Digital signature services for users
Improving user experience to support trust among work partners

Lorraine Tosi\textsuperscript{1,2}  
Phd Student  
lorraine.tosi@utt.fr

Aurélien Bénél\textsuperscript{1}  
Associate professor  
aurelien.benel@utt.fr

Karine Lan\textsuperscript{1}  
Associate researcher  
karine.lan@utt.fr

\textsuperscript{1} Tech-CICO, Institut Charles Delaunay (UMR CNRS), Université Technologique de Troyes  
\textsuperscript{2} Lex Persona, Troyes

1. INTRODUCTION
Fifteen years ago, most countries adopted digital signature as a legal equivalent to its physical counterpart \[1\]. But contrary to its great potential on streamlining work processes and business, digital signature is still underused. Whereas laws are usually low detailed, many technical and management standards specify how to implement digital signature services that should be admissible in a court of law.

Sadly enough, user tasks on software complying with these standards are known to be “the most difficult computer task[s] that [a research center] had ever asked [their CS engineers] to do” \[2\]. Hence it leads designers to a quanty developing such apps: standards require a certain amount of steps, whereas users are still looking for the easiest way to achieve their goal of signing a document.

One could even legitimatly think that it is better to ban a technology with a legal value that is not understood by their users (e.g. in ID cards \[4\]). Digital signature is often interwoven with “digital trust”, but if trust is related to “the risk you are willing to take” \[3\], what would be “digital trust” if you do not understand the risk taken in signing a document and checking (or not checking) someone else’s signature. Trust considerations arise: Will the service and proofs be available whenever I need it? a hacker view and alter proofs? Will the technology chosen by the service provider be accepted by a court? Trust is not enacted. How can we give rise to this trust and maintain it throughout the use of digital trust services?

We will make hypotheses on approaches in digital signature services that could have a positive impact on trust. Then, in section 3, we will present changes on visualization, interactions and processes that we experimented in a software dedicated to intellectual property.

2. HYPOTHESES
2.1 Learning by doing
As we saw earlier, one of the impediments to the use of digital signatures is a lack of understanding about how it works. Neither oversimplification nor display of all its technical details proved to help users successfully learning how digital signature works.

Indeed, the user faces a new and complex “apparatus”. If this apparatus were mechanical, the user would probably try to “learn by doing”, trying different settings and inputs, watching corresponding outputs, and making assumptions about general rules. The user may also take the machine apart, to apply the same method of pointing out outputs to inner parts for given inputs.

2.2 “Given enough eyeballs, all bugs are shallow”
The open-source mantra could also be applied to proofs management. As an example, a lot of offices used timestamp machines. A lead seal was there to certify that time was not altered, and, in the case it was broken, there was a check history to provide a \textit{terminus post quem} of falsifications. Another important feature for trust: a large clock. Although, timestamp machine did not need any clock to work, it was only there to be visible by anyone at anytime in the office. Coworkers, partners, customers and even mere visitors were able to detect a time offset, to notify it. Given this “social”, and “distributed” verification, everyone was able to trust the machine and its timestamping.

Our hypothesis is that the more different people (with competing interests) verify proofs (signatures, document history, etc.), and the more frequently they do, the more signatures will be trusted by people. This verification should be as easy as comparing the time machine clock to your own clock, it should be perceived quasi-preattentively. This contrasts with our observation that, currently, certification appears as being complex.

2.3 Identity: administrative statement vs interaction continuity
Most of the technical and organizational complexity of corporate digital signatures arises from certification: the hierarchical assessment of an \textit{idemity} link between the owner of the cryptographic keys used to sign and its administrative identity. It embodies the idea that “true identity” is indeed the firstname and surname assessed by on

hers country administration. Peer to peer alternatives (like “Web of Trust”) are not so different in their concept of identity: in “signing parties”, members show ID cards to each other.

Yet, a radical alternative exists: the one used by system administrators when connecting to a server (with SSH). Once the first interaction has been initiated (based on hints provided outside the system), \textit{identity} can be understood as being identical to the person involved in the former interaction. Identity would no more be about proper nouns but about pronouns. This latter approach of identity as a continuity in interaction may be more adequate to trust (or mistrust) between work partners. Therefore, the relevant identity appears as being a situated one, linked to collaboration practices like document sharing between people, whose joint action has allowed a given document to be cooperatively produced.
3. SOLUTIONS: VISUALISATION, INTERACTION, AND PROCESSES

Following examples are extracted from users tests on Lex4Lab software [5], intended to protect intellectual property among work partners documents. This qualitative study on two groups of target users was lead using a prototype. Whereas digital signature is used there mainly for trusted timestamping, solutions presented in this section could be also applied to generic digital signature.

3.1 “The game of cryptology’

The allusion to the book by Lewis Carroll (The Game of Logic) reminds us that there is not any domain – as complex as it may be – that cannot be grasped by newcomers in a playful way, provided that you propose an adequate visualization of the problem and interaction rules to solve it.

In most software (mail or web clients, readers, etc.), signature checking is visualized either as a green check mark (for positive result) or a red X mark (for negative ones). Nothing is provided to understand where the result comes from (apart from ‘cryptic’ data) and to compute the result by oneself. Moreover, because signing has legal consequences, the user is discouraged to play with her digital signature.

Because computations are too complex to be replayed by hand by the user, we let the user do only the last operation: an equality test on two very large numbers (hashes). By representing those two numbers by generated icons, the comparison can be done by the user’s preattentive perception (i.e. “in the glimpse of an eye”).

Moreover, when viewing the signature check, the user is invited to play a simulation of what would happen if a malicious person tried to falsify what was signed, or to sign it himself.

Technical elements shall be provided in an intelligible way, only when needed. Our study shows that a better designed interface can help users easily compare two elements, and help their understanding of what really matters in the digital signature, letting them try on the whole process (both signing and checking). The purpose behind this is to open up a little what appears to be a “black box”, so users would be encouraged to use it. Users effectively came to it, they sometimes act a “bad guy” role (a hacker who wants to falsify any signatures) and ask questions. The limit is we still are looking for a way to know the user behaviour on the length of an entire collaborative work project.

3.2 Recipients as witnesses

The same visual checking mechanism has been added to the history of the document. The idea is to use every recipient of the document as a witness of the validity of signatures and of the history integrity.