# Organizational aspect of trusted legally valid long-term electronic archive solution

HELENA HALAS, JAN POREKAR, TOMAŽ KLOBUČAR, ALEKSEJ JERMAN BLAŽIČ
Security Technology Competence Centre (SETCCE)
Tehnološki park 21, SI-1000 Ljubljana
SLOVENIA
helena.halas@setcce.si, jan.porekar@setcce.si, tomaz.klobucar@setcce.si, aljosa@setcce.si

*Abstract:* - Due to increase of electronic business and business process dematerialization organizations are facing today a problem of preserving vast amounts of electronic documents in coherent and trustworthy manner. A large amount of digital documents are produced every day even in small and medium-sized companies. The documents range from simple receipts to complex legal contracts and service level agreements. Many such documents need to be stored and preserved for longer period of time. Some services and technical solutions providing long term proofs of authenticity, integrity and non-repudiation of electronic documents are available on the market today. In order for these technical electronic archiving solutions and services to be successfully adopted by organizations they need to be deployed in a proper operational and organizational manner. Beside this organization needs to establish required operational procedures and to operate in accordance with them to assure that trusted electronic archive is legally valid. In this paper we present the first set of organizational approaches that organizations need to utilize in order to successfully integrate the operational and legal aspects of electronic archiving and to change the business processes accordingly. Following the approach of pattern oriented organizational design we capture the organizational trusted archiving solutions and best practices in the form of patterns, providing the context of the problem, the generic solution captured in the form of organizational diagrams, and preconditions that need to be met by the organization, and dependencies on other patterns are described. Finally the paper presents implementation of the generic solution to different organizations' contexts and indicates influence of different applications of the pattern to further solution development.

*Key-Words:* - electronic archive, long-term preservation, security, legal compliance, durable integrity, durable authenticity, organizational patterns

## 1 Introduction

Electronic commerce is in full swing today and loads of electronic documents are produced on a daily basis. Following the trend of business dematerialization the documents often exist in an electronic form. Electronic documents, such as invoices, legal contracts, medical records service level agreements, can be of highly sensitive origin. Due to legal requirements such documents often need to be preserved for longer periods of time (usually 10, 20 years or even more). Although the field of electronic archiving has been subject to extensive research in the past years, it is still not easily accessible to small and medium-sized companies. Organizations still have to tackle many problems, and they often store documents in an inappropriate way. Several standards and research papers written on this subject already exist ([6], [7], [8], [9], [10], [14], [21],[23]). They intend to serve as guidance for organizations when establishing solutions for electronic archiving. Also some more specific research papers on electronic archiving can be found ([15]).

Many technical solutions are readily available, but the real problem for organizations is hidden behind the organization aspects of those solutions. It is not enough just to implement a technical solution, the organization also needs to establish the required organisational procedures and to operate in accordance with them, which may sometimes require even subtle changes to the key processes of organizations. In many cases more stakeholders coordinate and interact with each other to achieve a common goal.

In this paper we present the integration of organizational aspect of electronic archiving solution from the point of view of security and legislation. Using the pattern approach to capture good practices the medium-sized and small-sized organizations are presented by alternative approaches to handle organizational aspects of electronic archiving. We present the whole umbrella

of electronic archiving with special focus on provision of authenticity and integrity proofs.

# 2 Long-term trusted electronic archiving

Electronic archiving in general refers to preservation of electronic records which originate in electronic form or are properly digitalized from paper form. While classic archiving is one time action, electronic archiving represents continuous process and is tightly connected with the whole document lifecycle from creation of the document to the archiving if the document or document destruction. The whole process of archivng either finishes with document destruction or it may continue perpetuately (100 years or more) if required by the laws, directives or internal organizational rules. As an electronic document can be easily manipulated by any party involved in the process of archiving, it is important to provide its integrity and authenticity through the whole archiving period.

The process of electronic archiving can be generally divided into the following steps:

- Selection, capturing and digitalization of the document
- Electronic storage, preservation of integrity and access to the stored material
- Providing proofs of authenticity and integrity for stored materials

Electronic archiving has many positive influences on organizations, for example optimisation of business processes, effective arrangement of business, better availability of information, easier and more efficient access control policies implementations, higher security levels of stored documents and business information, lower document archiving costs, and savings bounded by operational costs of paper archives. The influences vary between organizations, and they depend on the size of an organisation, nature of its business, documents quantity and format, existence of electronic commerce, and archiving needs. Every organization needs to value justification and feasibility of electronic archiving introduction for itself and also to calculate which type of preservation approach and archiving solution would be most appropriate for it.

In order for an organization to successfully migrate to electronic archiving the adoption of technical solutions is necessary. Aside to that organizational changes are required, such as establishing new operational procedures, defining new roles and assigning new responsibilities to employees and the rearrangement of accompanying documentation. In case of outsourcing of certain aspects of archiving the settlement of relations between all involved parties in form of contracts are required as well.

For all types of organizations that adopt electronic archiving practices it is of vast importance to assure proofs of legal validity of the stored documents that can be used as evidence material in court.

## 2.1 Requirements for electronic archive

Storage of documents in electronic format (electronic archiving) is one of the integral building blocks for doing business electronically. Secure electronic archive (EA) must provide equivalent legal value of electronic and paper forms of documents. Legislation specifically mandates that certain documents need to be stored for a longer periods of time (e.g. 10, 20, 50 years or more). Therefore we focus on secure long-term electronic archive (LTEA), which must ensure integrity of stored documents, proofs of authenticity of document source and proofs of authenticity of time origin of the documents over long periods of time.

Systems for secure long-term electronic archiving are advanced combination of different technological solutions that suit functional, formal and legal requirements for archiving. To provide secure EA it is necessary to assure appropriate solution on various levels: networking, infrastructure, preservation software solution, properly regulated organization, and regular execution of procedures. Beside appropriate organizational and technological solution, EA needs to be compliant with legislation and other regulations.

### 2.1.1 Why to use electronic archives?

We have already identified some advantages of EA and pointed out why organizations should decide to use electronic storage of documents. With years traditional archives are becoming bigger and bigger and more difficult to handle. Increase of the archive storage space and time to find particular stored document proportionally rise expenses of preservation**.**

With new technologies electronic business, where documents exist only in electronic form, come into use more and more frequently. After being printed these documents can lose their real value (for instance if they are digitally signed). So, in such situations organizations are forced to find other solutions for archiving, which provide

equivalent legal value of electronic and paper form of documents.

#### 2.1.2 How to choose an appropriate solution?

Organizations have different options for establishing secure long-term storage of electronic documents. One possibility is to invest in its own EA solution, which may have a significant impact on infrastructure costs and return of investment. Organizations like financial institutions, insurance companies and governmental institutions should consider such an option as well as other large scale organizations in which easy access to documents and validity of these documents are strongly coupled to organization's key business processes. The opposite approach is to outsource the entire service, which may be the most appropriate solution for the middle and small-sized companies in terms of cost savings and optimization of operation. As this approach is usually characterized by low start-up investment ratio and time saving approach it may be suitable for large scale organizations too, especially when electronic archiving does not affect the key business processes of the company. Furthermore the entire service of electronic preservation can be separated into partial services, which are in domain of one or more providers or are implemented by the user itself. Examples of partial services are repository or document management service, integrity and authenticity demonstration service, etc.

Outsourcing of the service (apartial or entire) seems to be the most probable solution for majority of organizations also because of the required expertise and complex and expensive infrastructure. Costs of outsourcing and usage of EA are usually lower than costs of acquiring, implementing and maintaining in-house solution. Because of professional expertise and experience in the field external providers are able to provide superiorly secure and reliable services. They also better follow technological changes and in accordance with them they adapt or modernize a solution if necessary. No additional employment and almost no training of human resources are needed.

### 2.2 Legislation

Legal value of electronic documents can be made equivalent to paper documents only when secure LTEA is in compliance with legislation. Legislation defines conditions that hardware and software solutions for electronic archiving must meet, the conditions and procedures of transforming paper documents into electronic form, and organization, infrastructure and realization of archiving documents in paper and electronic form, including legal consequences of such an archiving. Local regulations differ between countries, and we can not expect that there would be uniform rules in the future for the whole world.

In European Union there are some efforts to unify member states' requirements for secure legally valid EA. In 2001 Model Requirements for the management of electronic records (MoReq) was created ([9]). It defines generic requirements for an electronic records management system. In contrast to most other recommendations and standards it is formed for international use and convenient to any sort of organization (public and private sector). Although it was intended for use throughout the Europe in practice it can be applied in many countries over the world. Recently improved version MoReq2 was published ([10]). Efforts are now directed to recognition of MoReq as international standard, on which basis it would be possible to acquire certificate, which would confirm adequacy of EA solution in the whole EU and maybe also wider.

Another possibility is that a solution for electronic archiving takes into account different legal requirements of specific countries. If an organization using EA solution is involved in a business relationship with an organization from another country, the solution used needs to consider legal requirements of both countries. Other recommendations and standards must be captured in the provided solution aside to provision of general legal requirements.

## 3 Solutions for organizational aspects of electronic archiving

In this paper we do not discuss technical issues that concern appropriate technological or communicational infrastructure, software, nor their integration into complete solution, but focus on modelling generic operational organizational structure upon which a dependable EA should operate and capture organizational process needed to make EA legally compliant. Organizational structures are primarily studied by two disciplines: Organization Theory, that describes the internal structure of an organization, and Strategic Alliances, that model the external collaborations of independent organizations who have agreed to pursue a set of shared business goals ([12]).

For providing secure and dependable EA, different roles and responsibilities have to be introduced. Each role can be played by any of the

parties involved in the process. For effective establishing of a solution, relations between roles in the process must be clear. In order to provide proper solution, organizational and technical requirements need to be captured and analysed. Therefore the context of the overall system needs to be captured. Involved parties, their goals, roles and relations between them need to be defined.

To set up legally valid secure EA requirements arising from legislation must be satisfied. Legal aspect therefore deals with question which legal requirements need to be satisfied, how they influence on the solution and how to implement them.

From this perspective at least two different areas of same problem need to be covered. A question arises here on how to deal with a problem to satisfy all requirements from different perspective (organizational, technical and legal requirements) and how to integrate all parts to provide secure and legally compliant EA. Therefore the problem must be first accurately examined so adequate solution can be found and performed.

### 3.1 Modelling organizational security with security Tropos diagrams

Providing security through the whole software development process is one of today's challenges in software and requirements engineering research as it does not require to solve only technical problems but also to consider the organization as a whole. For the purpose of this paper we use Secure Tropos, a formal framework for modelling and analyzing organizational security ([12]). It is appropriate to describe organizational structures composed of both IT systems (hardware and software) and humans (liveware) and is an extension of Tropos, an agent-oriented software development methodology. With Secure Tropos diagrams we model the following organizational primitives (for more see Figure 1):

**Actors:** An actor models an entity that has strategic goals and intentions within the system or the organizational setting. It represents a physical or a software agent as well as a role or position. The role is defined as an abstract characterization of the behaviour of a social actor within some specialized context or domain of endeavour.

**Resources**: a resource represents a physical or an informational entity. The main difference with an agent is that a resource has not intentions.

**Goals:** a goal represents actors' strategic interests. Goals may further be distinguished into hard goals and soft goals, the second having no clear-cut definition and/or criteria for deciding whether they are satisfied or not. Soft goals are typically used to model non-functional requirements.

**Dependencies:** a dependency between two actors indicates that one actor, depends on the other actor to attain a goal or to deliver a resource. The former actor is called the depender, while the latter is called the dependee. The object around which the dependency centres is called dependum. In general, by depending on another actor for a dependum, an actor is able to achieve goals that it would otherwise be unable to achieve on its own, or not as easily, or not as well. At the same time, the depender becomes vulnerable. If the dependee fails to deliver the dependum, the depender would be adversely affected in its ability to achieve its goals.

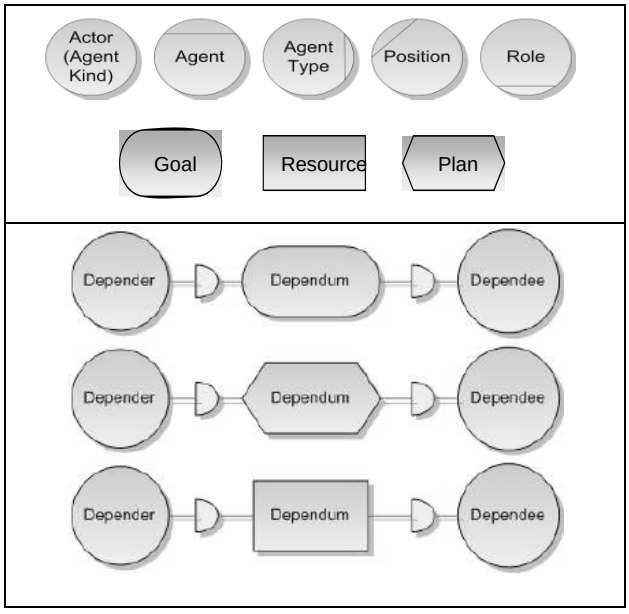


Figure 1: Schemantical description of main secure Tropos concepts and dependencies

Five security specific dependencies have been introduced in Secure Tropos:

**Ownership**: it indicates that the actor is the legitimate owner of a goal or resource. The owner has full authority concerning to achieve his goal or use his resource, and he can also delegate this authority to other actors.

**Provisioning**: it indicates that the actor has the capability to achieve some goal or deliver a resource.

**Request**: it indicates that the actor intends to achieve a goal by executing some tasks, or to require a resource.

**Trust**: it is relationship between two actors, which indicates the belief of one actor that the other will not misuse some goal or some resource. The former actor is called the truster, while the latter is called the trustee. The object around which the

dependency centres is called trustum. In general, by trusting another actor for a trustum, an actor is sure that the trustum is properly used. At the same time, the truster becomes vulnerable. If the trustee misuses the trustum, the truster cannot guarantee to achieve some goal or deliver a resource securely.

**Delegation**, it is relationship between two actors, which indicates that one actor delegates to the other the permission to achieve some goal, execute some plan, or use a resource. The former actor is called the delegator, while the latter is called the delegatee. The object around which the dependency centres is called delegatum. In general, delegation marks a formal passage in the domain that is currently modelled by the requirements engineers. This can be matched by the issuance of a delegation certificate such as digital credential or a letter if we are delegating permission or by a call to an external procedure if the execution is being further delegated.

In this paper we present use of the Secure Tropos framework in the real scenario, as like as Yudistra et al. ([3]) presented their experience in modelling and analyzing requirements for an air traffic management system with focus on modelling and reasoning about trust and risk relations within the organizational structure.

### 3.2 Capturing organizational knowledge in form of patterns

The first ideas of using patterns to capture software development best practices originated over a decade ago by the Gang of Four ([11]). In recent years the idea of patterns has been adapted and successfully applied to the fields of IT security and dependability (S&D) ([1], [22]). At least three different approaches towards S&D patterns have been introduced: The Open Group approach ([5]), the Schumacher et al. approach ([20]) and the Serenity project approach ([2], [18]).

Patterns present generic and proven solutions to problems that can be adopted to specific context. They capture the problem description, the context of the problem and the generic solution as well, and are as such independent of any particular technology. Because patterns are seldom fully independent they may also contain references to other patterns ([17]). More complex solution can also be represented by combining different patterns, what should be used in our case by combining security and legal pattern. With organizational patterns we capture existing organizational knowledge at organizational level: both level of stakeholder relationships and operational organizational level. For the purpose of this paper we present a simplified version of the European Commission 6th framework programme Security Engineering (SERENITY) project approach towards the organizational patterns ([17]). The following dimensions of patterns are important:

- ***Problem Description***: A description of the *broader context* and situations in which the pattern is suitable, describing under what conditions a pattern should be used. Aside to suitability it is important to state the generalized requirements that are solved by applying the pattern in the situation. Generalizations of requirements provided by a pattern applied into a broader context are called *provided properties* and are sometimes also referred to as pattern attributes. A pattern can provide one or more properties to different actors involved. Patterns may provide organizational security properties, better and more dependable operational maintainability, accountability, transparency of business, etc.

- ***Generic Solution***: It is a high level representation of reorganization of resources and cooperation between humans, organization and machines that is needed to solve the requirements to the generic problem. The solutions are described in form of plain text and additionally modelled and presented in the form of Secure Tropos Diagrams and sometimes in the form of different UML diagrams. For the purpose of this paper we use the UML activity diagrams.

- ***Dependence on other patterns:*** Patterns are not isolated blocks and may therefore often depend on other patterns and reuse them for achieving generalized requirements through solutions. The pattern should specify which part of the solution is part of itself and which parts are provided by other patterns that can also be considered as a kind of *solution preconditions.* The scope of dependencies of organizational patterns may often extent to more technical domains. The organizational archiving patterns described in this paper often rely on technical archiving solutions. Although such technical solutions are not subject of this paper they may define the boundaries of the pattern described.

- ***Specific context implementation guidelines***: A pattern description my contain guidelines and examples of application of the pattern to specific situations and contexts. The adaptations that were required to map the generic solution to

a specific context should be described as part of the pattern itself.

## 3.3 Specification of organizational archiving patterns

In this section we describe two patterns:

1. *Pattern 1: "A generic organizational structure for operating a trusted electronic archive"*: this pattern captures (i) the required roles and agents, (ii) their organizational interdependence and (iii) the processes required for operationally functional long term trusted archive. Some examples of application to different business environments are explained.
2. *Pattern 2: "Setting up a legally compliant trusted long-term archive"*: this pattern describes organization that stakeholders are required to adapt to for an archive to be legally compliant.

### 3.3.1 Archiving pattern #1: A generic organizational structure for operating a trusted electronic archive

***Problem definition***

An organization has an existing archiving system in place. Such existing archive can range from a fully implemented document management system (DMS) to a simple network shared folder. The existing archive does not provide trusted integrity and proofs of authenticity, therefore we refer to it as an "untrusted archive". The organization wants to establish (i) perpetual and (ii) maintainable document storage for different types of electronic documents originating from various internal processes. The agents responsible for archiving electronic documents play the role of "electronic archive user" – EAU.

The pattern should provide an organizational structure that will be able to provide the following properties to EAU:

- *Durable proof of authenticity* for the archived documents
- *Durable integrity* of the archived documents (durable storage)
- *Availability* of the archived documents

The agent playing the role of "Electronic Archive provider" – EAP is in charge of organizationally providing the above mentioned properties through an appropriate organizational structure. We further require that organizational structure is designed in such manner that it provides the following properties to the EAP:

- *Operational maintainability* of the trusted archive
- *Accountability* of the trusted archive procedures (also referred to as transparentness of operational procedures)

***Generic solution***

The following organizational roles should be introduced to support organizational solution to support trusted electronic archive:

- Electronic Archive Provider (EAP)
- DMS Provider
- Authenticity and Integrity Provider (AIP)
- Timestamp Authority (TA)

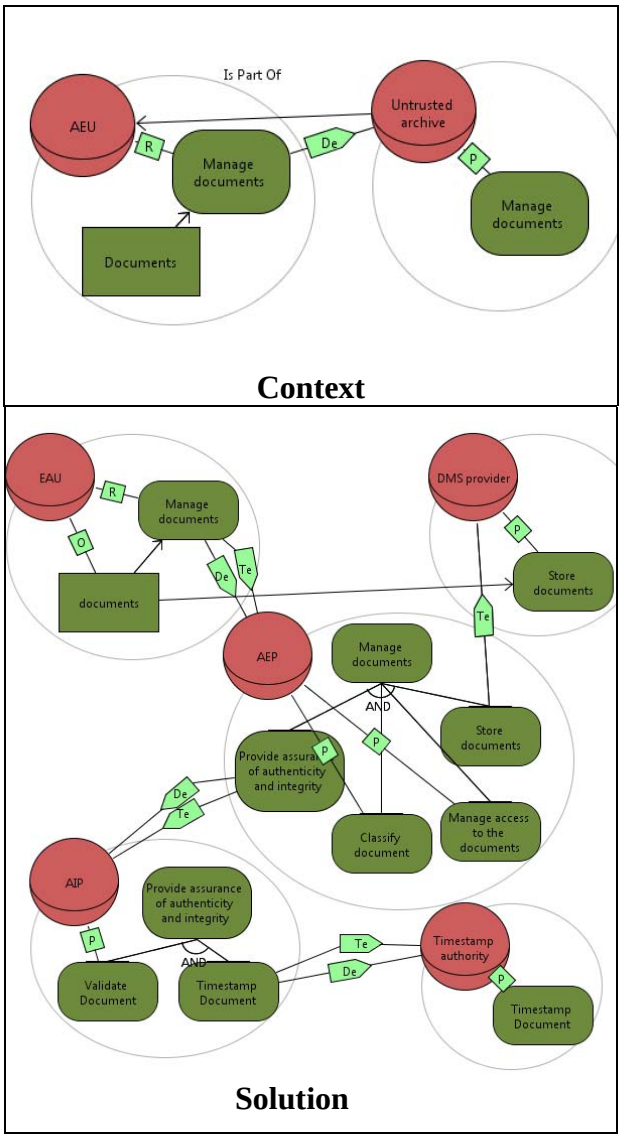


Figure 2: Tropos model for security pattern

An organization that will have agents acting as EAU needs to set up the role of EAP and find an appropriate agent to act on behalf of electronic archive provider. EAP further needs to utilize three roles: (i) the Authenticity and Integrity provider (AIP) that is responsible for delivering durable proofs of authenticity and integrity, (ii) the DMS provider responsible for delivering organization for dependable storage and consequently integrity of the documents on more technical level. The third role is (iii) the Timestamp Authority (TA). Organizational structure and separation and delegation of duties are presented schematically in form of a Tropos diagram on Figure 2.

Below we describe the process of organizational delegation in more detail: EAU requests EAP to provide the service. EAU delegates the execution of the goal to EAP and trusts him that the goal will be properly fulfilled. The goal "store electronic documents securely" is composed from sub-goals. EAP delegates some goals (store documents, provide durable authenticity and integrity) to other actors (DMS provider and AIP) and provide some by itself (archive document). EAP delegates DMS provider to provide availability of documents. With DMS electronic documents are managed and securely stored. EAU delegates IAP to provide integrity and authenticity of documents. AIP actually provides an evidence of integrity and authenticity of stored documents. For this purpose the system needs to acquire timestamp from a Timestamp authority (TA). A request is delegated to the TA automatically.

For convenience we also give the description of typical activity flow of tasks once the trusted archive it is set up (see Figure 3 for more details)

Agent playing the role of EAU provides the documents that need to be stored and EAU must define needed parameters (documents to be archived, preserving policy). The EAU chooses document to archive. Before a request for archiving is sent, it needs to define metadata and archiving policy. The archiving system receives the request and creates initial archiving object with status "in process". Before the selected document is stored the archiving system examines the document. If the customer digitally signs the document AIP software needs to verify the signature and to create evidence record. Next, it calculates fingerprints (hash) of the document, metadata and other evidences. After that, it prepares a request for timestamp and sends it to the timestamp authority (TA). Acquirement of a timestamp is executed automatically by the system with use of accredited external services. If everything is correct AIP completes archiving object with additional contents and passes it into status "archived". If a problem occurs, the archiving system tries with execution of an archiving process until the process is successfully accomplished or duration time of request has expired.

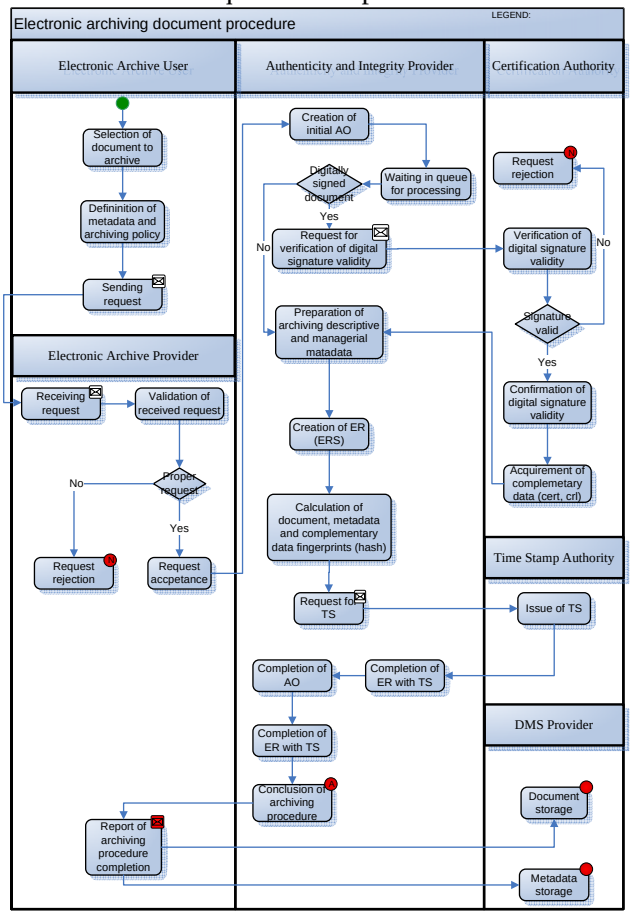

Figure 3: Procedure of archiving electronic document

***Dependencies on other patterns***

The organizational structure delivered by the trusted archiving pattern is a specialization of a generic work distribution pattern called "divide and conquer". This generic pattern is used in context of trusted archiving to provide manageability of task separation and delegation.

Further dependencies on technical patterns are given in form of solution preconditions that need to be met in order for the trusted archive to deliver the described properties. The preconditions are the following:

- Document management system (DMS) must be available to constantly assure storage integrity on technical level
- A technical system for Authenticity provision needs to be available in order to guarantee the validity of authenticity proofs on technical level

- Trusted time stamp authority (TSA) must be available

***Specific context implementation guidelines***

This pattern can be applied to different contexts. Different roles from the solution may be utilized by different organizations, totally depending on organizations' needs and preferences. These needs and preferences are normally a consequence of the size of the organization adopting trusted archiving, as well as other parameters, such as the domain of business and whether the archiving is a part of key business process.

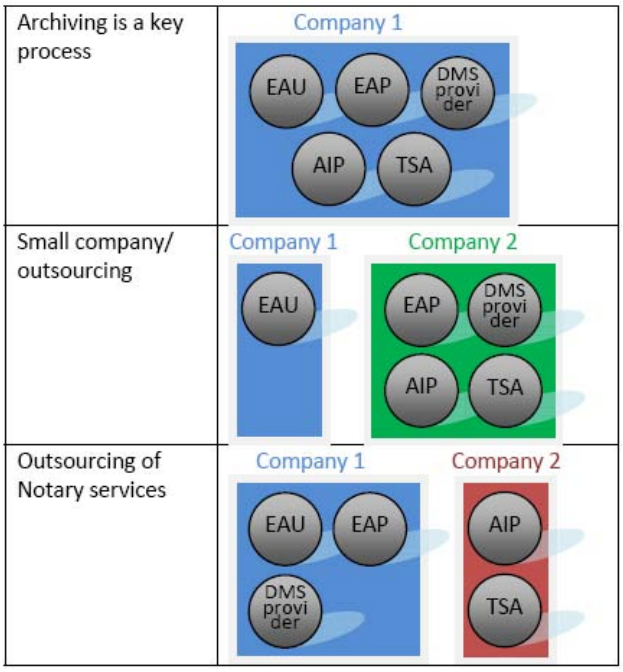


Figure 4: Distribution of rules between organizations at different pattern implementations

We give three different examples how this pattern can be applied to different organizations (see Figure 4 for more detail):

1. *Archiving is a key process*: big companies that consider archiving as their key business process, such as banks or insurance companies are able to utilize all the roles of the pattern inside their organization.
2. *Small company / outsourcing*: Small or medium sized companies may not have the necessary resources available in order to set up its own trusted archive. It is better for such companies to outsource the whole archiving infrastructure to an external partner. The external partner is the one utilizing the EAP role and all other roles of the pattern except the role of EAU, which is utilized by the small company. Because of this separation there is a need of additional agreement between the small company utilizing the EAU role and the Archive Provider utilizing the role EAP.
3. *Outsourcing of Notary services*: A bigger company that does not consider archiving as a key process might implement part of the solution concerning dependable storage, but outsource the provision of authenticity and integrity proof to a dedicated organization. Because of this separation there is a need of additional agreement between the bigger company utilizing the roles of EAU, EAP and DMS Provider on one hand and the company providing notary services utilizing the AIP role on the other.

### 3.3.2 Archiving pattern #2: setting up a legally compliant trusted long-term archive

***Problem description***

Even if trusted archive provided by pattern 1 has already been adopted, it will still be necessary for the organization to prove the validity of documents when brought to court of justice. If the organization wants to avoid providing proofs to the court for every single document, this can be achieved through accreditation of the implemented solution. This pattern shows the organizational steps needed to carry out the process of making an existing trusted archive legally valid. The property provided by such an archive is: *archive compliance with legal requests*.

Solution organized in this way will assure equivalent value of digitally stored documents with documents in paper format. Also this pattern can be applied to different context which is defined already with implementation of the first pattern.

***Preconditions and dependencies***

This pattern depends on implementation of the first one that defines distribution of the rules, activities etc. The generic solution needs to be applied to organizational structure provided by the archiving pattern #1: "A generic organizational structure for operating a trusted electronic archive". Specifically it should be applied to the present implementation of the pattern for the specific context where company decide to outsource the provision of authenticity and integrity proof to a dedicated organization, namely the "outsourcing of notary services". Therefore the presence of all the roles from the pattern 1 is a precondition for this pattern.

Other preconditions for provision of legally compliant trusted electronic archive are:

- Presence of needed actors: EAP, AIP
- Contract between EAP and AIP
- DMS system

***Solution***

Registration State Agency - RSA needs to be involved in the process. This role should be utilized by the legally appointed entity responsible for carrying out the auditing process. It will be checking necessary conditions that actors involved in provision of trusted archive need to meet. It is the entity that will in the end accredit the trusted archiving solution to be legally valid.

The following tasks need to be performed by agents playing the critical roles in a trusted archive organizational structure:

- EAP to be accredited by RSA
- In order to achieve this the following procedures may need to be carried out:
  - Registration of organization playing the role of EAP
  - Confirmation of internal rules that apply to organization playing the role of EAP
  - Technical solution used by EAP needs to be verified
- AIP to be accredited by RSA
- In order to achieve this the following procedures may need to be carried out:
  - Registration of organization playing the role of AIP
  - Confirmation of internal rules that apply to organization playing the role of AIP
  - Technical solution used by AIP needs to be verified

The solution must assure that electronic archive, which satisfies all security conditions, is also legally valid.

Therefore involved parties EAP and AIP need to sign a contract by which they obligate to perform their duties. AIP obligates to provide notary services and in exchange EAP pays for the service. Providers of electronic archive services (partial or entire) are obliged to be registered at corresponding state agency. Registration serves just for evidence and does not guarantee the quality and usability of the service or solution. They need to establish internal rules which define all required organizational procedures for preservation of electronic documents. Finally the solution needs to be accredited what means the solution is checked by corresponding organization, and the internal rules must be confirmed.

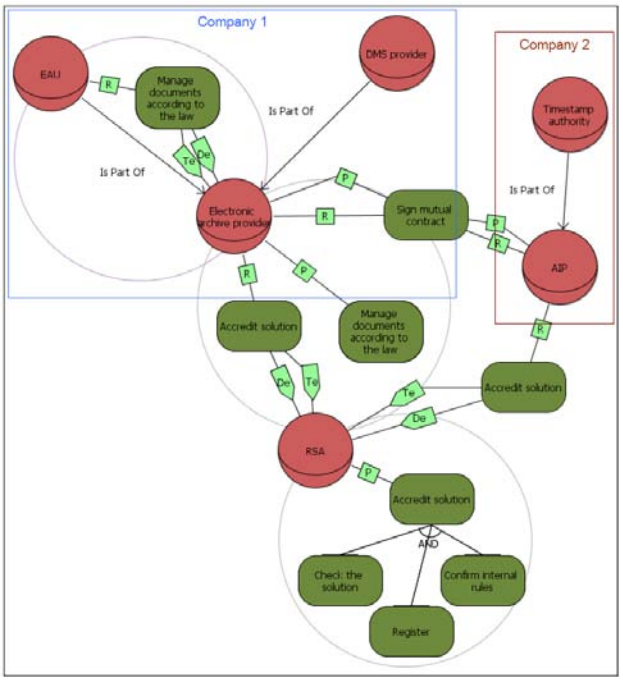


Figure 5: Tropos model for organizational solution for setting up a legally compliant trusted archive

## 5 Conclusion

Following the Serenity methodology we have presented the first set of organizational patterns applied to the domain of long term trusted electronic archiving. We have described two solutions as patterns: (i) the organizational structure required for achieving operational and (ii) organizational procedures needed to be carried out in order to set-up a legally compliant archive. We have presented the mapping of the patterns to different specific organizational contexts. In further research we aim to broaden the spectrum of organizational patterns relevant to trusted electronic archiving. One of the solutions that will most likely be adopted as pattern is the organizational management of cryptographic primitives, such as suitability of hashing algorithms or public key infrastructure schemes. Such management is very important to prevent loss of validity of proofs maintained by AIP.

*References:*

[1] Adamopoulos, D., Papandreou, C., "Design Patterns in Telecommunications Service Engineering", *WSEAS transactions on information science and applications*, Issue 1, Vol. 1, 2004, pp. 624-629

[2] Asnar Y. et al., "Initial set of security and privacy patterns at organizational level", Serenity Project Deliverable A1.D3.1, 2007.
[3] Asnar Y. et al., "Secure and Dependable Patterns in Organizations: An Empirical Approach", Requirements Engineering Conference 2007, 15th IEEE International, 15.-19. Oct. 2007.
[4] Archives of the Republic of Slovenia, "Protection of documents and archives and archival institutions act" (PDAAIA), 2006.
[5] Blakley B., Heath C., and members of the Open Group Forum, "Technical Guide: Security Design patterns", The Open Group, UK, April, 2004.
[6] Consultative Committee for Space Data Systems, "Reference model for an Open Archival Information System (OAIS)", Blue book CCSDS 650.0-B-1, CCSDS, Washington, USA, 2002.
[7] Data Capture Solutions Ltd, "ISO 15490 – the essentials", White paper, Data Capture Solutions, 2005.
[8] DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard", Department of Defense, Washington, April 2007.
[9] European Commission, IDA Programme, "Model Requirements for the Management of Electronic Records – Moreq specification" (Moreq), CECA-CEE-CEEA, 2001, available at http://www.cornwell.co.uk/edrm/moreq.asp
[10] European Commission, IDABC Programme, "Model Requirements for the Management of Electronic Records – MoReq2 Specification", CECA-CEE-CEEA, 2008, available at http://www.moreq2.eu/
[11] Gamma E. et al, "Design Patterns: Elements of Reusable Object-Oriented Software", Addison-Wesley, 1995.
[12] Giorgini P., Massacci F., Zannone N, "Security and Trust Requirements Engineering", In Foundations of Security Analysis and Design III - Tutorial Lectures, LNCS 3655, pp. 237-272. Springer-Verlag GmbH, 2005.
[13] Kolp M., Giorgini P., Mylopoulos J., "Organizational Patterns for Early Requirements Analysis", 15th International Conference on Advanced Information Systems Engineering (CAiSE'03), 2003. 17 str.
[14] National Archives of Australia, "Digital Recordkeeping: Guidelines for Creating, Managing and preserving Digital Records", Commonwealth of Australia, May 2004.
[15] Pei-Jeng, K., Terumasa, A., Hiroshi, Y., "An Experiment on Personal Archiving and Retrieving Image System (PARIS)", WSEAS transactions on computer research, , Issue 2, Vol. 1, 2006, pp. 369-373.
[16] Pfitzmann A., Köhntopp M., "Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology", Designing Privacy Enhancing Technologies: International Workshop on Designing Issuses in Anonymity and Unobservability, Berkeley, CA, USA, July 2000, Version v0.31 from February 2008 available at http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
[17] Porekar J., Jerman Blažič A., Klobučar T.,"Towards Organisational Privacy Patterns", *icds*, pp. 15-19, Second International Conference on the Digital Society, 2008.
[18] Presenza D., "Monitoring", Serenity project draft, 2007.
[19] Sanchez-Cid F., Botella A., Torres J. S., "Patterns and Integration Schemes Languages", Serenity Project Deliverable A5.D2.3, 2007.
[20] Schumacher M. et al., "Security Patterns – Integrating Security and Systems Engineering", John Wiley & Sons Ltd, 2006.
[21] Wallace C. et al., "Long-Term Archive Service Requirements", RFC 4810, The IETF Trust, 2007.
[22] Wei-Shuo, L., Shyue-Liang, W., Tzung-Pei, H., "A Bottom Up Discovery of Generalized Web Browsing Patterns", *WSEAS transactions on information science and applications,* Issue 1, Vol. 1, 2004, pp. 341-344.
[23] Williams R.F., Ashley L.J., "Electronic Records Management Survey", White paper, Cohasset Associates Inc., 2005.