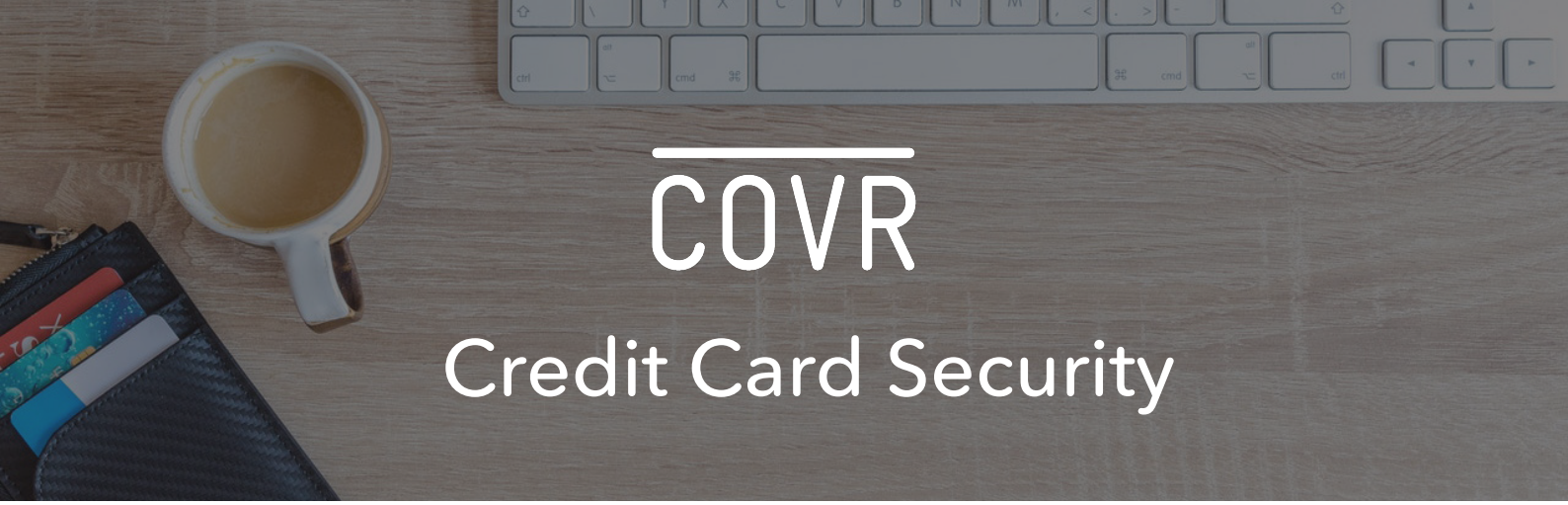


COVR

Credit Card Security

User-controlled security for credit card companies

When automated fraud detection systems detect potentially fraudulent activities, they often reject credit card transactions or freeze accounts. In many cases, these alarms are triggered by unfamiliar, but harmless actions made by the credit cardholders themselves.

When a bank denies payments, it's a complicated procedure to convince the bank to re-approve the transaction that involves phone calls to the credit card issuer, security questions, and passport verifications, or other payment methods like cash/another credit card.

Enterprises and e-commerce companies could lose revenue due to automation technologies and technical details, as false alarms prevent people and companies from completing payments. AI and Machine Learning is not the answer to everything!

Seamless transactions and trusted purchases

With COVR, a credit card holder can authorize the transaction directly, which eliminates the problem with payment rejection and false-positive denials.

The users are bound to their smartphone with COVR's true out-of-band and powerful encryption technologies that lock the user's identity to their device, guaranteeing the authenticity of the user/transaction.

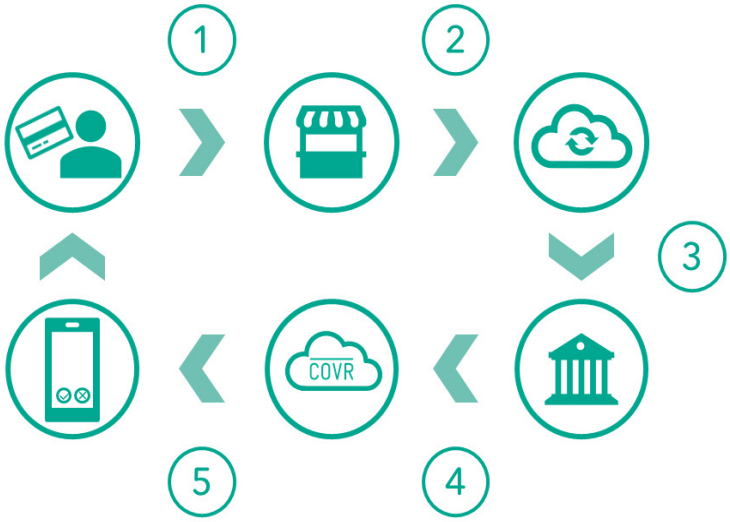
Every smartphone can be reached by the bank in seconds, anywhere in the world. It is also registered to send authorization request push notifications with a response time of a couple of seconds. The result: seamless card transactions, and fully trusted, accepted purchases - both by the bank and its customers!

COVR's convenient setup

COVR, built on strong asymmetric (public-key) cryptography, which ties the smartphone to a credit card holder in a very secure way. This tie is tough to trespass, and any changes in the payment information are detected right away.

Besides the direct out-of-band communication channel, COVR also provides proof that the data is authentic to a degree where it can't be questioned (non-repudiation) for all communication, sent between the bank and the credit card holder.

The user can also benefit from smart remote facial recognition to amplify protection and is also able to recover their account in case their smartphone is stolen or lost.



1.The credit card holder presents the card to a POS in the store.

2.POS in store contacts the credit card network for approval.

3.The credit card network contacts the issuing bank

4.The issuing bank requests the credit card holder's approval via COVR

5.The credit card holder approves the payment on their smartphone

Covr Security - enabling trusted identities for people, services, and things.

Covr Security provides mobile, multi-factor authentication-as-a-service to a wide range of industries that depend on strong customer authentication: banks, payment networks, credit card companies, eID providers, IoT companies and mobile carriers. Our user-friendly solution is built on a modern, patent-pending architecture originating from Nordic bank security.

Available as a native mobile app ready for a quick roll-out, and as a powerful SDK for trouble-free, white-label integration into existing mobile applications.

COVR

Nordenskiöldsgatan 24
211 19 Malmö Sweden

+46 (0)40 -654 06 46

covrsecurity.com
info@covrsecurity.com

Get in touch

We are ready to provide advice to any business in need of secure authentication. Contact our expert team and find out how you can secure your business with Covr Security today.

sales@covrsecurity.com