Legal Security for Transformations of Signed Documents: Fundamental Concepts

Andreas U. Schmidt[1] and Zbyněk Loebl[2]

[1] Fraunhofer Institute for Secure Information Technology SIT, Dolivostrasse 15, 64293 Darmstadt, Germany,
Andreas.U.Schmidt@sit.fraunhofer.de,
WWW home page: www.sit.fraunhofer.de, www.math.uni-frankfurt.de/~aschmidt
[2] Central European Advisory Group, Betlémská 1, 110 00 Prague 1, Czech Republic
ceag@ceag.cz,
WWW home page: www.ceag.biz

Abstract. Transformations of signed documents raise questions of technical and organisational nature which render the legal security of the transformed document doubtful. In particular, digital signatures of originals break depriving documents of probative force. This report elucidates legal problems, and introduces fundamental concepts of legally secure document transformations in a deliberately generic, application-independent way. A process analysis of transformations of signed documents is carried out to elicit common security requirements. This leads to the solution approach *transformation seal*, a cryptographically secured container used to ensure legal security for transformed documents by securing the content's integrity, attesting a transformation's correctnes, and attributing it to a responsible party.

1 Modern Legislation Governing Electronic Transformation and Archiving

The principal regulation of legal issues related to the electronic transformation and archiving of documents was created as early as 1996 in the UNCITRAL Model Law on Electronic Commerce [1] (UMLEC). Since its inception, the UMLEC has served as an inspiration for the most developed countries in the preparation of national legislation, and the European Commission draws on it in the drafting of European legislation addressing certain aspects of electronic communication, e.g., the recently adopted EU Directive 2004/17/EC uses the UMLEC's definition of a data message (Article I (11)).

1.1 UNCITRAL Model Law

The UMLEC presumes a consistently applied technology neutral approach and distinctions between the notions of 'data message', 'writing', 'original', 'signature', 'legalisation/notarisation', 'legal effect/evidential weight', and 'document archiving'. Basically, the UMLEC defines a writing at the lowest requirement

level as anything in any form and on any carrier that may be reproduced and read for the purposes of subsequent reference [1, Article 6]. Therefore, any e-mail messages or any texts in electronic form ought to be viewed writing as well as data messages, regardless of the level of security that may apply to them, or regardless of whether their source is apparent, let alone trustworthy.

Further, the UMLEC defines an 'original', not only with regard to the form of the original document, but also with regard to the integrity of content of it [1, Article 8]. Therefore, an n-th electronic copy of a document is deemed to be an original if the integrity of its content from the moment when it was generated in its final form can be proved. In particular, this notion was adopted in the US.

In France and the UK, this provision of the UMLEC was commented to the effect that it is difficult, currently, to talk about an original document in electronic form, and that this notion ought to be abandoned altogether. Contrary to that, it was necessary to focus on stipulating general conditions pursuant to which documents in any form (on paper or in electronic form) have full legal effect/evidentiary weight comparable to that of original documents on paper. If such conditions were satisfied, it would be possible to present the court for instance with an electronic document containing information from a document that was originally on paper, and the court ought to give such document legal effect identical with the legal effect afforded to the original document. The problem with this notion arises in situations where the law expressly requires that an original be submitted. There are only a few such provisions, however, and they can be amended.

The UMLEC also stipulates general conditions that affect the full legal effect/legal force of electronic documents [1, Article 9(2)]. This provision places an emphasis on securing the integrity of information, authenticity of the originator and credibility of the process of generation, storing and communication of data messages. The satisfaction of such conditions is to a significant extent influenced by requirements regarding a credible (authenticated) electronic signature. The UMLEC sets out the requirements applicable to electronic signatures in its Article 7. Owing to the principle of technological neutrality, it was impossible to adopt for general electronic signatures the same concrete presumptions which exist it in the EU Directive 1999/93/EC and national laws in EU member states[1] with respect to authenticated electronic signatures based on asymmetric cryptography. Such legal presumptions concern precisely the equivalent of a handwritten signature (proof of authenticity) and the integrity of content[2]. A part of the professional practise now views their absence as a drawback - e.g., in the USA where the principle of technological neutrality was also adopted.

The UMLEC distinguishes between these general conditions and electronic legalisation/notarisation. It merely recommends in this regard that any obstacles contained in national laws that prevent legalisation through electronic means be removed (e.g., changing the requirement of affixation of an official seal, etc.) [2, Article 6]. This recommendation was implemented in all the countries referred

[1] e.g. Czech Act on Electronic Signatures, Act No. 227/2000 Coll., as amended
[2] Directive 1999/93/EC

to below. The UMLEC further expressly regulates electronic transformation and archiving of documents (Article 10), drawing there on the notions of original, data message and full legal effect/evidentiary weight, and in essence merges all the requirements mentioned above. Section (1) of the said provision sets out the following three (sets of) requirements applicable to a data message that ought to meet the requirements for long-term archiving of documents in any form:

- requirements applicable to the data message (information contained therein needs to be accessible so as to be usable for subsequent reference);
- the data message needs to be retained in the format in which it was generated, sent or received (i.e., the original format), or in a format which can be demonstrated to represent accurately the information generated, sent or received *(this provision is expressly directed at transformation of documents on paper into electronic form)*; and
- such information is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

1.2 USA

In the USA, an equivalent of the UMLEC was prepared in 1999: the Uniform Electronic Transactions Act UETA. The draft law was prepared by the National Conference of Commissioners of Uniform State Laws which prepares uniform laws for the individual US states. In the meantime, the act has been adopted by an overwhelming majority of US states. In 2000, a federal law on electronic signature, the E-Sign Act, was enacted. Both laws draw heavily on the UMLEC, but further elaborate on it. They represent the latest comprehensive provision of law pertaining to electronic transactions, recognised by experts worldwide. The UETA regulates electronic transformation and archiving in Article 12. In the requirements for an original (indent (d)), the UETA includes requirements for transformation and archiving (indent (a)), as well as requirements for the full legal effect/evidentiary weight of electronic documents (indent (f)). A similar provision of law is contained in the federal E-Sign Act, Article 1 (d).

As the UETA and E-Sign Act do not apply to certain special types of documents, in 2004, the Uniform Real Property Electronic Recordation Act (URPERA) was drafted, pertaining particularly to documents related to real estate and property ownership. This is not a valid law, but was drafted by the above-mentioned National Conference of Commissioners of Uniform State Laws and is to be implemented by individual US states. It provides for electronic transformation and archiving in Articles 3, 4 and 5, where it expressly permits electronic transformation and archiving (Article 4), including the replacement of the requirement of submission of an original document with its electronic record (Article 3). Nonetheless, it does not set out general requirements the way the UETA and E-Sign Act do; instead, it refers to special commissions formed at state level (state electronic recording commissions - Article 5) that are to formulate the standards applicable to electronic administration of documents falling under the URPERA.

1.3 United Kingdom

The UK accomplished a legal status similar to that of the USA, only not pursuant to special laws but rather by virtue of court rulings. As mentioned above, English law virtually abandoned the requirement of original documents. First court rulings have been rendered in the UK that afford electronic documents full legal effect and evidentiary weight[3]. These rulings pursued requirements similar to those contained in the UMLEC. Moreover, the UK adopted laws implementing relevant EU directives, in particular Directive 1999/93/EC (electronic signatures), Directive 2000/31/EC (electronic commerce), and Directive 2001/115/EC regulating invoicing for VAT purposes, including electronic invoicing.

1.4 France

French law underwent significant amendments with regard to these issues in 2000. The French Civil Code again draws on the UMLEC and defines a data message along similar lines (Article 1316). It further focuses on the stipulation of general requirements for the full legal effect/evidentiary weight of electronic documents (Article 1316-1), again corresponding to the requirements of the UMLEC, and in the US legal regulations and UK court rulings, i.e., authenticity of originator and integrity of content. This provision is interpreted in a way allowing for electronic transformation and archiving[4]. Moreover, the Civil Code stipulates that the requirements for full legal effect/evidentiary weight shall be identical for documents on paper and electronic documents (Article 1316-3).

The Civil Code further stipulates, again similarly to the other examples, that notarial acts may be executed or archived in electronic form in accordance with implementing regulation (Article 1317). The implementing decree, which is about to be finalised, will set out detailed standards for electronic transformation and archiving with regard to documents issued by notaries and persons with similar powers (e.g. bailiffs). There is currently an ongoing debate in France whether it would not be appropriate to issue an implementing regulation also with regard to Article 1316-1 of the Civil Code. French law, similarly to UK law, implemented Directive 2001/115/EC permitting electronic invoicing.

2 Technological Development

The most developed countries in the world no longer debate whether and how electronic transformation and archiving ought to be regulated. Rather, it is the implementation of general provisions of such legal regulations that now commands attention. The situation in this area is far from standard anywhere in the world. For instance, in the USA in June 2004, the OCC (Controller of the Currency and Administrator of National Banks) issued a recommendation to

[3] see e.g. R v Spiby (1990) 91 Cr.App. R186; or R v Shepherd (1993) 1 All ER 225
[4] see e.g. L'archivage electronique, Frédéric Mascré, September 2003

banks to exercise caution with regard to a fast practical implementation of the provisions of the E-Sign Act, pointing out the absence of standards and court precedents. According to the OCC, the main problems lacking a satisfactory resolution include the electronic transformation of documents on paper signed by hand. Similar problems are addressed by the state commission established with respect to electronic real property recordation, see Section 1.2. In France, the drafting of an implementing regulation setting out detailed requirements for electronic notarial acts, including electronic transformation, is in full swing. In Germany, the government has been funding an extensive project with the aim of electronic transformation of (state) archives, where emphasis is placed on a safe electronic transformation of documents on paper, signed by hand, as well as on genuine transformations of electronic documents [3]. Several European countries already have first standards regulating electronic invoicing, including electronic transformation of older invoices on paper, or archiving. This may be due to the fact that invoices do not need to be signed, and further due to the existence of Directive 2001/115/EC that expressly regulates the electronic invoicing requirement. For instance, the electronic invoicing standards in France are regulated by a special tax instruction of August 2003. Nonetheless, there is still an ongoing debate as to whether the French law permits electronic transformation of invoices on paper into electronic form.

The IETF formed a working group for long-term archiving and notary services, LTANS [4], working precisely on electronic transformation and archiving. It has already published several Internet Drafts for long-term archiving [5]. At the same time, there are several companies worldwide (like AuthentiDate and IXOS in Germany, XEROX, DOCUMENTUM, and many more) that focus on the comprehensive electronic processing of documents. Their systems offer comprehensive solutions including security functions, and the transformation of documents on paper into electronic form. In most cases, such systems enable more functions than expressly provided for in the law. That may increase the legal risk associated with the application of the said technologies, see for instance the recent recommendation of the American OCC. The DMS industry therefore has a genuine interest in the progress and resolution of associated legal issues.

The above shows that it is currently impossible to identify business models and standards acceptable for electronic transformation and archiving. The central problems of secure long-term archiving and secure transformation of digitally signed documents are closely related, the main connection being the latent threat for long-term usability of documents of data formats becoming obsolete. This necessitates proper consideration of transformations, in principle already in the planning of an electronic archive. Legal regulations often demand time-spans for document preservation which are well beyond the expected lifetime of common data formats. After such time-spans, the 'original document' may acquire another important attribute, namely non-reproducibility, e.g., if the original signer is deceased We do not view the two issues as identical or, as is often purported, transformation as a technical sub-domain of archiving. Rather, a more generic approach suggests itself, one which enables a unified treatment, at least on a

conceptual level, of transformations of data formats, electronic notarisations, trusted ingestions and issuance of documents by public authorities, and so on (more examples follow below). The UMLEC follows a paradigm of technological neutrality which translates, in the present context, into 'transformation neutrality'. This means that transformations must be enabled and secured by fundamental methodologies which are not bound to specific data formats or underlying technology like document management systems, cryptographic (signature) algorithms, and PKI. The following sections present our contribution to the ongoing technological and scientific effort in the described problem domain.

3 Secure Document Transformations

3.1 Context-Neutrality

We introduce a context-neutral set of basic notions with the aim of defining what a secure document transformation consists of. Such abstract concepts are needed for two reasons. First, many application contexts, in particular the legal domain, possess genuine terminologies from which special criteria for the assessment of document transformations may be derived. Such notions are to be avoided in a generic analysis of transformations. Second, the properties which render a transformation secure vary strongly between application domains and transformation purposes. A transformation may be carried out for reasons of data protection or secrecy. The need for this can arise for instance when government documents are used in court, and parts of them need to be deleted beforehand. An example from the medical sector where data protection necessitates deletions is given below. But the result of a transformation might also be judged from aspects of monetary value of the result (e.g. digital images at different resolutions). The application context determines security in the concrete case. Legal regulations and considerations are of importance in many domains since they pertain to almost every part of human life and in particular to the exchange of signed documents. Thus, to obtain a concept system which is on the one hand flexible enough to span many application domains but on the other hand independent of them, a certain level of abstraction is inevitable. A second goal of these abstractions is to elicit the interface between the 'real world' context, in which humans ultimately interpret and assess documents, paper as well as digital ones, according to their meanings, and the aspects of secure document transformations which are amenable to a formal analysis. This enables the delineation of limits for the formalisation and consequently the automation of transformations.

3.2 Purpose and Purport of Transformations

The **transformation**[5] of a signed document is the deterministic conversion of a **source document** with a certain purport into a **target document** with a

[5] Here we address not only transformations between electronic documents (E→E), but also those involving paper documents as source or target (P→E and E→P).

certain purport. The **purport** of any signed document is to be understood pragmatically as the union of its possible utilisations within the context of the given application domain, i.e. those usages of the document which can be realised in it[6]. In principle the purport of the target document can be larger, smaller or equal to that of the source document, but apart from these exceptional cases their respective purports are rarely directly comparable. The **purpose** of a transformation is to obtain a target document with a certain purport from a given source. In general, the purport of the target will be partly determined by the source, often in a restrictive sense. At this point, we do not yet differentiate between contents and signatures which are both counted as contributing to the purport, and can therefore support the purpose of the transformation as well as determine it.

The three mentioned special cases of transformations are fundamental in the sense that other transformations can be considered as mixtures or combinations of them. They correspond to three fundamental purposes.

1. The target has to convey — as far as possible — an identical purport as the source if it is to be replaced by the former. ***Examples*** of **replacement** documents are attested copies (exemplifications) of paper documents[7]; P→E transformations as pre-processing steps of digital workflows. Ensuring the readability of a document for the addressee can often necessitate transformations of data formats, for instance when a document is submitted to a government authority.
2. If only a **partial copy**, restricted to certain utilisations is required, the purport of the target is less than that of the source. ***Examples*** comprise attested excerpts from official records for designated purposes; anonymised versions of documents for reasons of data protection; health records might be anonymised for usage in medical studies, yet keeping attributability to the attending physician (by his signature of the source).
3. A transformation may entail the **valorisation** of a target document with respect to the source, i.e., enable certain utilisations that are beyond those of the source. A simple, yet practically relevant example is the migration of an electronic document format to a new version by addition of an empty field for later use; by addition of an alternative font or other representation a document can become accessible to handicapped persons.

It is desirable to distinguish the notion of transformations against genuine administrative procedures and workflows in which documents are recombined and meaningful contents can be added (e.g. another signature to a file in circulation).

Thus we define that valorisations by adding contents or signatures do not fall into the considered category of transformations.

[6] If the context could be formalised in the sense of a formal languages, a usage would be a model of it in which the document is a valid expression, and the purport would be the union of all those models — but this is hardly ever feasible in practise.

[7] Note that identical copies make no sense as E→E transformations since it is loss-free and the original digital signature remains valid. Here, replacements of signed digital document are understood as resulting from a nontrivial conversion of contents which are free of losses and additions.

3.3 Faithfulness, Trustworthiness, and Security

To satisfy a purpose, a transformation must fulfil the appropriate requirements of **faithfulness**, to be understood as 'converting the contents faithfully for the desired purpose' as opposed to one-to-one correspondence of source and target contents. Faithfulness pertains to all relevant parts of source and target, including signatures. The referral to revisable properties of source, target, and transformation is a characteristic of the concept of faithfulness. This is in intentionally in contrast to the differences between the semantic content, i.e. the meaning, of source and target, which can hardly be grasped formally. Which properties *must* be inspected to assess faithfulness depends on the purpose of a transformation. What *can* be inspected, depends on the source and target documents as such.

Examples: Faithfulness can be assessed on very different levels. It can be sufficient to check resolution and colour depth of a scanner, or necessary to compare source and target letter-wise. The adequacy of the source's data format can be as relevant as its printing quality if it is a paper document. Properties of the transformation may be important, e.g., that the conversion algorithm eventually deletes all personal data in a document that is to be anonymised.

Essential for faithfulness is also the question whether the data formats of source and target are appropriate to present all signed contents correctly. This is necessary to enable forensic inspection of a transformation and requires a proper consideration of the presentation problem[8] for signed digital data.

Without appropriate security measures, the *a posteriori* survey of faithfulness cannot be carried out. Thus, in order to arrive at a **secure transformation**, a record must be kept which asserts that the target has the right faithfulness to the source according to the purpose of the transformation. The **trustworthiness** of this assertion means that it can be retraced at later times, what kind of transformation has taken place and how, that faithfulness has been assessed and by whom, and finally who is responsible for the transformation and the assessment of the result. The necessity to enable forensic inspection sets high standards for trustworthiness in that the target must serve its purpose *even if the source is no longer available*, the most important examples being non-reproducibility and obsolete data formats.

Several instances can assess the faithfulness of a transformation and attest it at the end of the process. In a large-scale application, the transformation system itself can affirm that a certain algorithm was applied for data conversion and, e.g., that source signatures have been verified successfully, whereas in the case of notarisations it is necessary that an authorised person inspects faithfulness, and establishes trustworthiness by noting the inspection result and confirming it with his signature. Figure 1 compiles the notions introduced, and is to be understood as follows. A secure transformation is ensured through the trustworthiness of faithfulness for a given purpose. In turn, the purpose is the conversion between source and target with their respective purports. A central result of this system

[8] Also termed 'What You See is What You Sign' (WYSIWYS) problem [6,7].

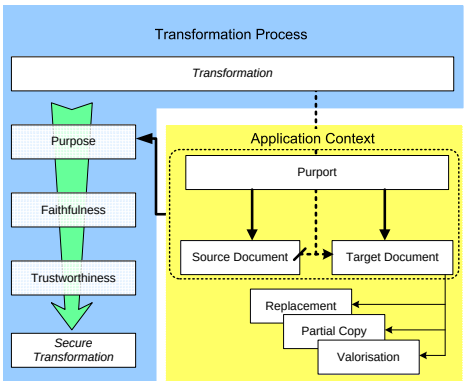

Fig. 1. Fundamental concepts of secure document transformations

of concepts is that application context and transformation process are linked exactly where the purpose is determined by the desired changeover of purports. Here lie the main difficulties for the formalisation and practical realisation of secure transformations.

4 Process Analysis of Document Transformations

To fulfil the requirements of a secure transformation laid out in section 3, it is not enough to convert the contents of a document 'in all conscience'. Even in the case of simple format conversions, additional process steps and organisational measures are required to ensure security. To elicit these requirements, a procedural analysis of a generic transformation process is helpful. In the following, a transformation is presented as a sequence of phases, independently of the kind of transformation (P→E, E→E, or E→P). This yields the maximal set of high-level **transformation phases**, with the understanding that in special cases some of them can be less important, be subsumed under or combined with another, or be parallelised if they become logically independent. Figure 2 gives an overview.

4.1 Pre-processing

Classification. In an initial step the source document is inspected to determine the purpose of the transformation. Apart from ascertaining source formats like 'Word document' or 'technical drawing on paper', this is essential for the whole following process. The classification does not only determine the relevant properties of the source but also those of the target and the transformation, which have to be satisfied to achieve the desired faithfulness. From this classification follow the rules that govern the way in which trustworthiness is to be established, in particular which data from the process must be kept for forensic inspection and which checks have to be performed on the target (see below).

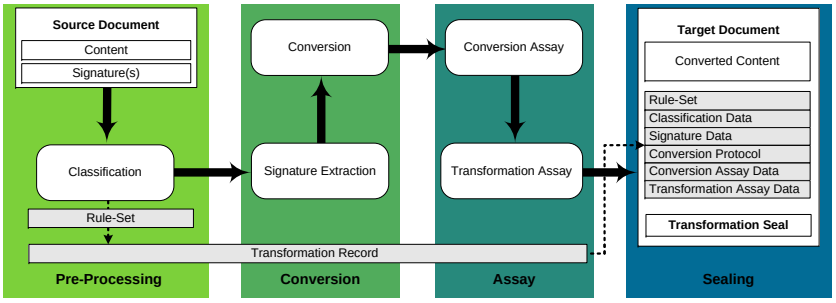

Fig. 2. Processual view on secure document transformations

Examples: Assume the source is a construction drawing that is to be replaced for electronic processing of an application by a city building authority. Then, dimensional accuracy and preservation of colours are essential criteria for faithfulness. Faithfulness and the possibility to revise it afterwards must here be ensured through usage of devices and software of appropriate quality, suitable target data formats (JPEG, e.g., is known not to be adequate for line drawings due to artifacts), and a proper choice of settings. In a secure e-government workflow, the requirements on the target with respect to cryptographic security and signature level might be low, and an automated signature applied by the transformation device can suffice. Classification can be carried out by a human inspector who checks, e.g., a paper drawing for qualitative defects, or in a highly automated way by checking that an XML document satisfies the syntactic rules of a certain schema.

The classification also determines if the source is at all appropriate for the desired purpose. An important example is the mentioned presentation problem of signed digital data, which can raise requirements for presentation components in the transformation system, set limits on automation, or even completely prohibit a secure transformation. Even for signed paper documents the proper handling of marginal notes, cancellations, and corrections of text must be completely and clearly prescribed. On a higher level, (legal) formalities that have to be satisfied by the source, for instance the presence of a certain number of signatures in the right places, can be criteria to decide if it is admissible for transformation.

Before delving into the transformation process proper, two basic data structures must be introduced.

The **rule-set** is, along with the classification data describing the source and the transformation purpose, a central result of the classification. It is an abstract term for the comprehensive set of rules governing all the following phases. Yet, it has a very concrete meaning in every special application case, comprising organisational provisions, technical measures, attributions of responsibility, rules for signature verification and generation, etc. Generically, the rule-set consists of a combination of machine-processable instructions, with normative prescriptions understandable only by humans. In some cases, like notarisations, the latter can

already be implicated by existing legal regulations. Since application scenarios with transformations for special purposes abound, it is pragmatic to define generic rule-sets for particular domains and adapt them through *profiles* which reference the generic rules and specialise them appropriately. It is desirable that the generic rule-sets be extensible, modular, combinable, and parameterisable.

As a data container which carries the information compiled during the transformation, the **transformation record** is useful not only for purely technical reasons, but also to establish security by conserving relevant meta data and, e.g., protocols of the conversions and inspections carried out in later phases. The first item in the transformation record is the rule-set.

The transformation record serves also to ensure the proper binding of relevant data with each other. In particular: 1. The source contents must be uniquely identified throughout the whole process, for which the record carries an identifier. 2. Likewise, the rule-set must be unique during the process. 3. The integrity of the target's contents and their association with the source's must be ensured. 4. Protocols and meta data generated must be kept unique for the process and unadulterated.

While in closed transformation systems the record may be a simple data container storing the objects mentioned, distributed processing or genuine security requirements can necessitate that portions of it are cryptographically secured to maintain the mentioned bindings and data integrity.

4.2 Conversion

Signature Extraction. During signature extraction, the signatures of the source are gathered from it and added to the transformation record as source signatures. The rule-set determines whether digital signatures must be verified or the signers of handwritten ones be authenticated. In this case, it also prescribes validation policies and names the signature data to be carried to the record (e.g., time stamps, attributes, etc.), and the result of the validation is also added to the record.

Conversion. In this phase the proper conversion of source to target contents takes place according to the rules of the rule-set. Apart from the target contents, a conversion protocol and error log is filed in the record.

4.3 Assay

Conversion Assay. In many, but not all cases it is possible to include two steps of *ex post* inspection into the transformation process to raise the level of trustworthiness. To indicate that these steps can comprise a mixture of human inspection of the converted contents, automated comparisons with the target, consistency checks on the data of the transformation record, we use the not very common word 'assay' for them[9].

[9] This is also to distinguish it from the notion of verification which is often understood as being specifically bound to digital signatures.

The first step assays the results of the conversion of the contents by any means possible, and as prescribed by the rule-set. As mentioned, this can mean anything from a person comparing source document and converted contents using a trusted viewing component, to merely checking the syntactic compliance of the converted contents with a specific data format (e.g., an XML Schema). Similar checks, if they have not already been implicitly applied during signature extraction, can take place for signature data. Most importantly, the source can at this point be discarded from the transformation process if this is allowed and the conversion assay leads to a positive result — both criteria being specified, again, by the rule-set.

Transformation Assay. A final assaying step can inspect the correctness of the whole transformation process. For instance in distributed transformation systems, it can be necessary to ascertain that all necessary phases have been traversed, or to counter-check the hash values associated with certain parts of the transformation record.

4.4 Sealing

After the two assaying steps have obtained a positive result, the transformation record is complete and the transformation as such is ended. It remains the task of securing these results to achieve the ultimate goal of a secure transformation. For this, a **transformation seal** is attached to the transformed document and signed by the transforming entity.

The result of a transformation needs to be secure even if the source is not available for later comparison. This is the main reason why relevant data produced in the transformation process must be persistently and trustworthy bound to the target to enable a thorough forensic inspection. This possibility to assess the quality of a transformation *a posteriori* is an important building block for the probative force of the target. It is embodied in three subordinate goals, which describe the essential purpose of the transformation seal. 1. Securing the integrity of the transformed document, and other recorded data. 2. Attestation of the correctness of the transformation according to the specified rule set. 3. Attribution of the transformation to the transforming entity and non-repudiation of that fact.

In general, the rule set will contain instructions on which parts of the transformation record need to be transferred to the transformation seal. The seal attests that the transformation process was carried out correctly according to the rule set and that the desired faithfulness between source and target is thus achieved. Technically, the transformation seal can be realised as a cryptographically secured data container and selected data from the transformation record and other relevant meta data. It always has to be (digitally) signed by the entity or person that performed the transformation.

In particular in the assaying and sealing steps specific need for human inspection can arise for technical, security, and legal reasons. A regular inspection of the transformation system and probing of results is perhaps a standard organisational requirement for secure transformation systems. If the content of

the original is not structured, the transformation itself must in part be carried out by hand and consequently the result should be (independently) inspected by a human. Legal responsibilities borne by the person sealing the target may, as is likely to be the case for notaries, entail the necessity of inspecting the target. Needless to say, human interference always introduces its own risks into technical processes. Since it is unavoidable in general though, technology must support secure and failsafe means for it, e.g., trusted viewing components in view of the mentioned presentation problem, and trusted signature terminals. The remaining risk of malicious behaviour is, however, already covered by civil and criminal legislation, for instance with regard to the liability in case of negligent or fraudulent use of notary or official seals.

5 Case study: Secure Translations

With the structure of the transformation processes at hand, we present a final ***example*** to exhibit their scope, which by no means is restricted to conversions between data formats. It also sheds some light on the limits of automation of legally secure doument transformations. Authorised translations[10] are essential for transnational document exchange. Let us, as an abstract exercise, describe an authorised translation as a document transformation — classically between paper documents. The translator classifies the source by checking it for illegibility or other severe defects that would forbid performing a translation, and also inspects the contents to avoid becoming involved into obviously illegal proceedings. After conversion of the contents by translating it to the target language, she attaches her seal to source *and* target in a way which makes them inseparable as items of probative force — by stapling the source with the target and stamping the seal over the staple. She finally applies her written signature to the target to authenticate the target and the seal. The purports of source and target are not bound to special area, and therefore the purposefulness of the translation depend on the competence of the translator and is subject to human error. Thus, a secure transformation can only be achieved through the organisational requirement that the translator possesses a certified credential (the seal). The seal ensures trustworthiness in two senses. It attests the capacity of the translator to convert the document contents faithfully, and ensures the possibility to forensically compare source and target.

Interestingly enough, a counterpart for authorised translations is completely missing for electronic, digitally signed documents, though it would be very useful. We offer some thoughts on it at a high level, based on the concepts developed, and following the process structure worked out above.

[10] Under German law, an authorised translation is performed by a professional translator, sworn, registered with a certain judicial circuit, and equipped with a special seal for the purpose of translations. The special prerequisites for authorised translators vary within Germany between federal states. In most states a translator is required to sit a state exam before being able to apply for authorisation.

The classification of the source in the case of paper documents is rather simple for the translator who essentially checks if the document is written completely in the proper source language and is free from qualitative defects which would bar him from reading and translating it. The latter is a bit more complicated for electronic documents since the presentation problem has to be taken into account. The translator must be sure to be shown all signed contents. This leads to the first organisational requirement of the rule set, namely that the translator possesses a trusted viewer for the source signed document format This implicitly entails that he has access to the PKI in the source country that was used to create the source's signatures, which can be utilised in the next step.

Signature extraction for E→E translations clearly offers more possibilities and variants than for paper documents with handwritten signatures, where signer authentication hardly ever takes place and targets mostly carry a note 'illegible signature' in the approximate place of the original ones. In contrast to that, the translator can verify the digital signatures in the source and carry that verification data into the target in some form. Depending on the level of PKI interoperability between the two countries in question, the translator could either — if the two respective CA domains are not connected — serve as an independent authentication instance for signatures from the source country and attest their validity through his transformation seal. For this, bilateral accords and a special authorisation of the translator from the target country (where the signatures are to be accepted) would be necessary. Or, in the more preferable case where the CAs are bridged by a transnational infrastructure like that envisaged in the European Bridge CA project [8], source signature verification can be directly, and without special organisational prerequisites, be carried out by the translator as well as by the target's recipient (i.e., where the document is to be utilised). In both cases however, it makes good sense to carry the original signatures completely to the target for forensic inspection. If the source consists of signed and unsigned data and/or carries more than one signature over different portions of it, the pertinent associations must be recorded.

Clearly automation of content conversion will not be possible in the foreseeable future, and can only be carried out by a responsible human being. This simplifies the transformation process. In particular, conversion and transformation assay become implicit steps carried out by the translator while translating the contents.

Three simple rules govern the sealing of the target. 1. The certificate of the translator must be issued by an appropriate authority of the target country and identify him as an authorised translator. 2. The translators signature authenticates at least source and target contents, and if desired also the signatures of the source, to enable forensic inspection. 3. If there is a many to many association between source signature(s) and portions of signed data, this must be re-traceable in the target by introducing appropriate meta-data structures.

Requirement 1. is in fact paradigmatic for the transformation seal. In analogy to paper documents which are signed *and* sealed, two authentication characteristics will generally be required for a legally secure seal. An electronic signature

identifying the transforming person (or entity, where such is admissible), and a means to authenticate his/her role as a person authorised to carry out the transformation. Technically, a solution through the use of attribute certificates in transformation seals can be envisaged. Since the issuance of 'seals' to notaries, authorised translators, public officials, etc., is governed by detailed legal regulations, and organised in highly heterogeneous and de-centralised administrative infrastructures, the actual implementation of this sound technological solution approach still poses a non-trivial organisational problem. Questions to be resolved include decisions on the carrier and operator of the certificate infrastructure, cost-sharing between administrations, guaranteed service availability, regulation and of certificate revocation[11]

6 Conclusions

Assuring legal security of document transformations is a demanding task necessitating an interdisciplinary approach. Such an approach must combine organisational measures with technical solutions to meet the legal requirements pertaining to a concrete application case. In some cases it may be doubtful whether legal existing regulations, e.g., those of EU member states that realise the Digital Signature Directive and subsequent regulatory statutes, suffice to achieve the necessary security for transformed documents. Concrete solutions for a broad application spectrum should be devised on the basis of the present concepts. These comprise organisational guidelines, process and technical prescriptions, as well as generic software components which perform the transformation process, and realisation of the transformation seal. This work programme is at the core of the project TransiDoc [3].

A point for current research is the instantiation of rule-sets. The general concepts presented above cover a wide range of transformations, too wide to be covered by uniform rules which do not remain on the level of commonplaces. The central idea here is to come to concretely usable rule-sets by profiling along the two axes of application and legislative domain. The latter regards the projection of organisational and technical guidelines to national legislations, whereas the former concerns those rules which are determined by the purpose of a transformation and entail, e.g., machine-processable rules for transformation systems. These rules delineate the boundaries of the notion of transformation, for instance the classification P→E, E→E, and E→P, replacement, partial copy, and valorisation, and more specifically changes of data format, formatting, and layout. The two axes are clearly not orthogonal. An intermediate aim is to create a methodology and standard data structures for profile creation and recording.

Besides the problem of long-term conservation of digitally signed data, which is addressed, for instance by LTANS, see also [9,10,11,12], legally secure trans-

[11] In the German Signaturgesetz, the relevant regulations governing issuance and revocation of, and authority over attribute certificates are stipulated in §§5, 7, and 8, respectively.

formations may be the most pressing issue for business and legal relations based on signed electronic documents.

Acknowledgements

The parts of this report authored by A. U. Schmidt are results of the project TransiDoc — Legally Secure Transformations of Signed Documents, funded by the German Ministry of Economy and Labour under contract no. 01 MS 401. Full responsibility for the contents of this report resides with the authors. A. U. Schmidt wishes to thank Stefanie Fischer–Dieskau, Thomas Kunz, and Ursula Viebeg for discussions.

References

1. The UNCITRAL Model Law on Electronic Commerce. www.uncitral.org/english/texts/electcom/ml-ecomm.html. 1, 2
2. Guide to Enactment of the UNCITRAL Model Law on Electronic Commerce. www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf 2
3. Website of the TransiDoc project. www.transidoc.de 5, 15
4. Long-Term Archiving and Notary Services Working Group of the IETF. ietf.org/html.charters/ltans-charter 5
5. Wallace, C., and Chokhani, S., 2003. Trusted archive protocol (TAP) IETF Internet draft. www.ietf.org/internet-drafts/draft-ietf-pkix-tap-00.txt. 5
6. Landrock, P., Pedersen, T.: WYSIWYS? What you see is what you sign? Information Security Technical Report, **3** (1998) 55–61 8
7. Schmidt, A. U.: Signiertes XML und das Präsentationsproblem, Datenschutz und Datensicherheit **24** (2000) 153–158 8
8. Website of the European Bridge CA project. www.bridge-ca.de 14
9. Ansper, A., Buldas, A., Roos, M., Willemson, J.: Efficient long-term validation of digital signatures. In: Proceedings of 4th International Workshop on Practice and Theory in Public Key Cryptography (PKC 2001), Korea; 2001, 402–415. 15
10. Dumortier, J., van den Eynde, S.: Electronic signatures and trusted archival services. In: Proceedings of the DLMForum 2002, Barcelona 6–8 May 2002, Luxembourg, Office for Official Publications of the European Communities, 2002, 520–524. 15
11. Lekkas, D., Gritzalis, D.: Cumulative notarization for long-term preservation of digital signatures. Computers & Security **23** (2004) 413–424 15
12. Website of the ArchiSig project. www.archisig.de