# Token-based remote signing infrastucture

Degree programme: BSc in Computer Science | Orientation: IT-Security
Thesis advisor: Prof. Gerhard Hassenstein
Expert: Prof. Dr. Andreas Spichiger
Partenaire du projet: Tessaris AG, Maegenwil



As of today, the most common procedure to produce a qualified signature is to either plug a token directly in the computer or to use a remote signing service. The goal of this project is to develop a new middleware which would allow applications to access tokens remotely as if they were connected locally. The user would then benefit from the advantages of both local signing and remote signing.

## Electronic signatures

Electronic signatures are electronic data which are added to documents or e-mails, for example, for the purpose of authentication. An electronic signature guarantees the integrity of the document in a similar way to a seal. In other words: on the one hand, the recipient recognizes if the document or the e-mail has been changed after the signature or if the seal has been broken. On the other hand, the signatory is identified by the signature in a similar way to a stamp in the seal.
To produce an electronic signature, one needs a private key. Keeping that private key safe is one major issue when it comes to digital signatures. The safest way to store private keys are hardware devices, specially design to avoid any unwanted intrusion. Those hardware devices range from big Hardware Security Modules (HSM) to small smartcards.
Since there's many different device manufacturers, some APIs were made to make interactions with such devices easier through standardization. The most common is the PKCS#11 standard, developed by RSA Laboratories. Manufacturers usually provide those interfaces, allowing programmers to write generic code.

## Remote signing service

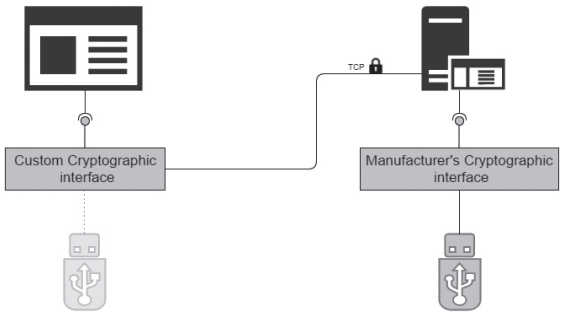
Remote signing services store the user's Token(s) in a safe environment within a certified Trustcenter, and execute operations on his behalf. But such solutions do not always scale well: they are indeed way too expensive for private users or small companies. Furthermore, remote signing services lack flexibility: the user sometimes has to interact with them through specific applications (web portals or proprietary software) and they do not always allow access to all the functionalities of a Token.

## Remote Token Server

An alternative to remote signing services is to plug the Token to a server located within the user's environment, rather than in a Trustcenter. This would allow for private users or small companies to have a remote access to their Token(s) while still having complete physical access to it. Applications will then interact with that remote token through some standardized cryptographic interface. In this way, the user would benefit from the advantages of having a remote signing service while still having the same functionality provided by a Token connected locally to the machine. The whole remote signing process is indeed totally transparent to the application using the remote token.

François Philippe Jean Jolidon
f.jolidon@gmail.com


SuisseID tokens were used to test the infrastructure.




Token-based remote signing basic architecture.