Designing a Modelling Methodology for Legal Workflows

Ignacio Alamillo, Daniel Martinez
Agencia Catalana de Certificacio, Spain
{lalamillo, dmartinez}@catcert.net
Dr. Philip Seltsikas, Nikolaos Papas
University of Surrey, UK
{p.seltsikas, n.papas}@surrey.ac.uk

Abstract

This paper analyses the requirements that need to be met in order to provide a modelling methodology suitable for the modelling of legal workflows. It subsequently provides a methodology for the legal environment which meets the stated requirements.

Introduction

With the increasing ubiquity of information technologies there has been a sharp increase in the use of digital documents. One technology which has been developed to address issues relating to the authenticity of digital documents is the digital signature. Some authors refer to digital signatures as a tool which can be used to prove the authenticity of a document and verify the person that signed it [18]. The importance of digital signatures has come into focus in applications where non-repudiation is a strict requirement such as for legally binding documents [1]. Digital signatures, in combination with digital certificates, can also provide a statement of who digitally signed a document [12]. Digital Signatures can also be used to ‘prove’ that a document received by a party is the same document as was sent by the sender [5][1]. In other words, Digital Signatures have become useful tools in proving the authenticity and validity of digital documents.

Digital Signatures are gaining significant importance in the growing digitisation of government. Considerable political pressures, such as the European Union’s Manchester Declaration [9] and i2010 [8] that push for increased digital communications between administrations and citizens or businesses will necessitate the use of Digital Signatures. The increase in the exchange of electronic documents will necessitate the use of tools that can be used to verify the validity of documents exchanged. One such ‘tool’ is the digital signature policy.

In many governmental transactions, electronic documents, similar to their paper counterparts, need to adhere to administrative legislation that governs the information contained in a document, as well as its use and any approvals or authorisations that are related to the business/government process that the
document relates to. Clearly, electronic documents that require a series of approvals are not carried by hand from one office to another to be signed and stamped by each authoriser. In an electronic document workflow some other processes are required to essentially achieve the same process – electronically [4]. Legislation that governs the use of documents in government needs to be updated when these ‘become digital’ so as to provide guidelines and rules for how digital signatures are to be applied, how secure they must be, and what type of digital certificates may be used. In order to assist with this requirement, the ETSI TR 102 038 standard was developed [10], which defines the concept and make-up of a Signature Policy. A Signature Policy is an electronic document that uses a specific format known as XML [20]. The structure of the XML document is defined in the ETSI standard and it ‘captures’ the legal requirements and constraints of a digital signature. These include requirements such as the ‘meaning’ of the signatures (for example p.14 in [10]) and the ‘roles’ (for example p.22 in [10]) of those who sign the document electronically. Therefore the general aim of a Signature Policy is to define all rules and meanings of all the signatures which can be found in a particular document that is used in a particular context. In the context of digital signatures, a signature policy can be used to verify whether the digital signature and digital certificate for a specific digital document complies with the applicable legislation that governs the use of a particular document. This can contribute to determining the document’s validity [10].

A major difficulty with using Signature Policies as the electronic equivalent of the relevant legislation is that legislation is created and exists in natural language. As described above, a Signature Policy, is however a machine-readable XML document. Turning natural language legislation into machine-readable Signature Policies is a lengthy and complicated process which involves elements of trial-and-error, requires lengthy testing by both technical and legal personnel, and is therefore difficult to produce for each legislative act. The aim of the research reported in this paper was to develop a methodology that allows legislation that is expressed as natural language to be converted into valid ETSI TR 102 038 adherent Signature Policies in a precise and repeatable manner.

Related Work in the Field

The major objective of the research reported in this paper was to develop a modelling methodology to represent legal workflows. The abstraction of legal workflows and of legislation in general, is a research stream that emerged soon after the development of artificial intelligence mechanisms. Since artificial intelligence (AI) tools became available, researchers have been trying to employ AI tools in the legal domain [14].

The majority of recent research outputs in the AI-law area have had a two-tier focus; the first focuses on representing and analysing the specific area of law that is to become IT enabled or IT assisted, whilst the second tier focuses on the implementation of IT for the specific area of law. This distinction is evident in the works of Bench-Capon [2], Daskalopulu [6][7] and other contemporary
Law and Computer Science research that typifies this pattern of investigation, e.g. [3], [11] and [13].

There are several areas of law that have been researched in order to enable the use of IT. One significant example is in the area of ‘legal arguments’, which is the focus of Bench-Capon’s research. This area comprises legal arguments of a defensible context [2] as they are conducted in a courtroom (e.g. New Mexico vs. Morton,) and involves the representation and abstract analysis of the arguments brought forward by both sides in such a case. Bench-Capon advocates the use of ‘argumentation frameworks’ as an important tool in such a context [2].

Another significant area of legal and IT research is in contracts. A major author on this topic is Daskalopulu, who focuses on contract assembly [7], contract representation and analysis [6] and other related efforts in the (eventual) automated handling of legal contracts. Other research in this area includes the analysis of legal contracts through the use of Petri Nets [3] and the representation of contractual agreements using RuleML [11].

More recently, research has looked at the representation and analysis of law using modelling languages [13][16]. The difference with these more recent efforts and the preceding research is that the representation and analysis of legal matters is performed using well known process modelling languages. For example, Sijanski and Muench used the process modelling language ‘Aris’¹ in their work for the e-Justice project [16], whilst Knackstedt et. al. researched and used an extended version of ‘eW3DT’² to represent legal requirements in system design [13]. These are relevant research streams in that they are very closely related to the research reported in this paper. This research examined the feasibility of developing an Event-driven Process Chain (EPC) [15]-based graphical methodology that can be applied to a legal environment.

**Modelling Requirements**

As mentioned above, this research aimed to produce a method through which a legal workflow can be presented using a business process modelling methodology which can in turn be used to automatically produce ‘legally valid Digital Signature Policies’. The research reported in this paper was conducted to define a methodology that met a range of criteria. These are introduced below.

Our research focused on the work of the Catalan Certification Agency (CATCERT) who had already deployed a manual process for defining legal acts. In considering previous related research and examining CATCERT’s current manual processes for defining legal acts and workflows we derived a number of requirements for producing a modelling methodology with that

---

¹ Aris is a proprietary and graphical Business Process Modelling Methodology developed by IDS Scheer. For more information: [http://www2.ids-scheer.com/international/english/products/53961](http://www2.ids-scheer.com/international/english/products/53961)

would help to support our aforementioned aim of eventually automating the production of ETSI signature policies. We decided to create a first-pass (prototype) methodology that would be used to refine the requirements further. Our findings are as follows.

The notation embodied in the modelling methodology needs to be capable of representing legal acts and processes that combine to form one uniform legal workflow. That is, a legal workflow will usually comprise a combination of several legal acts and processes that interconnect activities between different legal acts. This view of activity within a legal workflow should therefore allow the depiction of the sequence of legal acts and processes that combine to form the holistic actions of the legal workflow.

Furthermore, in addition to representing sequences of legal acts and processes, the modelling notation needs to be capable of showing how individual legal acts interact with legal resources, such as digital signatures and documents. In order to do this effectively we found that the notation should be able to depict digital signatures and documents as individual and separate entities. For clarity the interaction of the resource entities with specific legal acts need to be shown. This would enable the creation of graphical representations of how a digital signature and its legal requirements (the digital signature policy) are shaped; by which legal act(s) and how this affects a specific document in a legal workflow.

A further requirement is related to data. For each legal act in a legal workflow, as well as for each document and digital signature used, the modelling methodology should enable a large number of ‘attribute data’ to be recorded. The make-up of this attribute data is determined by the requirements of the standard that the digital signature policy should adhere to. This ‘attribute data’ is important since it will make up the bulk of the digital signature policy. The breadth of this attribute data includes information such as the legal quality of actors, archival periods, signature validation mechanisms, legal restrictions and so forth.

An additional requirement was to be able to see the signature and document flows within a workflow. That is, it must be possible to view how individual signatures or documents are passed through a series of acts and processes. This view therefore allows the user to analyse the flow of any particular resource entity.

In order to meet some of the above requirements, the Catalan Certification Agency developed a paper-based methodology known as PADS (Processes-Acts-Documents-Signatures). The PADS methodology is essentially a questionnaire that has a series of questions for each point of view in a legal workflow. The PADS questionnaire aims to define legal processes by splitting them into legal acts which can be documented and signed by an actor. According to this, legal acts are carried out by ‘actors’ who have to sign a document in order to provide evidence of legal value that satisfies a legal act.
The PADS questions that deal with ‘Processes’ are centred on describing the workflow (i.e. sequence of activities) either graphically or as a list. The aim of these questions is to elicit information about the content of the relevant processes. A specific aim of this is to draw out an understanding of the regulatory environment that affects the processes.

The PADS questions in the area of ‘Acts’ have the basic aim of extracting as much contextual information as possible. There are questions aimed solely at the regulations specifying an act, questions concerning the actor(s) involved and the actor(s) legal quality (i.e. can/can not be a legal representative), the legal requirements for validating the actor(s) and other such contextual information.

The PADS area that relates to ‘Documents’ comprises questions about the documents involved in the processes described, e.g. the legal lifetime of the document(s), the type of content of the document(s), formal requirements for securing and authenticating the document(s) and specifying any conditions relating to the validation methods of the document content and author(s).

Finally, there are several questions about ‘Signatures’. These questions centre on the legal meaning of any signatures involved in the workflow, the requirements on certifying author roles, as well as a question that elicits a description of the ‘signature flow’.

Through an analysis of the PADS questions, we considered a range of possible answers, and compared this with the requirements of the digital signature policy standard ETSI TR 102 038. We found that whilst the PADS questionnaire addressed some of the data requirements of the standard (around 35%; this increases to 45% when accounting for default data), it did not address all requirements. An in-depth analysis of the ETSI standard revealed several fields that could not be filled with information derived from the output of a PADS questionnaire.

We therefore decided to retain the use of the PADS questionnaire and expand it in such a way that would encompass all necessary data required by the digital signature policy standard. The advantage of the PADS approach was that it provided a good method of extracting a wide range of information about different elements of a legal workflow.

One of our aims in conducting this work to develop a methodology was to create an environment in which a ‘novice’ user could elicit information such as through the use of the PADS questionnaire and have the digital signature policy somehow constructed ‘automatically’ for them. Due to the very specialised application area and to the availability of PADS, we decided to develop a graphical notation based on the information elicited by PADS. Our aim was to make the construction of a legal workflow and elicitation of all the components required by the ETSI policy as easy as possible for a novice user. In order to do this PADS required modification. The graphical notation that we created replaced the questions on ‘Processes’ since it provided what the questions investigated. For example, a list of activities was no longer
required since the arrangement of processes in a graphical sequence already showed this information. Another important driver for adopting a graphical workflow approach was that Signature Policies are used to produce and validate signatures but do not define which signatures are needed to carry out a specific legal act, nor do they specify the order in which the signatures need to be ‘applied’. The number and order of the signatures needed in each legal act must be specified in a graphical workflow representation. Thus, the workflow will define which signatures (and their corresponding commitments) are needed in order to carry out a legal act, whilst also being able to define the order between the Signature Policies to be applied.

Furthermore, in order to bridge the gap between information elicited by PADS and information required by the ETSI TR 102 038 standard, the ‘Signatures’ section of PADS was expanded with a considerable amount of more specialised questions.

The re-structured and expanded PADS questionnaire was subjected to a validation exercise. This revealed that all data requirements of the ETSI TR 102 038 standard were now being elicited.

Despite the extensions to PADS, the basic concepts are still present in the graphical PADS notation. Specifically, in order to verify if a document has been correctly signed, each signature can be validated according to its associated policy and all required signatures have been produced and are in the correct order.

The graphical notation, therefore, can be seen as a combination of a notation that addresses the aforementioned requirements, but also contains the information originally supplied by PADS, thus fulfilling the data requirements of the Digital Signature Policy standard. In the next section we introduce the graphical component of the proposed modelling notation.

**The Graphical Modelling Notation**

The graphical component of the modelling notation (the updated PADS questionnaire represents the non-graphical component of the notation) consists of three major components, the components have been labelled ‘main model view’, ‘attribute container’ and ‘state change model’. These components are the graphical representation of the updated PADS questionnaire and provide a comprehensive breakdown of the various components of a legal workflow. The model components supply the attribute data that is required by the ETSI TR 102 038 digital signature policy standard.

The ‘main model view’ was designed around a structure of activities and decision paths, similar to what is used in Event-driven Process Chains (EPC), but with a strong emphasis on the use of documents and signatures as process resources.

The ‘attribute container’ model was designed around the PADS questionnaire and the questions that require textual answers. In this case, an ‘attribute
container’ is attached to each act, process, document and signature employed in the ‘main model view’. This interconnection of components allows a comprehensive insight into the regulatory pressures on each component of the legal workflow.

The ‘state change model’ was designed in order to provide a view of each individual resource entity (be they documents or signatures) as they pass through a legal workflow. Additionally, every time an act or a process affects the resource entity being depicted, a notification is added to the model, indicating a state change, as well as a description of the state change.

**The Graphical Modelling Notation – Applied**

This section introduces the implementation of the modelling notation. One of the main purposes for developing this notation is to be able to describe complete legal procedures. The contextual information of the legal acts involved in the legal procedure, as well as contextual information contained in the model itself and also attached to the individual signatures and documents, will all serve as inputs that yield a digital signature policy – one that adheres to the ETSI TR 102 038 standard. This is clarified in figure 1 below.

For the automated creation of digital signature policies that contain the data outlined above, our future research will aim at constructing a facility to
produce XML output of such a workflow model. The XML output of the workflow model can then be transformed into a signature policy as all relevant data is present within the workflow model.

Using the graphical modelling notation, we defined an eleven stage method that can be used to create a legal workflow model, the details of which are outlined in Figure 2.

1. Restrict the domain and scope of the legal workflow to a specific procedure or regulation
2. Create a first sketch of the workflow and annotate specific acts that may influence individual processes
3. Identify the major actors and their departments – create their respective swimlanes[19]
4. Arrange the workflow processes in the correct manner and name them appropriately
5. For each act in the workflow, attempt to answer the PADS questions, then add the answers to the appropriate ‘attribute container’
6. Add the documents to their respective locations within the workflow, then answer their PADS questions and fill in the information into their ‘attribute container’
7. Add the signatures to their respective locations within the workflow, then answer their PADS questions and fill in the information into their ‘attribute container’
8. Apply the decision and flow paths between processes/acts, documents, signatures (including the signing processes)
9. Double-check the model for consistency and accuracy
10. Create the State Change Models
11. Link the individual documents and signatures with their corresponding state change models – verify accuracy of document and signature flows

Figure 2: 11 Steps Method

The following sections describe the three elements that make up the graphical PADS notation of a legal workflow. The three elements are the Main Model View, the Attribute Container and the State Change Model.

Main Model View

The processes and legal acts are arranged in swimlanes – graphical depictions of different organisational units to which processes and acts are assigned [19]. The processes and acts are interconnected using lines, denoting decision paths. Each process and act is assigned a responsible actor, which can be a citizen, an administrative worker, or an administrative department. Each process and act can also ‘consume’ one or more document or signature, indicating the use of a document or signature in order to perform a specific legal act or process. Each element depicted in the main model view (bar the swimlanes and the interconnecting lines) is linked with an ‘attribute container’.
Attribute Container

As mentioned above, each element in the ‘main model view’ is linked with an attribute container. The ‘attribute container’ contains controls with which information can be stored in them that can not be captured graphically. The “look and feel” of the Attribute Container is partially determined by our choice of tool, the Adonis BPMN toolkit\(^3\). The benefits of the way this facility is provided by the tool allows for necessary information to be collected in a clear and structured manner. Also, due to the tool’s organisation, the collection of information is performed very efficiently. Below is an example of an attribute container for a legal act:

\(^3\) For more information, please see [http://www.boe-group.com/jumpto.jsp?goto=ADONIS&lg=en](http://www.boe-group.com/jumpto.jsp?goto=ADONIS&lg=en)
State Change Model

As can be seen, the ‘state change model’ is very similar to the ‘main model view’. However, unlike the ‘main model view’, this model does not show all involved resource entities through the entirety of the legal workflow. Instead, there is one ‘state change model’ for each resource entity. Furthermore, every time a resource entity is ‘consumed’ by an act or process, there is an indication within the model that a state change has taken place, as well as a quick description of the nature of the model change. These models are not created manually, but with the help of the tool in which the modelling notation has been implemented (ADONIS).
Figure 5: Example of ‘State Change Model’

**Future Work**

With legal workflows modelled in the manner described above, the question remains as to how this digitised model of a legal workflow can be used to produce ETSI compliant digital signature policies. Our future research will focus on determining how the data stored in the model can contribute to each of the many data fields required by the ETSI TR 102 038 standard. Future work will also aim to produce an application which can perform this data mapping automatically. Since the modelling tool used for the implementation of the above notation includes a facility for creating XML models out of graphical ones, this facility can be used as a starting point to perform the change from graphical model to standards-compliant digital signature policies.

We believe that this would be a major contribution to the field as currently there is no structured method of arriving at a legally valid Signature Policy. The original aim of this research was to arrive at such a methodology and thus this future work is a key step to creating a methodology for producing legally valid Signature Policies. The key challenge to our future work is the ability to take all necessary information out of the graphical workflow and apply transformation rules (which will be a key research item) that transform this information into an ETSI TR 102 038 compliant signature policy. These *transformation rules*, in combination with the developed graphical notation, will therefore represent the methodology of creating digital signature policies in a structured and reproducible manner.
Conclusion

The predicted increase in electronic document exchange between citizens and administrations implies a large amount of responsibility for administrations to secure documents in a way such that the integrity of both citizen and administration is upheld. Authentication and verification tools will need to be developed and implemented and digital signatures are one of the tools that can help achieve this integrity. Digital signatures by themselves are not capable of achieving required security levels and must therefore be accompanied by digital signature policies, which carry important information about the legality of digital signatures. Since the legal environment can influence the use of digital signatures, the ‘capture’ or modelling of the legal environment is extremely important in order to be able to produce consistent signature policies that do follow legislative guidelines and restrictions. Our research has provided a method by which legal workflows and their associated regulations can be modelled in such a way as to provide useful input for the creation of legally valid digital signature policies. The addition of a graphical element to this domain aids the visualisation of legal workflows and their influence on documents and digital signatures, which is important as otherwise important interconnections may not be revealed. It is hoped that future research can deliver a complete solution to the automatic provision of digital signature policies.

References


