



CRYPTOMATHIC AND SWISSIGN PARTNER TO DELIVER CENTRAL SIGNING TECHNOLOGY TO THE BANKING INDUSTRY

Cryptomathic, a pioneer in central signing and WYSIWYS technology, partner with SwissSign, an industry acknowledged CSP, to deliver a unique signing experience to retail banking users.

Achieve the business' digital strategy with central electronic signature services

Being able to provide trust and convenience is critical in electronic banking. As part of your digitalisation strategy, what if you could digitalise the last step of digital journey during which the end-user provides his legally binding consent to the documents presented over the portal? What if the signing experience could be made without breaking the browsing experience from any device at any time whilst at the same time featuring non repudiation and leveraging your existing authentication technology?

This is exactly what the partnership is about, namely the possibility to offer advanced or qualified electronic signature using zero footprint central signing technology featuring strong WYSIWYS (What You See Is What You Sign). The Cryptomathic Signer technology combined with SwissSign certificates renders a unique signing experience which leverages your strong authentication techniques.

The technology offers great advantages

- Enable advanced or qualified electronic signatures as revised EU directive on electronic signature (eIDAS) and the Swiss Federal Act ZertES

- Offer a unique signing experience for all banking channels incl. web portals, desktop applications, mobile platforms
- Make PKI transparent for the end-user
- Leverage existing 2-factor authentication (2FA) deployment
- Offer non repudiation
- Reduce operational costs

Remote central signing

The best way to deliver electronic signatures across different channels is to use central signing technology. It integrates smoothly with web banking and does not require user software installation, plug in or additional components, and can be used anywhere at any time from any device with web browsing capacity. It also makes PKI transparent to the end user. Once registered and enrolled, he simply signs what he sees using his legacy authentication token. The signed document is then rendered for visualisation and the document can be downloaded by the user and archived by the bank.



eIDAS and ZertES

The EU regulation No 910/2014 has set a legal and standardisation framework for the provisioning of advanced and qualified electronic signatures in EU member states and also in Switzerland. The solution complies strictly against TS 419 241:2014 Sole Control Level 2, SR 943.03 ZertES and other relevant industry standards.

The solution is integrated with SwissSign swissnet services and also works with the managed PKI services.

As such, SwissSign can also delegate the RA process to the bank as per Art. 8 Abs. 4 ZertES (Delegation of the identification to third party).



Non-repudiation

Non-repudiation is critical to build and maintain trust and security for e commerce services. Even though the PKI infrastructure may be transparent to the user, a key pair and a certificate are still generated on his behalf upon trustworthy and duly controlled identification by a registration authority.

When a signing operation is made, Signer keeps secure usage logs centrally and features strong WYSIWYS functionality. These logs, combined with audited security protocols, demonstrate that the user actually retains control over the signing process and provide convincing evidence before court of the authenticity of the signature on a document or transaction.

Leverage 2-factor authentication

Banks already rely on 2-factor authentication to secure user access to the ebanking portal. Most users are already equipped with hard or soft tokens generating one time passwords, or use SMS based OTPs or a challenge/response solution. These techniques help to ensure that the user is actually present during the session but it does not safeguard against man in the middle attacks nor does it provide legal binding consent or non-repudiation. Signer can remedy this and builds on existing 2FA methods to strengthen the customer experience with trustworthy digital signatures.

What You See Is What You Sign (WYSIWYS)

The signature is the step of a process where a user commits to a transaction of document. It is of utmost importance that this process is secure, and inspires trust and confidence. Technically this is achieved by delivering what Cryptomathic's founder coined in the term "What You See Is What You Sign" (WYSIWYS). This also renders the signature to the user so that they can visually observe what they have applied their consent to. Cryptomathic Signer features an optional WYSIWYS module where the data to be signed is received as input, and Signer produces the signed document after having presented it to the user over a trusted viewer using your custom branding.



ABOUT CRYPTOMATHIC AND THE SIGNER

Cryptomathic is one of the world's leading providers of security software solutions to businesses across a wide range of industry sectors, including banking, government, technology, cloud and mobile.

Cryptomathic is the world's most experienced player in central signing and WYSIWYS. We have invented and engineered the concepts fully in

our labs. Our internationally acclaimed experts are a sounding voice in the standardisation committees and we are proud of being the technology providers of many nation-wide central signing deployments and are very active in the banking industry, enabling eBanking portals with digital signature technology.

[Learn more at cryptomathic.com](https://cryptomathic.com)

ABOUT SWISSIGN AND CERTIFICATE PROVISIONING

SwissSign, a subsidiary of Swiss Post, protects and accelerates your business processes with simple solutions for unique identification, digital signatures and secure communication.

SwissSign AG is authorized and able to issue qualified electronic certificates, which correspond with Swiss law (the Swiss Electronic

Signature Act or ZertES) and the European Telecommunications Standards Institute (ETSI). The Swiss Federal Act on Electronic Signatures, ZertES, officially took effect on 1 January 2005 and enabled the secure, provable, and legally valid development of electronic business transactions as well as electronic document archiving.

[Learn more at swissign.com](https://swissign.com)