assembled and distributed. Each of the receivers of the document will use the keys that allow you to open various parts of the document. Thus, each read only what is allowed to read in the document. Therefore, it creates a single document that will meet the organization's privacy policy.
As described above, data and information are found in documents. Documents can be simple if there have only one author (single document), or complex (multiple document) where parts of the document have different authors. Document may contain data or information needed for information/decision-making process that occurs throughout the entire life of the organization. Further, we agree to name the data or information "document elements" short "elements". These "elements" can be grouped into "categories of elements" according to their place of origin and the group of subjects acting on them. Elements together form "object" of the subjects activities, which we can denote simple objects (those containing only one object) or complex objects (consisting of several objects), by number of authors and component objects.
Example:

- The category of "financial accounting elements" - which can translate into objects like
    - financial report;
    - payroll;
    - etc.
- The category of "commercial items" that may be part of such objects as:
    - situation of procurement contracts;
    - situation of supply contracts;
    - situation of cooperation;
    - etc.

In the picture below, we present a complex object model required by the leadership of a hypothetical organization, which must contain information held by the commercial and economic.

Action object (document) consists of the following elements

:

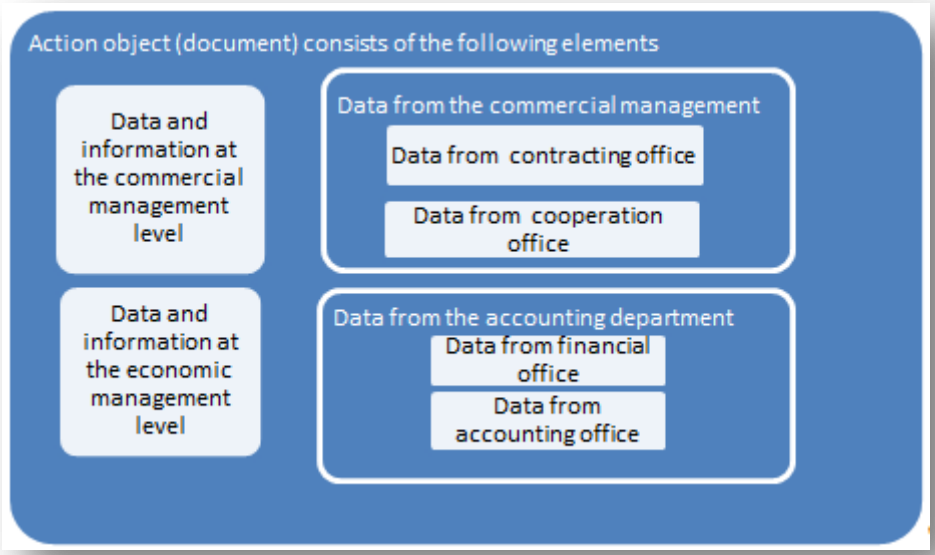

Figure 1. The components of a document

The document will contain the elements (data and information):

Given by	Completed by
Contracting office	Commercial department
Cooperation office	
Financial office	Economic department
Accounting office	

The analysis of the above elements can draw the following conclusions:

- The object (file data) was initiated at the execution level on each branch of activity (at the office, or department level)
- Verification and data completion was made at the next level of competence.
- At the same level was the assembly of two component objects.

- Elements (dates) that were supplemented were not notified to the lower level, which means that it doesn't have the adequate trust level in accessing these items.

Analyzing how to create a document, results that each object that can be created independently or part of a complex object has:

- Author (Author) - who initiates the document;
- Co-author/contributor) – who complete the document;
- Commentator (Annotator) - who comment on the data file;
- Supervisor - who approve the document and may be subject recipient of the object;
- Reader - who read the document and may or may not object.

If we intend to present a document life cycle, results the following scheme:

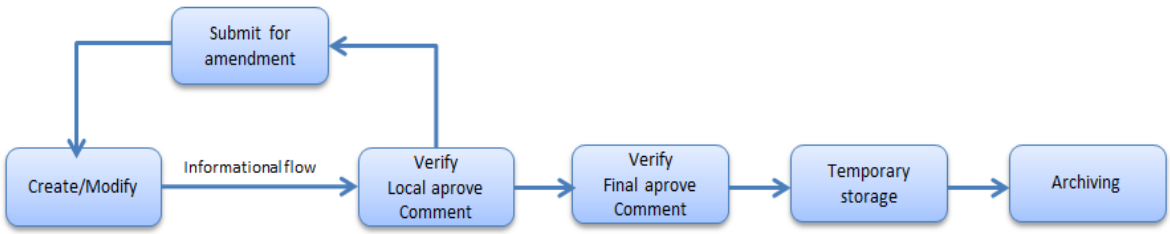

Figure 2. Document life cycle

In addition to the above actions, the elements of an object can support the following processes from the subjects:

- Quoting/citation;
- Printing
- Copying

A document pass through the following milestones during its existence:

- Stage of creation;
- The consultation period;
- Stage of storage (archiving).

The creation stage of a document is the stage in which subjects are authors, co-authors, commentators and supervisors of the document.
The consultation phase is the one in which a subject read, comment, cites a document.

The achieving stage is the stage when the document is stored in a special location or is printed on paper and can be consulted for specific purposes by certain subjects.
During the creation, validation, archiving documents, namely, any of the times specified in the "document life cycle", this, at a time can have a single state well established and can run on it a single action that will change the status again. From here stems the need to associate a **state vector** of the document that will indicate, at any time, in what stage of its evolution is the document. Also the state vector indicates the path traveled by the document from creation to archiving or destruction.
If the document is fragmented into elements that have different paths, then each vector is associated to each element and the joining vector leads to the **document state matrix**.
Below is shown the document circuit, on which applies the trusting policy

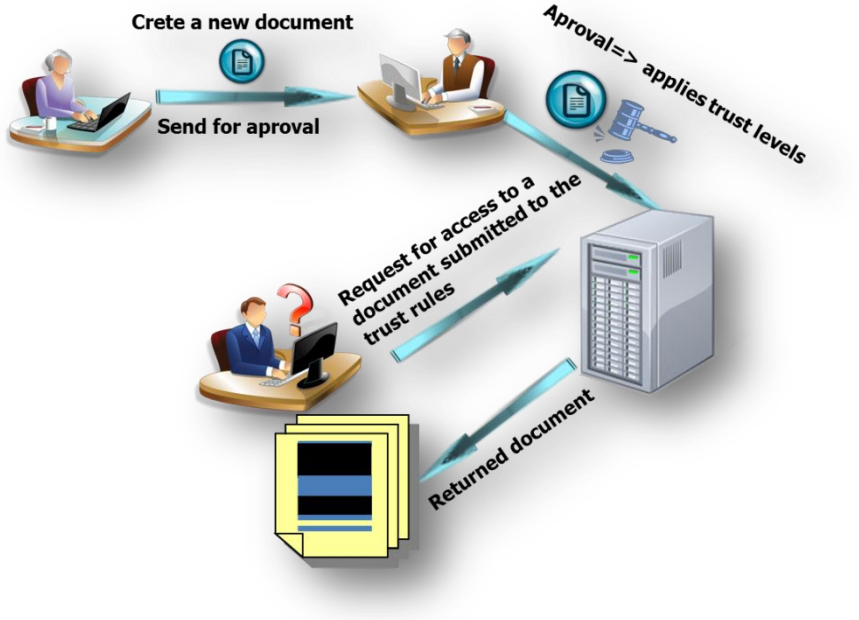

Figure 3. Document circuit from creation to final stage

3. Implement trust policies on documents

Trusting manager or his delegated person has access to the categorization of objects and objects which are subject to the trusting policy, but can not access the content unless specially authorized to have access to them.
The figure below illustrates the role of the management team in allocation of trusting levels for both users and objects.

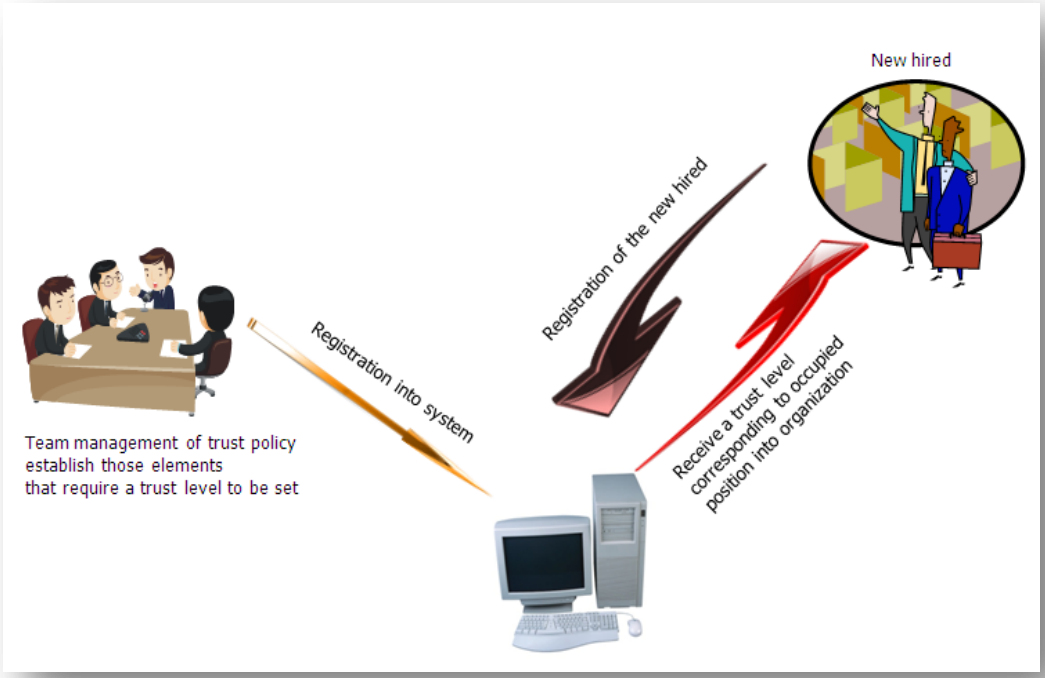

Figure 4. Allocation of trusting levels

Trusting actions must comply with policy decisions and applicable trusting policy:

- Read,
- Quoting,
- Comment,
- Printing,
- Amendment, Supplement,
- Establish
- Approval

For verification of application actions, policy validator will check their compliance with any change in status to a category of objects, object or subject.
Any subject in the TAP can not change policy without the consent of trusting person board. Policy change may be made only on request when the situation demands.
Any formal or informal group which is involved in the process of creating and operating trusted documents will be responsible for approving a temporary member of the group activity and will be marked as head of the group.
Trusting policy change may be permanent or temporary and will be logged.

4. Conclusions

Reporting needs of the organization are different, which leads to the need for the creation of information policy. Reporting needs requires also information protection to prevent the sensitive data disclosure at levels of competence that are unable to process and store such data. Therefore, is very important the privacy policy which complements the security policy for information circulated inside the organization.

Regarding data access control, it cannot be a simplistic approach to the type of access rights such as *allowed/deny*, or in other words, *trust/distrust*. Therefore, research topic, by refining the approach to define hierarchies on access rights based on trust brings a new model for security of information conveyed by the organization, substantially improving reporting needs of all levels.

7. References

P.Gloor. Making the e-Business Transformation. London : Springer-Verlag, 2000.

Albrechtsen, E. A qualitative study of user's view on information security. s.l. : Computers & Security 26 (2007), 276–289.

S. Furnell, A. Jusoh, and D. Katsabas. The challenges of understanding and using security: A survey of end-users. s.l. : Computers & Security 25 (2006).

17799, SR ISO/CEI. Information Technology. Code of Practice fior Information Security Management. 2004.

Danilescu Laura, Danilescu Marcel. Organization's Data Access Control Policies Based On Trust. Galati : EuroEconomica, CNCSIS B+, Issue 2(25)/2010 ISSN 1582-8859, pag.113-122, 2010.

Matt Blaze, John Ioannidis, Angelos Keromytis. Trust Management. s.l. : Springer Berlin / Heidelberg, 2003. Url: http://dx.doi.org/10.1007/3-540-44875-6_21.

Danilescu Marcel, Danilescu Laura. Control Access To Information By Applying Trust Policies. Bucuresti : Conferința Internațională "Educație și creativitate pentru o soceitate bazată pe cunoaștere" ediția a IV-a 2010, Universitatea "Titu Maiorescu", 2010.

O. Adam, A. Hofer, S. Zang, C. Hammer, M. Jerrentrup,S. Leinenbach. A collaboration framework for cross-enterprise business process management. s.l. : Preproceedings of the First International Conference on Interoperability of Enterprise Software and Application (Geneva, Switzerland), 23–25 February.

Stankard, B. Gehling and D. eCommerce security. s.l. : InfoSecCD '09: Proceedings of the 2nd annual conference on Information security curriculum development (New York, NY, USA), ACM Press, September 2009.

G. Chakrabarti, A. Manimaran. Internet infrastructure security: A taxonomy,Network. s.l. : IEEE 16 (2002), no. 6, 13–21.

S. Katsikas, J. Lopez, and G. Pernul. Trust, privacy and security in e-business: Requirements and solutions. s.l. : Lecture Notes in Computer Science 3746 (2005).

Danilescu L., Danilescu M., "Control Access To Information By Applying Policies Based On Trust Hierarchies", 2010 International Conference on Computer and Software Modeling, ICCSM 2010 – Manila, Philippines,