Trustworthy Remote Signing

Degree programme: BSc in Computer Science | Specialisation: IT Security
Thesis advisor: Prof. Gerhard Hassenstein, Prof. Dr. Annett Laube
Expert: Dr. Andreas Spichiger

With Remote Signing, users no longer hold on to the cryptographic keys themselves, instead a remote service generates keys in their name. This has a serious drawback: the signing service is able to sign arbitrary documents without the user‘s consent. In this thesis, we provide a specification as well as a proof-of-concept of a Remote Signing Service that does not require the user to trust it unconditionally.

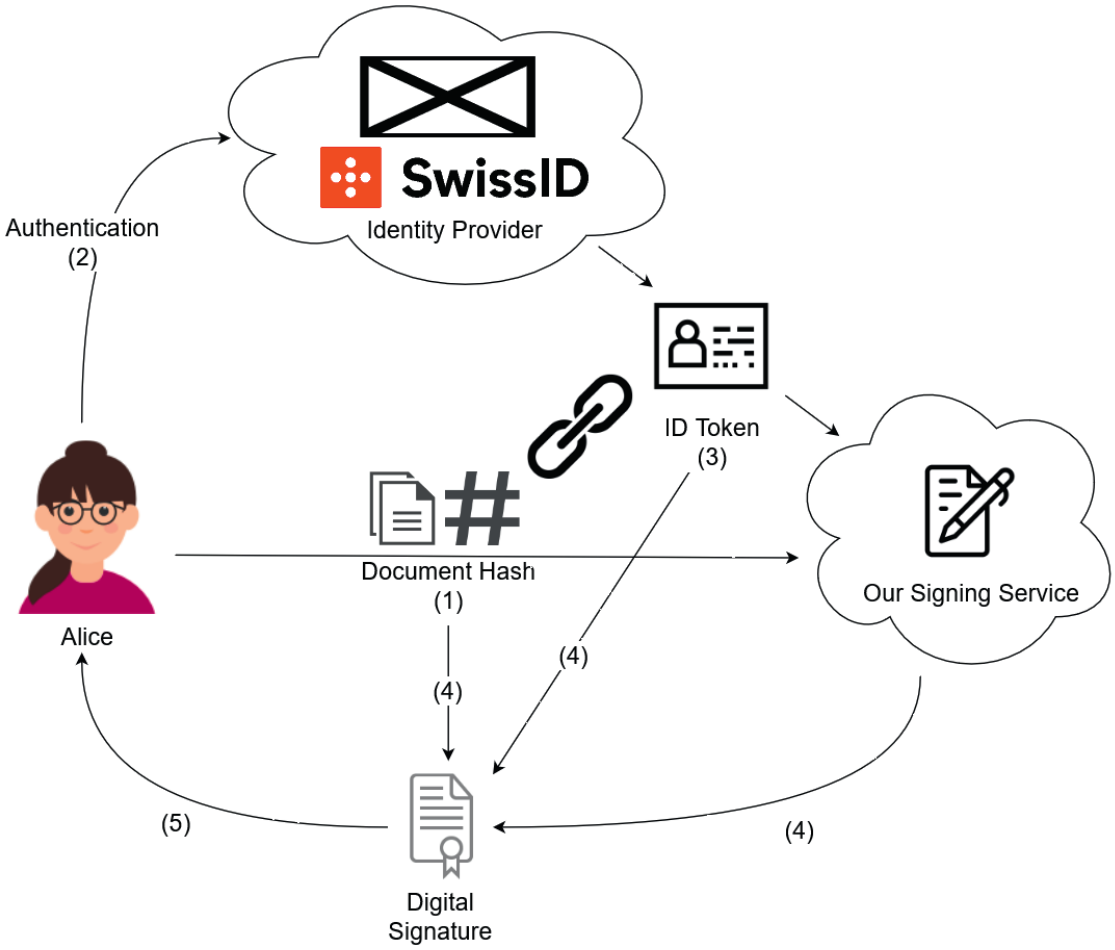
Remote Signing Services

Such services allow people to create digital signatures, no matter where they are, what device they are using, and without the need for them to carry their keys with them. However, since these services are in control of the user's private key, they are able to sign any document they want without the user's consent or knowledge. These are legally binding signatures in the user's name, recognised in a court of law.

Our Solution

In our solution, the signing service alone cannot sign a document, despite possessing of the user's private key. We accomplish this by distributing the trust between the identity provider and the signing service, and by cryptographically linking the intent of the user to sign specific documents, the authentication for that intent, and the signature created by the signing service.

Patrick Hirt



Signing Process

Gabor Björn Tanz