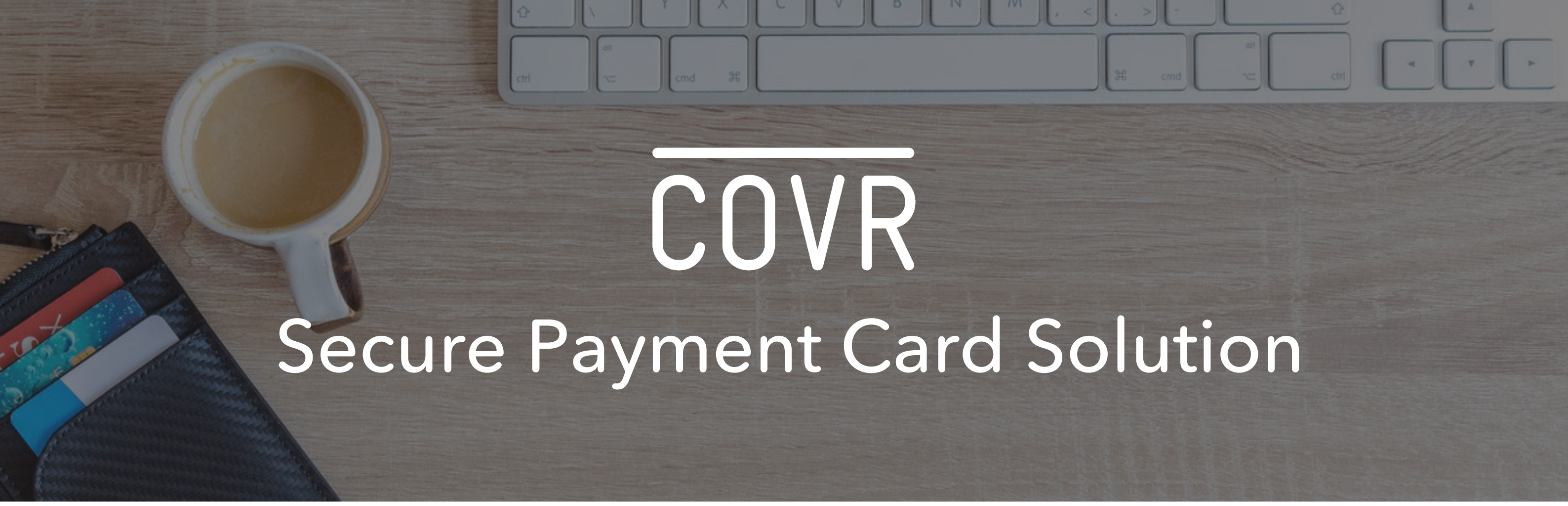


COVR

Secure Payment Card Solution

User-controlled security for payment card issuers

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

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

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

Seamless transactions and trusted purchases

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

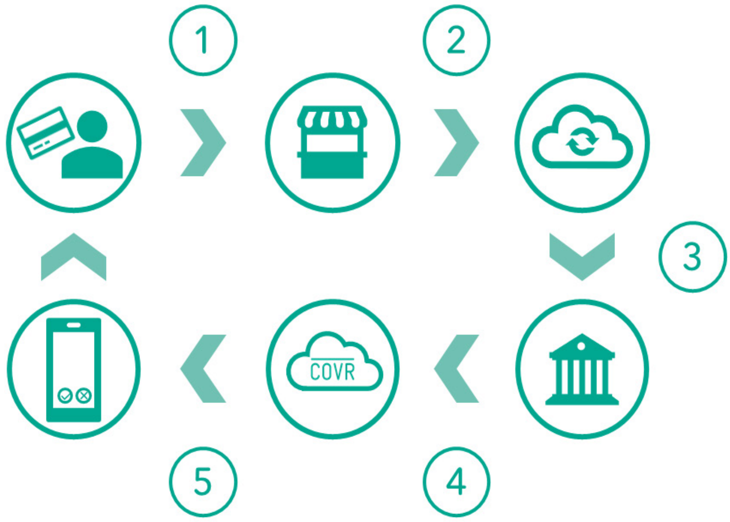
Every smartphone can be reached by the bank in seconds, anywhere in the world. It is also registered to send authorization request push notifications with a response time of a couple of seconds. The result: seamless, authorized transactions trusted by both the issuer, merchants and customers!

COVR's convenient setup

COVR is built on strong asymmetric (public-key) cryptography, which ties the smartphone to a card holder in a very secure way. This multi-layered approach is virtually impossible 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 issuer and the 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 card holder presents the card to merchant checkout

2. The merchant submits the transaction for authorization

3.The issuer receives the transaction request for authorization

4.The issuer requests authorization from the card holder via COVR

5.The card holder receives a notification and authorizes the payment

COVR - enabling trusted identities for people, services, and things

Covr Security provides mobile, multi-factor authentication in the cloud to a wide range of industries that depend on strong customer authentication: banks and payment providers, eID providers, public services, and health care providers. Our three-layered authentication solution is truly customer-friendly and built on modern, patent-pending encryption technology.

COVR is 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
info@covrsecurity.com

covrsecurity.com

Get in touch!

We are ready to provide advice on how to achieve optimal customer experience and secure authentication. Contact our expert team and find out how you can secure your business with Covr Security today.
sales@covrsecurity.com

Available on the App Store

GET IT ON Google Play