Policy Frameworks for Secure Electronic Business

Andreas Mitrakas
Ubizen, Belgium

INTRODUCTION

Terms conveyed by means of policy in electronic business have become a common way to express permissions and limitations in online transactions. Doctrine and standards have contributed to determining policy frameworks and making them mandatory in certain areas such as electronic signatures. A typical example of limitations conveyed through policy in electronic signatures includes certificate policies that Certification Authorities (CAs) typically make available to subscribers and relying parties. Trade partners might also use policies to convey limitations to the way electronic signatures are accepted within specific business frameworks. Examples of transaction constraints might include limitations in roles undertaken to carry out an action in a given context, which can be introduced by means of attribute certificates. Relying parties might also use signature policies to denote the conditions for the validation and verification of electronic signatures they accept. Furthermore, signature policies might contain additional transaction-specific limitations in validating an electronic signature addressed to end users. Large-scale transactions that involve the processing of electronic signatures in a mass scale within diverse applications rely on policies to convey signature-related information and limitations in a transaction. As legally binding statements, policies are used to convey *trust* in electronic business. Extending further the use of policy in transaction environments can enhance security, legal safety, and transparency in a transaction. Additional improvements are required, however, in order to render applicable terms that are conveyed through policy and enforce them unambiguously in a transaction. The remainder of this article discusses common concepts of policies and certain applications thereof.

BACKGROUND

An early example of a transaction framework is open EDI (Electronic Data Interchange) that aims at using openly available structured data formats and is delivered over open networks. While the main goal of open EDI has been to enable short-term or *ad hoc* commercial transactions among organisations (Kalakota & Whinson, 1996), it has also aimed at lowering the entry barriers of establishing structured data links between trading partners by minimising the need for bilateral framework agreements, known as interchange agreements. One specific requirement of open EDI is to set up the operational and contract framework within which a transaction is carried out. Automating the process of negotiating and executing agreements regarding the legal and technical conditions for open EDI can significantly lower the entry barriers, especially for non-recurrent transactions (Mitrakas, 2000).

Building on the model for open EDI, the Business Collaboration Framework is a set of specifications and guides, the centre of which is the UN/CEFACT; it aims at further lowering the entry barriers of electronic commerce based on structured data formats. The need for flexibility and versatility to loosely coupled applications and communication on the Internet has led to the emergence of Web services. A Web service is a collection of protocols and standards that are used to exchange data between applications. While applications can be written in various languages and run on various platforms, they can use Web services to exchange data over the Internet.

In Web services, using open standards ensures interoperability. These standards also include formal descriptions of models of business procedures to specify classes of business transactions that all serve the same goal. A trade procedure stipulates the actions, the parties, the order, and the timing constraints on performing actions (Lee, 1996). In complex business situations, transaction scenarios typically might belong to a different trade partner that each one owns a piece of that scenario. Associating a scenario with a trade partner often requires electronic signatures. When a trade partner signs with an electronic signature, she might validate or approve of the way that individual procedural components might operate within a transaction. The signatory of an electronic document or a transaction procedure depends on the performance of complex and often opaque-to-the-end-user systems.

Trust in the transaction procedures and the provision of services is a requirement that ensures that the signatory eventually adheres to transparent contract terms that cannot be repudiated (Mitrakas, 2003). Policy is seen as

a way to formalise a transaction by highlighting those aspects of a transaction that are essential to the end user (Mitrakas, 2004). The immediate effect of using policies to convey limitations is that the party that relies on a signed transaction adheres to the limitations of that policy. Policy is, therefore, used to convey limitations to a large number of users in a way that makes a transaction enforceable. While these limitations are mostly meaningful at the operational or technical level of the transaction, they often have a binding legal effect and are used to convey contractual terms. Although these terms are not necessarily legal by nature, they are likely to have a binding effect. Sometimes they can be more far reaching by constraining relying parties that validate electronic signatures. Limitations might be mandated by law or merely by agreement, as in the case of limitations of qualified signatures according to European Directive 1999/93/EC on a common framework for electronic signatures (ETSI TS 101 456).

POLICY CONSTRAINTS IN ELECTRONIC BUSINESS

Electronic signatures have been seen as a lynchpin of trust in electronic transactions. The subject matter of current electronic signature regulation addresses the requirements on the legal recognition of electronic signatures used for non-repudiation and authentication (Adams & Lloyd, 1999). Non-repudiation is addressed in both technical standards such as X.509 and legislation. Non-repudiation addresses the requirement for electronic signing in a transaction in such a way that an uncontested link to the declaration of will of the signatory is established. Non-repudiation is the attribute of a communication that protects against a successful dispute of its origin, submission, delivery, or content (Ford & Baum, 2001). From a business perspective non-repudiation can be seen as a service that provides a high level of assurance on information being genuine and non-refutable (Pfleeger, 2000). From a legal perspective non-repudiation, in the meaning of the Directive 1999/93/EC on a common framework on electronic signatures, has been coined by the term, *qualified signature,* which is often used to describe an electronic signature that uses a secure signature creation device and is supported by a qualified certificate. A qualified signature is defined in the annexes of the directive and is granted the same legal effect as hand-written signatures where law requires them in the transactions.

Policies aim at invoking trust in transactions to ensure transparency and a spread of risk among the transacting parties. Policies are unilateral declarations of will that complement transaction frameworks based on private law. Policies can be seen as guidelines that relate to the technical organizational and legal aspects of a transaction, and they are rendered enforceable by means of an agreement that binds the transacting parties.

In Public Key Infrastructure (PKI), a CA typically uses policy in the form of a certification practice statement (CPS) to convey legally binding limitations to certificate users, being subscribers and relying parties. A CPS is a statement of the practices that a CA employs in issuing certificates (ABA, 1996). A CPS is a comprehensive treatment of how the CA makes its services available and delimiting the domain of providing electronic signature services to subscribers and relying parties. A certificate policy (CP) is sometimes used with a CPS to address the certification objectives of the CA implementation. While the CPS is typically seen as answering "how" security objectives are met, the CP is the document that sets these objectives (ABA, 2001). A CP and a CPS are used to convey information needed to subscribers and parties relying on electronic signatures, in order to assess the level of trustworthiness of a certificate that supports an electronic signature. By providing detailed information on security and procedures required in managing the life cycle of a certificate, policies become of paramount importance in transactions. Sometimes, a PKI Disclosure Statement (PDS) distils certain important policy aspects and services the purpose of notice and conspicuousness of communicating applicable terms (ABA, 2001). The Internet Engineering Task Force (IETF) has specified a model framework for certificate policies (RFC 3647).

Assessing the validity of electronic signatures is yet another requirement of the end user, most importantly, the relying parties. A signature policy describes the scope and usage of such electronic signature with a view to address the operational conditions of a given transaction context (ETSI TR 102 041). A signature policy is a set of rules under which an electronic signature can be created and determined to be valid (ETSI TS 101 733). A signature policy determines the validation conditions of an electronic signature within a given context. A context may include a business transaction, a legal regime, a role assumed by the signing party, and so forth. In a broader perspective, a signature policy can be seen as a means to invoke trust and convey information in electronic commerce by defining appropriately indicated trust conditions.

In signature policies it is also desirable to include additional elements of information associated with certain aspects of general terms and conditions to relate with the scope of the performed action as it applies in the transaction at hand (Mitrakas, 2004). A signature policy might, therefore, include content that relates it to the general conditions prevailing in a transaction, the discreet elements of a transaction procedure as provided by the various parties involved in building a transaction, as well as the prevailing certificate policy (ETSI TS 102 041).