EUROPEAN COMMISSION
Information Society and Media Directorate-General

Emerging Technologies and Infrastructures
New Working Environments

FP7 POSITION PAPER ON “COLLABORATIVE WORKING ENVIRONMENTS” (CWE)

The Need for Collaboration Infrastructures for Signed Digital Documents

Title (Dr, Mr, Ms):	Dr.
Family Name:	Schmidt
First Name:	Andreas U.
Organisation:	Fraunhofer Institute for Secure Information Technology SIT
Position:	Senior Research Scientist
Address:	Rheinstraße 75
Country:	Germany
Email:	Andreas.u.schmidt@sit.fraunhofer.de
Phone:	+49 6151 869 60227
Web site:	http://www.sit.fraunhofer.de http://www.math.uni-frankfurt.de/~aschmidt

Description of the Research challenges on the area of CWE of the interest of the proposer:

In many contexts such as business, administrative, or science the need for collaborations on a shared goal increases with the growing number of EU wide and international acting companies, consortia, and, e.g., EU wide R&D projects, like the development of the Airbus 380, or the creation of a technical design, e.g. for a new car model. Aside from interoperability aspects the basis of a successful collaboration between distributed entities (humans, machines, etc.) is mutual confidence in the partners, which, as a rule, is achieved by the exchange of signed documents – memorandums, agreements, notices, contracts, et cetera – at central stages.

Collaborative working environments have to deal with the coexistence of digital and paper documents, with an increasing share of digital documents (or other forms of content) being handled in computer supported workflows. Usually paper bound originals or copies have to be filed in parallel to their digital counterparts due to high requirements – in accordance with the legislation governing the application domain – to preserve the evidentiary value of signed documents. This is costly, inefficient and, seen from the workflow perspective, leads to media breaches and out-of-band processes which create the need to correlate the electronic and paper forms of documents.

Although the technical interoperability of digital workflows and the enabling of inter-organisational collaborations is a hot R&D topic, electronically signed documents are only scarcely considered in this context. This is in accord with the slow uptake of digital signature technology in electronic transactions, despite of the enactment of the relevant legislation by the Commission and member states. In effect, this leads to media breaches at the mentioned central stages of collaborations, at which paper documents with handwritten signatures are still the state of the art. It would be desirable to lever these problems utilising the security provided by electronic signatures. However, the adoption of signature technology is slow and almost non-existent in current systems supporting digital workflows.

Three particular **processes** can be identified at which these media breaches occur:

- **Document Acceptance.** The ingestion of documents into electronic workflows is dominated today by reception and handling of paper documents, at best supporting the following digital workflows by initial paper-to-electronic conversions (i.e., scanning). Efforts to enable the acceptance of electronically signed documents are isolated and mainly related to the public sector, i.e., to e-government initiatives (for instance electronic mailrooms and the electronic submission of tax declarations). Even then, the used technology is often insular and – also due to the lack of widespread digital signature technology – not easily transferable to other sectors.
- **Document Archiving.** Longevity is a key requirement for the archiving of documents with existential value for an organisation. It is a classical security requirement in the sense that integrity and availability must be ensured over long time-spans. Electronically signed documents face severe practical problems in this respect. First, the probative force of digital signatures is limited in time since cryptographic algorithms used 'age' and become weak in confront with increasing computing power that can be used to break it. Secondly, data formats of digital documents used today might not be readable tomorrow, let alone in fifty years. Accordingly, document archives are still mostly based on paper or microfilm.
- **Document Issuance** is prone to the same problems as document acceptance. The readability of data formats and the verifiability of digital signatures by the intended receiver of a document is seldom guaranteed. To achieve the required assurance level, postal mail is the rule at least for more important documents.

In the following: if we speak of ***processing*** in summary reference to the three points above. It is important to mention that these processes often take place even in workflows within a single organisation, e.g., when a proceeding is transferred from one department to another.

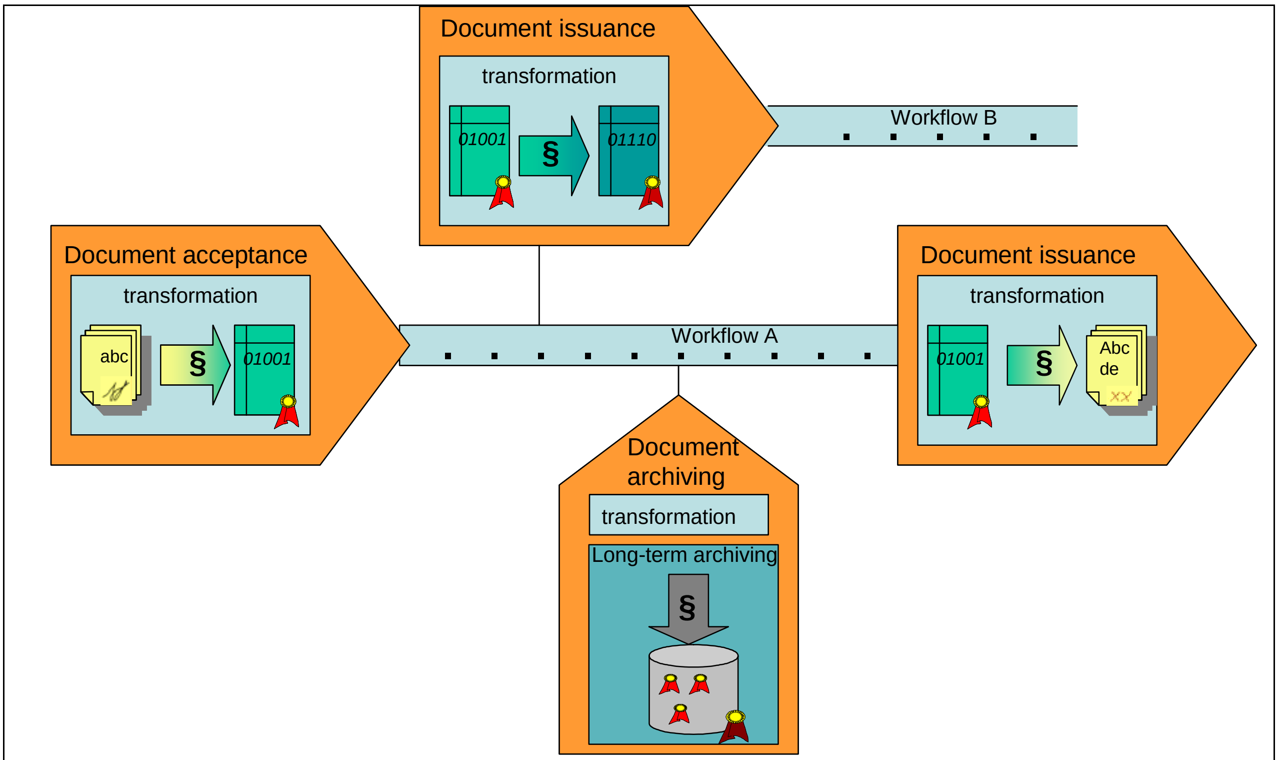

Figure: Inter-organisational Workflow involving signed documents

Today's collaboration environments don't provide securely verifiable evidence of document processing. Digital signatures provide the necessary security, i.e. data integrity, authenticity and non-repudiation. Digitally signed documents, however, have to this date not found widespread application, let alone in trans-national contexts. The latter is caused by the lack of signature interoperability concerning both legal and technical aspects. Furthermore there exists a lack of assurance of legal validity in the processing of electronically signed documents, and in particular in the transformation and long-term archiving of signed documents.

For the reasons described above, we view it as an important point for research on CWE to establish trust in collaboration and to increase efficiency by enlarging application domain for electronically signed documents by, in turn, addressing their secure processing. The processing and exchange of documents has to be considered also in international context. To that end, at least the following four core infrastructure components for signed document processing are required.

- **Signature interoperability** is a base technological infrastructure component on which the secure processing of documents rests. A common understanding of the relevance of an electronic signature must be achieved. An interoperability platform for digital signatures is needed that allows the verification, and creation of digital signatures within various technical and collaboration environments, as well as the integration of a multitude of public-key infrastructures (PKI).
- **Secure transformation** of signed documents between data formats is essential for all three document processes above. In order to support a paperless collaboration, means for a secure conversion between physical, e.g. paper, and digital representation are needed. Changing the digital document format leads to the problem that the original electronic signature breaks. A similar problem arises during digitisation of paper documents. The digital representation of a handwritten signature has not the same validity as the original. Therefore one needs means to preserve the probative force of digitally/handwritten signed documents even after transformation/conversion.
- **Long-term archiving (LTA)** can rest on established and ongoing scientific research and existing standards (IETF/LTANS). The integration to a comprehensive document longevity support platform is an important novel requirement for

collaboration infrastructures and rests on the two aforementioned infrastructures – the requirement for signature renewal in LTA necessitates signature interoperability, while transformations into durable formats become necessary at the introduction of a document into an archive or later, as formats change.

- **Legal guidelines and legally sound methodologies**. The requirements for document processing which apparently dictate the use of paper, more often than not, stem from the legal background governing the specific application sector of the collaboration workflow, e.g., compulsory periods of record-keeping. Though legislation generally allows for electronically signed documents to have the same probative force as paper documents, specific rules still cause practical problems. Existing legal requirements for document processing in different application areas and international collaboration have to be respected. Thorough research on this subject should result in guidelines to ease the transition to electronic processing of documents. In particular, a legally sound deployment methodology for the organisation of comprehensive inter-organisational workflows and signed document processing is desirable.

An anticipated solution for the described problem domain should even allow document processing to be legally secure, i.e. the use of according information as elements of proof in legal procedures. A consideration of legal implications within a number of European legal systems should be carried out. A generic concept should allow the application of signed document based collaboration in many different application scenarios, which are not supported by today’s collaboration environments. The ultimate goal is a generic architecture for legally secure document handling which can be flexibly integrated into existing intra-organisational ECMS and DMS, or can be used as an added value to inter-organisational document exchange.

Why do these research challenges have to be tackled with at European level?

Today, businesses are confronted with an accelerating competition in global markets. A chance to survive it is collaboration between companies, for which in turn trust, security, and efficiency are enabling conditions. Signed document based collaboration is needed not only by big businesses. Particularly SMEs and even individuals who offer dedicated services, should have the chance to collaborate in larger business co-operations and thus to increase their commercial relevance on the market. Public administrations likewise experience the need to collaborate with other authorities or individuals in an efficient and trustworthy way, and also the current rise of different forms of virtual cooperation (work over Internet, opportunity driven global partnerships, virtual supply chains etc.) calls for IT support for secure and trustworthy document sharing within flexibly defined workflows. Thus, collaboration using signed documents needs to be supported in a multitude of potential application scenarios in e-government, e-health, e-business, and so on. Through a flexible framework that can serve the needs of different user groups, not only more efficient procedures in one sector should be enabled but also the possibilities for inter-sectoral collaboration or electronic communication (e.g. B2B, B2C, G2B, G2C, etc.) should be increased. As a particularly desirable effect this would promote the large-scale usage of electronic signatures in Europe and worldwide.

The need for communication and transactions based on digital documents is on the rise in the common European market, in particular for trans-national applications. We should respond to this by aiding businesses and administrations throughout Europe to organise intra- and inter-organisational workflows and in effect their collaboration centred on signed digital documents. This increases the level of trust in European business transactions and therefore contributes to the formation of the common market. Furthermore, this contributes to the harmonisation of the European legal domain in the relevant field of electronic signatures. Because of the security-related nature of the pertinent subjects, research in this area enhances the deployment and application of security primitives such as electronic signatures in Europe. Through the focus on the legally valid technology evolution in Europe as a whole, the necessity of a coordinated

European strategy is exhibited and may lead to a broader distribution of necessary infrastructures in Europe. Carrying out the described research agenda will also help to unify European efforts for technical specifications, in particular, a trustworthy and reliable inter-European framework for the processing of signed digital documents. Therefore, interoperability of European digital document management systems will be fostered.

In summary European competitiveness can be enhanced. For example, the described research will enable collaboration where the partners come from different European countries, thus facilitating pan-European working groups. Furthermore, it meets the need for SMEs and citizens to be able to access and process electronic documents from anywhere in Europe, thus addressing European societal challenges (This was recently stressed again by EU Commissioner Viviane Reding when she announced the new EU I2010 initiative: « I will also set the target to create an internal market in information goods and services, such as content, games, interactive software and value added services. It is essential to create the conditions to facilitate the production and distribution of online European content, preserving and sharing Europe’s different cultural identities, strengthening the single market and the economic strength of this important sector. ».)

Industry interested on the possible outcomes of this research. Please give concrete names of IT organisations interested in **turning the research outcomes into IT commercial products/services/solutions**. Give also names of possible organisation interested **to buy** these commercial solutions/products/services.

Besides the mentioned target sectors, we view businesses and organisations handling signed documents at a large scale as the natural target for this research. This comprises financial institutions and the insurance sector, but also government authorities as a whole. On the production side, the whole IT industry which focuses on document and workflow management can benefit. So far we have confirmed interest from Ceska pojistovna, the largest insurance company in the Czech Republic and the Piedmont Region of Italy, to become adopters of the research. BALTORO Ltd. in the Czech Republic is committed to turning the research outcome into tangible software products.

Date: 07. March 2006	Andreas U. Schmidt