

WAYPOINT Electronic Contracting System

Introduction

Agreements are at the heart of almost everything that humans do together. No business is transacted without some form of agreement, often requiring a legally binding signature. The fact that business information systems arose long before the widespread use of the internet created a condition where each enterprise was an island unto itself, necessarily limiting signing ceremonies to offline and partially offline methods. While nearly everyone recognized the imperative of bring contracting fully into the present day, most organizations were ill-equipped to do so, since by definition, contracting is inter-organizational. Compounding that were concerns about information and data security, lingering questions about the legality of electronic signatures, and the lack of a solution appropriate for each organization's actual business requirements within the context of the type of business being transacted.

From click wrap to digital certificates to signed images to document contract management systems and secure email, there are many solutions which address pieces of the puzzle, very effectively in some cases. The problem with all of these solutions is that, in general, they fail to treat electronic contracting as a distinct type of software in itself. Being rather organic outgrowths of the existing paradigm, each of these efforts represents merely a way of solving specific problem sets, and thus ultimately suffers from a lack of fit into the actual process.

The Recombo electronic contract execution system simplifies and automates most of the process of distributing and gathering signatures on agreements. By mirroring the actual flows in the way paper contracts are generated, distributed, negotiated and signed, Waypoint is able to increase the efficiency of the entire process for any business that has the capability to access the internet. Waypoint's sophisticated workflow engine allows workflows to be further streamlined and improved beyond the scope of what is possible with courier, fax and other electronic contracting solutions. The result is a dramatically reduced time requirement from the distribution to execution and storage of agreements.

Essential elements of electronic contracting

Execution

The core use of an electronic agreement system is, of course, executing the signing of documents. This must be accomplished in a way that is legal, logically sound, and workable for the end users. Firstly, the intention of the signatory to sign must be captured in some way by the system. This can be accomplished by designing the process so that the moment of intent cannot be bypassed in the workflow, by relating the intention to sign to the document via a relational data store, or by embedding the signature into the agreement document itself, or some combination of the above. Secondly, the process of by which a signature is applied must be auditable for consistency, logic and security. Finally, the process cannot be so onerous that a significant number of users are not able to complete it.

Identity

Stipulating that an agreement was in fact executed, in order to prove that it was actually executed by the specifically named parties, it is necessary to be able to prove that each executor was, in fact, who they claimed to be. Due to the largely anonymous nature of the internet, the identity of the signatory is not intrinsically obvious. While identity is a much larger issue in the internet in general, for the purposes of electronic agreements, the degree to which a person's identity must be established varies with the importance of the agreement in questions, whether that is determined by dollar value, or social or other considerations. A variety of techniques exist for establishing identity, from process (e.g. email verification), to stored credential solutions, such as digital certificates, to knowledge-based identity verification services. The method of identity verification must be appropriate to the importance of the agreement being signed.

Non-repudiation-

In comparison with paper documents, electronic documents are inherently easy to edit in a way that is difficult to detect. This gives rise to valid concerns about fraud for completed agreements. If it can be shown that a document has been altered in any substantive way, the viability of electronic agreements is suspect. In order to prove that documents have not been tampered with, and that the content and format remains exactly the same after signing as it was during signing, a range of algorithms exist that compute a hash digest or "fingerprint" of the document at each point in the process. This digest is stored and subsequent viewings and executions of the agreement are re-processed and compared against the stored value. There are varying strengths of these algorithms, from md5 to SHA-1 to SHA-256 and beyond. In order to prevent "collisions", the remote possibility that two different documents could produce the same digest, algorithms of greater integrity than SHA-1 should be used. To make sure users are not beholden to a particular signing solution vendor, the document may include the audit trail embedded within itself so that it can be verified outside the vendor's context.

Approaches

Click-wrap

The most common form of electronic contracting is "click-wrap". These are simple forms which bind a user to an agreement by positioning text which constitutes the body of agreement at a point in the process whereby the user cannot use the product or service until they select an "I agree" option and submit this fact back to the system. One of the problems with this method is that there is no way to tie the actual person to the agreement being signed, so that authority to sign, and even the intent to sign (if signed on behalf of an organization), cannot be strongly established.

Relational data store

Another approach is to associate signatories, the act of signing and the document through a relational database of some kind. The sort of approach requires that the entire internal process by which signatures are obtained by the system be auditable, and further requires that the database be locked down. For example the concept of "write-once" should be implemented for tables in the critical path for the signing solution. Also, documents signed using this approach will not be transportable outside of the context of the vendor.

Signed Image

In this method, documents are either originated, or converted to some form of image. The image is placed in a container or environment which allows for the applications of signatures and or a certificate which signs the document. In the event that the signatures or certificate is actually attached to the image, the documents may be transportable. However, complex processing, such as full text search, dynamic interaction, etc is difficult to obtain without a host of supporting sub-systems which keep a non-signed version of the document to work on.

Digital Certificates

Digital certificates, generated for each user, and resident on the desktops of those signatories, may also be used. In this case, a certificate is generated from a certification authority, and the user applies that certificate to certain types of documents when he or she wishes to sign them. Because there may not be a central server managing the process, it may be difficult to obtain any functionality other than the simple collection of signatures. Also, of course, there is a significant administrative barrier to adoption, because each signatory must obtain a certificate from the CA.

Recombo's Approach

If you would like to obtain the other 11 pages of this whitepaper, including detailed information on the WAYPOINT approach, agreement processes, and security, send an email to Whitepaper@recombo.com. We will be glad to arrange it.