# E-Business Data Access Authorizing Architecture By Applying Trusting Policies

Laura Danilescu

*Lecturer drd., Danubius" Univeristy Galați, Faculty of Economic Sciences,*

*ldanilescu@univ-danubius.ro*

**Abstract:** *A large number of organizations have implemented security or privacy policies through classified documents. However, this does not resolve a unitary information within the organization and does not complete disclosure of confidential data, according to the hierarchical level that a person occupies. For this reason, have been defined policies to control access to information based on hierarchies and relations of trust. Policy generation is performed using algorithms and their enforcement through an XML-based language.*

**Keywords:** policies, trust, hierarchies , algorithm, tuples, TAP architecture

## Introduction

One feature of modern organizations, and especially of an e-business organization (1) is the distribution of resources. With the transition of business from the traditional model to the electronic one, the number of users involved in business operations has increased, and these users (both inside and outside the organization) need access to the information of the organization. This information produced and circulated by the organization, whether as documents, or reports presented in various formats (text, spreadsheet, database), has a specific target group; in other words, "not all information is visible to everyone". Hence arises the necessity for designing a security system (2) that can provide the desired level of transparency or opacity of the documents that are the object of reports or information exchanged between business partners.

## Security policies

The need to define security policies (3) arose when information was grouped into two broad categories:

- classified information, which in turn may be confidential, secret and top secret
- public information

In addition, there is code words based system through which information of any type may be subject to other restrictions, called *compartmental classification* (the American version) or multilateral security (the European version). For this purpose use:

- descriptors
- warning words
- international defence markers

All these aspects are scientifically treated through security policies models, grouped *in multilevel and multilateral security models.*

**Security policy** (4) consists of a set of measures, supported by management, which provides clear rules, but flexible to determine the operations and technologies required to ensure security.

A security policy is a document that highlights the main requirements or rules to be known and applied for security insurance.

*Security models are important in determining the company's security policy in the computer system. Study of the abstract models of security can be determined in understanding of the security mechanisms to be applied.*

The **security model** is a mechanism that implements an established security policy.

When we refer to an organization's information security, a policy can be represented by several elements:

- Firewalls used to control access
- Routes that circulate information
- Access cards, cameras that record everything controlled perimeters
- Many other items

## **Trust authorization policy (TAP)** (5)

We call **trust policy** set of tuples of the form ($a_i$, $u_i$, $e_m$, $r_n$,), defined like: $\mathbf{a_j}$ is the action permitted to be executed by the user $\mathbf{u_i}$ on the element $\mathbf{e_m}$ based on trust relation $\mathbf{r_n}$ and where:

- $\mathbf{u_i \in\ G_i \subseteq Du}$ is a hierarchy of users which forms a group $G_i$ which belongs to the users domain $D_u$. Table 1 presents, custom hierarchy within an organization

| **Position in the** | **Coding** |
|---|---|
| User | $u_1$ |
| Data operator | $u_2$ |
| Head department | $u_3$ |
| Head project | $u_4$ |
| Director | $u_5$ |
| Project Manager | $u_6$ |

*Table 1 – users hierarchy within organization*

- $\mathbf{e_m \in\ C_i \subseteq De}$ is a hierarchy of elements which forms a category $C_i$ which belongs to the elements domain $D_e$;
- $\mathbf{r_n \in R}$ is a trust relations (6) hierarchy;

Those relations we assign the following numerical values:

| **Trust** | **Trust value** |
|---|---|
| $r_1$ | 0,5 |
| $r_2$ | 0,6 |
| $r_3$ | 0,7 |
| $r_4$ | 0,8 |
| $r_5$ | 0,9 |

| | |
|---|---|
| $r_6$ | 1 |

*Table 2 – Numerical values assigned to trust relations*

- $\mathbf{a_j \in A}$ where A is a hierarchy[4] of actions corresponding to relationship hierarchy R, and a relation **r** corresponds to at least one action **a**, where $a_1 < a_2 < a_3 < a_4 < a_5 < a_6$:

  - $a_1$ = elements reading
  - $a_2$ = create new document
  - $a_3$ = modify document
  - $a_4$ = register document
  - $a_5$ = archive
  - $a_6$ = approval

The fact that any $a_j$ corresponds to a $r_{n,\ \text{can}}$ lead to a simplified definition of policy, as ($a_j$, $u_i$, $e_m$), or to a detailed definition, as ($r_n$, $u_i$, $e_m$).

**Restrictions**: We call restriction, limiting a user action on an item or category of items, although he had the trust level necessary to accomplish the action.

There are situations where a user's position within the organization makes it possible action on the items by changing their status, which could lead to their alteration or destruction. To prevent such situations, measures can be taken to restrict user actions.

To designate a restriction on an activity, we note with “$-a_j$” a detailed restriction and with “$-r_n$” all the restrictive politics. Thus, we have a set of elements ($-a_j$, $u_i$, $e_m$) sau ($-r_n$, $u_i$, $e_m$).

## TAP Arhitecture

In figure 1 are presented TAP (7) components and interactions between them.

The core of this architecture is PDP - Policy Decision Point. It receives a request, assumes the applicable policy from the **PAP** (Policy Administration Point), evaluates actions from the point of application of policies, evaluates the request and returns an authorization decision to **PEP**.

**PEP** is the Policy Enforcement Point. It receives an access request, extracts actions, generates a TAP request and sends it to PDP for evaluation.

**PAP -** Policy Administration Point, creates a TAP policy and stores it in a policy database server.

**PIP -** Policy Information Point is a component that acts as a server that stores the state matrixes of elements and actions can be performed on them and make them available to the PDP.

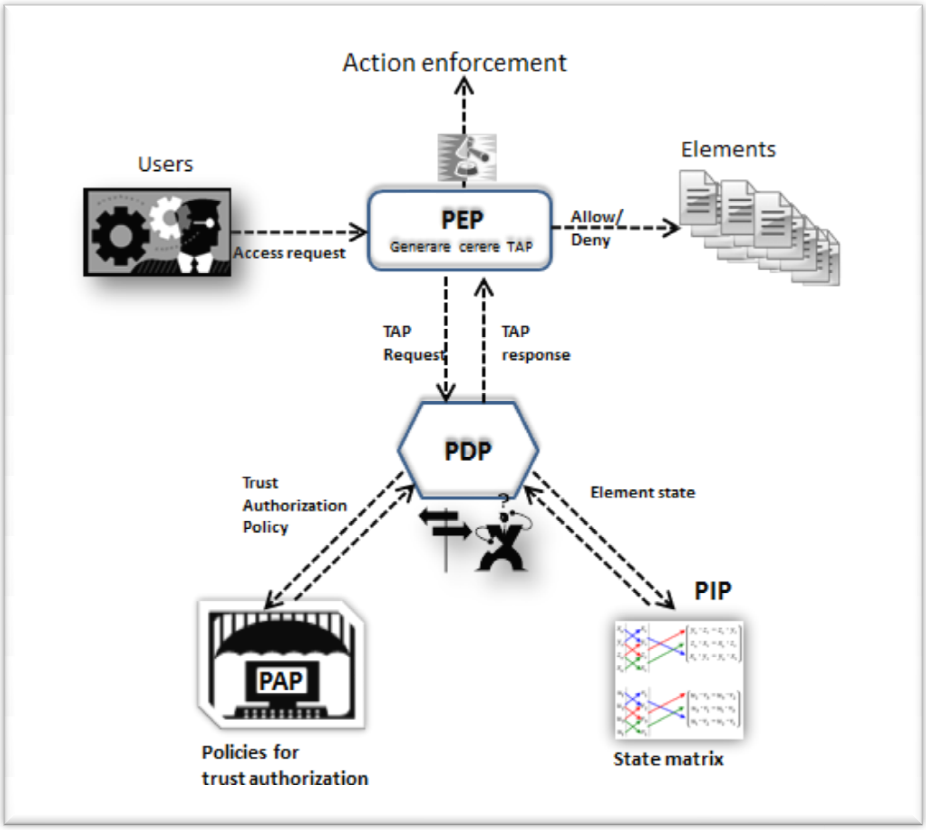

*Figure 1 TAP Arhitecture*

## Conclusions

Regarding data access control (8), it can not 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 (9) based on trust brings a new model for security of information conveyed by the organization, substantially improving reporting needs of all levels.

## Future research

The directions for further development we identified, are:

- improving the developed theory and adding new elements to the trust-based policies;
- the utilisation of the policies generated by TAP as a research base for the management of documents by the "state vector " and "path matrix" of a document;

References

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

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

3. **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).

4. **17799, SR ISO/CEI.** *Information Technology. Code of Practice fior Information Security Management.* 2004.

5. **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.

6. **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.

7. **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.

8. **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.

9. **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.

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

11. **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).