ALIS UNFORGEABLE ORIGINAL DOCUMENTS

ALIS is based on an electronic signature binding both the content of the document and the physical support it is written on.
Once signed, the content of the document cannot be modified, and a copy on a different support cannot be mistaken as an original.

Université catholique de Louvain
UCL

How it works ?

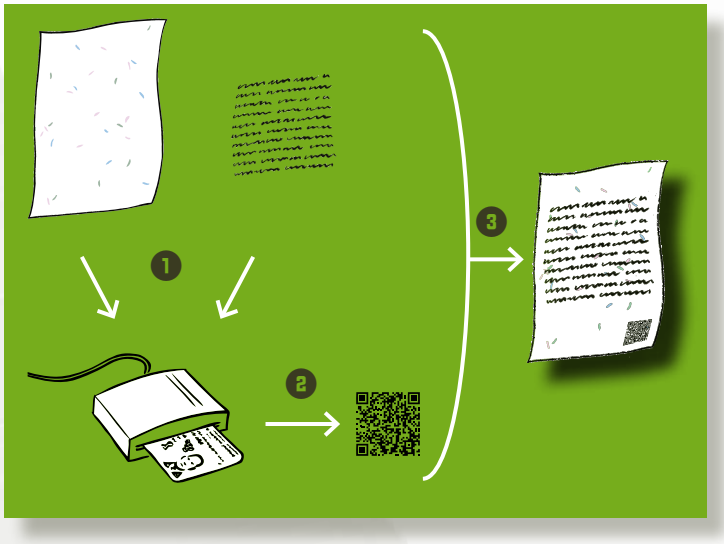
ALIS is based on the use of a secure support with inherent characteristics making it intrinsically unique. As an example, in the prototype we developed, UV-colored fibers are randomly distributed in paper sheet. However, any other intrinsic or extrinsic characteristic that is hard to reproduce could be used.

ALIS defines the concept of certified authors (e.g. a doctor, a notary, ...) entitled to generate authentic original documents. Each certified author possesses an electronic signature key, allowing anybody to verify the origin and authenticity of signed data.

GENERATING AN AUTHENTIC ORIGINAL DOCUMENT

To generate a new original document, the certified author performs the following steps :

1. a new secure paper sheet is scanned and a unique and robust identifier is extracted from it ;
2. the certified author then electronically signs both the robust identifier and the text he is going to print ; the signature is encoded as a 2-D barcode ;
3. the text and barcode are printed on the support.

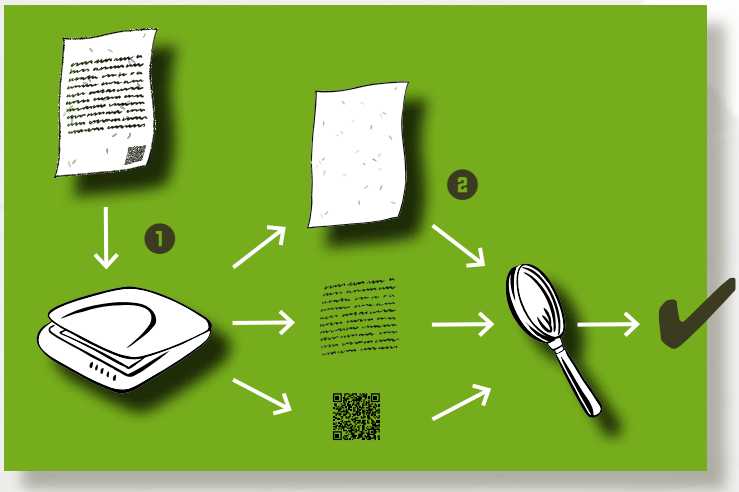


VERIFYING A DOCUMENT

Verifying the authenticity of a document goes as follows :

1. the document is scanned to retrieve its robust identifier, content and signature ;
2. the signature is verified with the certified author's public key.

This guarantees that the document is authentic, on its original support, and has not been tampered with.



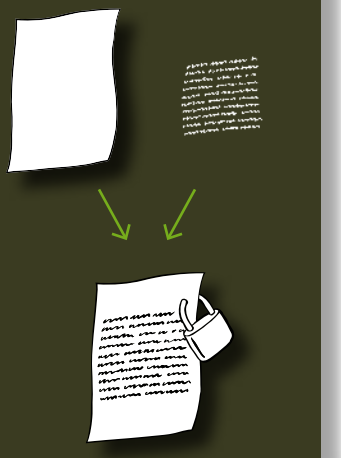
CONTEXT

Even though electronic data are omnipresent nowadays, there are many fields where physical documents are still required. This is especially the case when we need a document that is both :

- **unique** : the document cannot be duplicated without being noticed. A copy of a concert ticket, for example, is not the same as the original ticket.
- **authentic** : the content of the document cannot be modified unnoticeably. A patient should, for example, not be able to change the content of his drugs prescription.

AT A GLANCE...

ALIS allows producing authentic original documents using state of the art cryptographic and security technologies to guarantee unforgeability.



SECURITY

To forge a document, a pirate could try one of the following ways.

- Xerox an authentic document on a blank sheet. As this process will not be able to reproduce the inherent characteristics of the original support, the copy will not be considered as an original.
- Obtain secure paper and copy the text and signature on a new secure sheet. This would be detected by the verification process, as the signature depends on specific features of the original support.
- Modify the text on its original document. This, too, would be immediately betrayed by an incorrect signature.

Each document is unique and its content is certified.

ROBUSTNESS

For the solution to be effective, the system must be robust, i.e. :

- each sheet of paper is actually unique, and two different ones will never be deemed identical by the system ;
- the system is resistant to stains, folding... so that an original document will keep being recognized as such throughout its lifetime.

SOUND BASES

Our system is based on the use of physically unclonable functions (PUFs) and fuzzy extractors.

A PUF [2] is a function embodied in a physical structure that is easy to evaluate, but hard to characterize. In the secure paper context we used as a working example, checking the fibers position on a given sheet of paper is easy, but predicting (or forcing) such positions for a new sheet is presumably difficult. The security level can be tuned by adapting the number of characteristics taken into account and the granularity of the measurements, yielding the classical cost-security tradeoff.

To associate the same identifier to the same sheet of paper scanned multiple times, small variations must be discarded. This is achieved through the use of fuzzy extractors. Fuzzy extractors [3] allow reconstructing original information from noisy data, provided that the noisy data is sufficiently close to the original, without exposing the original if this is not the case.

PUFs allow obtaining an unique identifier characteristic of a given support, and fuzzy extractors allow obtaining it in a way resisting minor modifications.

APPLICATION FIELDS

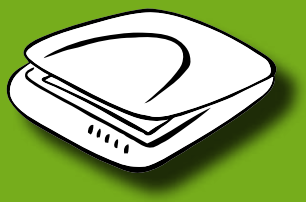
ALIS can be applied in any context where valuable documents are to be delivered in one single copy. This includes for example : doctor's prescriptions, event tickets, notarized documents, diplomas, ...

References

[1] P. Bulens, F.X. Standaert, J.-J. Quisquater, How to strongly link data and its medium : the paper case, to appear in IET Information Security
[2] R. Pappu, B. Recht, J. Taylor, N. Gershenfeld, Physical One-Way Functions Science, 20 September 2002: Vol. 297. no. 5589, pp. 2026 – 2030
[3] Dodis et al. Fuzzy Extractors : How to Generate Strong Keys from Biometrics and Other Noisy Data. Advances in Cryptology - Eurocrypt 2004, LNCS 3027, Springer-Verlag, 2004

What we developed

Thanks to Walloon Region funding, our research team developed:



- a prototype of modified scanner for UV scanning;
- a characterization of secure paper produced by Arjo Wiggins, yielding a robust identifier extraction method; our method can extract a robust 80-bit identifier from a paper sheet. This means for example that even if 10^{10} paper sheets (that is, thousands of tons of paper!) were randomly produced, the probability to have two sheets that would yield the same identifier would still be negligible;
- a full software prototype, simulating paper production, scanning, generation of drug delivery prescriptions and verification of the document validity, even after some alterations (stains...) of the support.

Partnership

We are looking for partners to undertake the production and exploitation of this new technology.

UCL Crypto Group, place du Levant, 3, 1348 Louvain-la-Neuve (+32) 10 47 81 41 uclcryptogroup@listes.uclouvain.be