Motivations for a Theoretical Approach to WYSIWYS

Antonio Lioy, Gianluca Ramunno, Marco Domenico Aime, and Massimiliano Pala

Politecnico di Torino, Dip. di Automatica e Informatica,
Corso Duca degli Abruzzi 24, Torino Italy
{lioy, ramunno, m.aime, massimiliano.pala}@polito.it

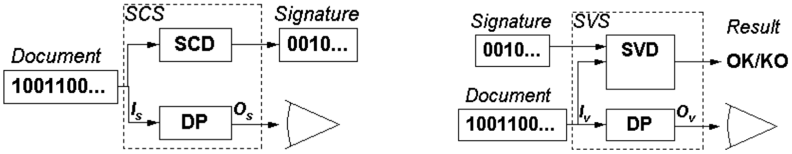
The statement "What You See Is What You Sign" (WYSIWYS) expresses a functional requirement for digital signatures of electronic documents, in particular when considering legally binding signatures. However this statement is intrinsically wrong. In fact a signer never really sees what he digitally signs, namely the bits of the electronic document, but he sees only one of the possible representations of these bits. This is due to the theory and the technology underlying the actual implementations of the digital signatures. Moreover, while the acronym refers only to the presentation on the signer side, in legal settings the presentation on the recipient side must be also taken into account as well as the relation between the twos.

The current status of research in this field can be summarized as follows. Many different definitions of WYSIWYS can be found and sometime this requirement is described only through some of its supposed effects. Therefore a clear and unambiguous definition of WYSIWYS is still missing. Conversely many security threats related to the document presentation have been described. In addition some theoretical and practical solutions have been proposed to design applications capable to properly present the electronic documents. Anyway many proposals take into account only a subset of the problems to be solved while others guarantee a correct presentation at the price of compromising their usability. We think this is the current situation first because the *exact* requirements for the document presentation on both the signer and the verifier side have not been clearly identified. Then because of the lack of a theoretical and comprehensive model to deal with these requirements. In this short paper we intend to show one of the possible directions the research in this field could move towards.

Fig. 1.1(a) shows a simplified and high level model of a Signature Creation System (SCS). The document bit string is displayed by the Document Presenter (DP), a set of software components and of a hardware device; it is then digitally signed by means of software components and of the Signature Creation Device (SCD), often a hardware device. First, there is the need to guarantee that the input to both the SCD and the DP is exactly the same bit string, that of the document being signed. This can be achieved by designing a proper architecture for the SCS (e.g. CEN-CWA14170). Similar considerations hold on the verifier side about the input to the DP and the Signature Verification Device (SVD) in a Signature Verification System (SVS), see Fig. 1.1(b).

Now, what relation does exist between the bit string to be signed or verified and what the human being reads, namely between the DP input (I_S or I_V) and its output (O_S or O_V)? *What do the signer and the verifier see?* What is really displayed by the DP? We can say that it depends on how the sequence of bits is "interpreted" by the DP. It takes as input the document bit string and transforms it into physical quantities that appear as symbols and images meaningful for the human being. Therefore both the signer and verifier always see the result of transformations applied to the document bit

J. Dittmann, S. Katzenbeisser, and A. Uhl (Eds.): CMS 2005, LNCS 3677, pp. 289–290, 2005.
© IFIP International Federation for Information Processing 2005



(a) Signature Creation System

(b) Signature Verification System

Fig. 1. Simplified models of a SCS and a SVS

string: the signer sees the DP output (O_S) of the SCS while the verifier sees the DP output (O_V) of the SVS.

Given that, we think that the WYSIWYS functional requirement should be defined as follows: *"the presentations O_S on the signer side and O_V on the verifier side* must be *semantically equivalent at each verification done by any verifier at anytime after the signature creation and by using any computer system, application or configuration"*.

The legal rules for legally valid digital signatures can impose stricter constraints on the document presentation and these constraints may differ from country to country. Anyway we think that, from the functional perspective, the above constraint is the minimum to be met. In our opinion, in fact, there is no need for the two physical presentations to be identical. Moreover this is a goal really difficult to achieve because of the variety of systems and platforms deployed and of their possibly different configurations. An example of different physical presentations with the same semantic is given by the use of the fax machine. An order placed by fax is not to be invalidated simply because on the recipient side the quality is lower than on the sender side, if it is possible to verify that the received document is semantically complete and unambiguous. Thus imposing the same physical presentation would be an oversized constraint. Instead, the use of a less featured DP on the recipient side should be possible.

Let F_S be the sequence of transformations done by the DP over the document bits on the signer side, then $O_S = F_S(I_S)$. Let F_V be the sequence of transformations done by the DP on the verifier side, then $O_V = F_V(I_V)$. Let doc be the document bit string sent as input to the DP both on the signer and the verifier side and $\overset{sem}{\equiv}$ the semantical equivalence operator. Then the WYSIWYS requirement can be expressed as $F_S(doc) \overset{sem}{\equiv} F_V(doc)$ and this has to be true any time (after the signing time) the F_V transformations are performed and whatever hardware-software platform and configuration is used.

To define the real technical requirements and constraints to be applied to the SCS and SCV architecture in order to satisfy the WYSIWYS requirement as defined above, we need to model the sequences of transformations F_S and F_V. This could be done by defining an abstract model based on the actual hardware-software architectures, by formalizing F_S and F_V in terms of mathematical functions and by studying the properties they must have to satisfy $F_S(doc) \overset{sem}{\equiv} F_V(doc)$ independently from the time when and the platform where the F_V transformations are performed.

Such a theoretical and comprehensive model could be used as a reference to evaluate the trustworthiness of existing applications as well as to design new usable WYSIWYS architectures.