COVR

WHITE PAPER

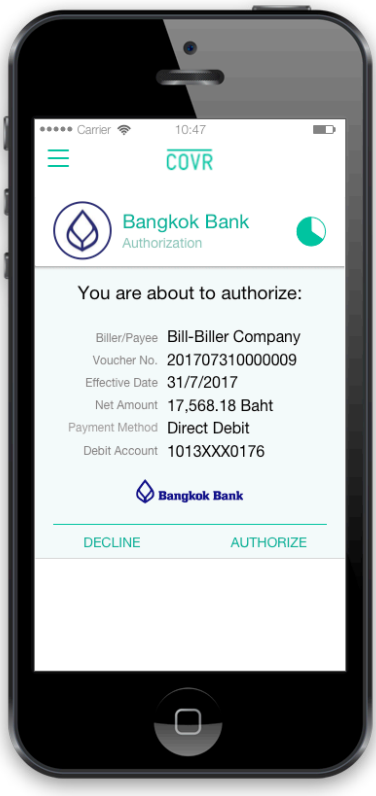
Table of contents

A Better Deal - Customer Choice and Security in Financial Services

For decades, we have relied on password security to make sure that our data is, at least to some extent, protected. But the traditional methods of using passwords to access everything from internet bank accounts to online-shopping websites is no longer enough. Every hour of every day, there is a bombardment of malicious attempts to steal digitized personal credentials. Luckily, there is a solution: Covr.

Covr is a true user-centric mobile security management platform developed with online, mobile banking and digital payments in mind. It is developed to solve the enigma of user authentication contra user experience, without any need for complicated and expensive hardware installations.

However, Covr is not just another authentication system. The beauty of Covr is that it gives the endusers themselves full control over their remote bank, credit card transactions and digital identity while it provides maximum security on all levels, throughout the whole transaction. As a matter of fact, Covr eliminates the need for passwords altogether.



From closed to open - the immediate future of traditional banking

As more and more transactions take place on mobile devices, customers start taking safe, personalized and real-time payment experiences for granted. Until now, banks have occupied a very privileged space – traditionally the only way for customers to access their bank accounts has been via the services that are provided by their banks. However, this is about to change. The realization of the Second Payment Services Directive (PSD2) will force financial service providers, primarily banks, to re-invent themselves – and fast.

Open banking - a radical security shake-up

PSD2 is meant to encourage innovation and competition between European financial service providers, but more importantly, to augment online payment security, user control and account access. In practice, it means that banks have to grant thirdparty providers (TPPs) access to a customer's payment services or online account. As a result, non-banking players like social media networks, telecom operators and a variety of other enterprises are now able to provide the same services as banks do.

Banks can claim a stake - new value creation

PSD2 has a big impact on traditional bank's payments revenues and customer ownership as it levels the playing field for market entry of new third-party services that will more or less dilute the whole payments ecosystem. Banks now have a clear choice of direction; either wait and see what is going to happen and jeopardize their position, or claim pieces of the pie and use PSD2 as an innovation trampoline.

Covr is different from other security solutions

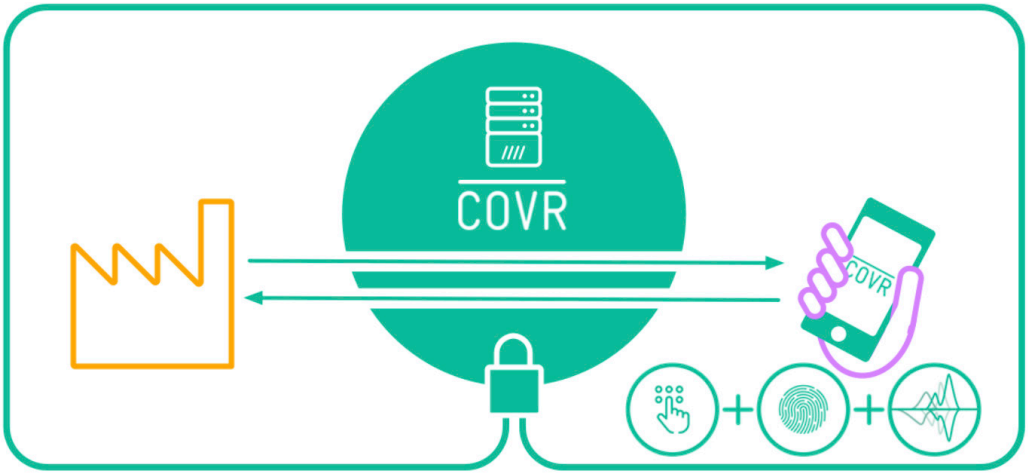
Strong Customer Authentication (SCA)
One of the immediate issues of the deregulation of the bank monopolies is that credentials are open targets for cybercriminals logging in to third-party websites. Covr eliminates that threat altogether using a combination of so-called two-channel, Out-of- Band separation, several layers of encryption and identification to diminish any conceivable threat.

This means that customers can move money or data over a secure communication channel – even when using an open, unknown or public Wi-Fi connection. Two-factor authentication is a (pretty well known) method to determine if a user is who they claim to be by using two different pieces of information. It can be a combination of any two of the following three:

- Something you know, like a password, pin or passphrase
- Something you have, like a smartphone, chip enabled bank card or token
- Something you are, like the iris, fingerprints or voice recognition

The uniqueness Covr is that it doesn't require hardware it it's extremely cost-efficient in comparison, weighing in the security gains contra the integration and maintenance costs. Covr is easy to install, user intuitive, has flexible customer adaptation and a low per-user cost.

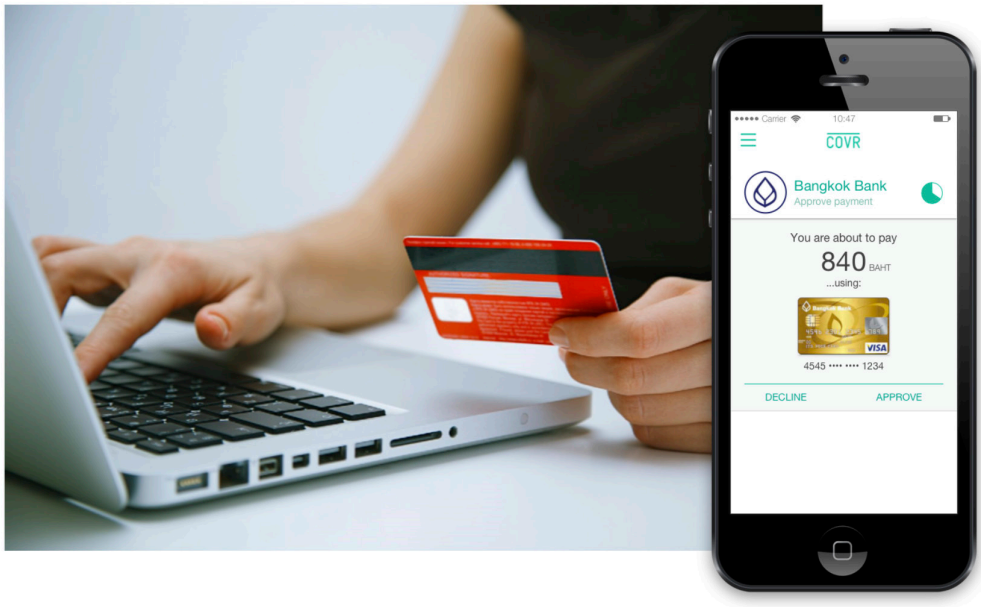
With Covr your customers are in total control with a 6-digit access code and biometrics instead of complicated passwords. Covr uses true out-of-band, three-factor strong custo- mer authentication (SCA) with a secure second channel between the user's mobile device and your service.



The balance of security and convenience for online retailers

Although strong customer authentication definitely lowers the likelihood of fraud, it can also have a negative effect on customers' online checkout experiences as it adds an extra step in the payment process. For online retailers, this can be a serious conversion problem. If the payment process is not transparent enough and provide a great user experience, consumers will - without a doubt - abandon an online shop and jump to the next one without further hesitation.

To sidestep this dilemma Covr's unique solution makes a SCA-compliant checkout flow extraordinary user-friendly because it only intervenes when it detects a suspicious activity.



The Covr real-time protection guarantee

We've established that there is a huge risk of fraud every time people access their online banks or carry out digital payments, no matter how well protected the system may be. So, it goes without saying that sensitive banking and payment applications must be 100 % protected against these attacks and this is where Covr comes into play.

Personal finance management

What really separates Covr from any other security solution is that it works in real-time. It gives the user full power to manage their own protection and there is no need to rely on the bank or the credit card issuer to fix the problem after the fact. What happens with Covr in place is that the user is notified and will get a request to authenticate herself whenever a suspicious action with sensitive and valuable information is underway. As a result, the user is prevented from being tricked into providing sensitive data like credit card numbers and passwords. To put it simply, the ownership of personal data will be returned into the hands of the consumer.

Summarizing the offer to our customers

What really differentiates Covr is the decentralized system architecture that certifies a strong connection at all times. Because the client side is operated entirely by software, the end-user is exempted from having to handle special hardware.

This is a brief summary of the benefits of Covr:

- Covr's reliable security channel for two-way communication is created between you and each user and, as a side effect, prevents less secure access points like password-based credential interfaces
- The transactional method of identity handshakes enables immediate intervention in any situation where sensitive resources are handled
- The integration is scalable and often a one-time step task
- Rollout doesn't need manual system administration
- The user registration process is tailored to be lightweight is handled entirely by the user
- The essential ambition of the Covr system is not necessarily to protect entry points, but rather to minimize their existence

Finally, people will continue to give their banking platform permission to swop to the best solution without having to make an active decision, and they will take for granted that their credentials are totally safe and protected.

Covr comes fully prepared and has all the requirements for this new reality.

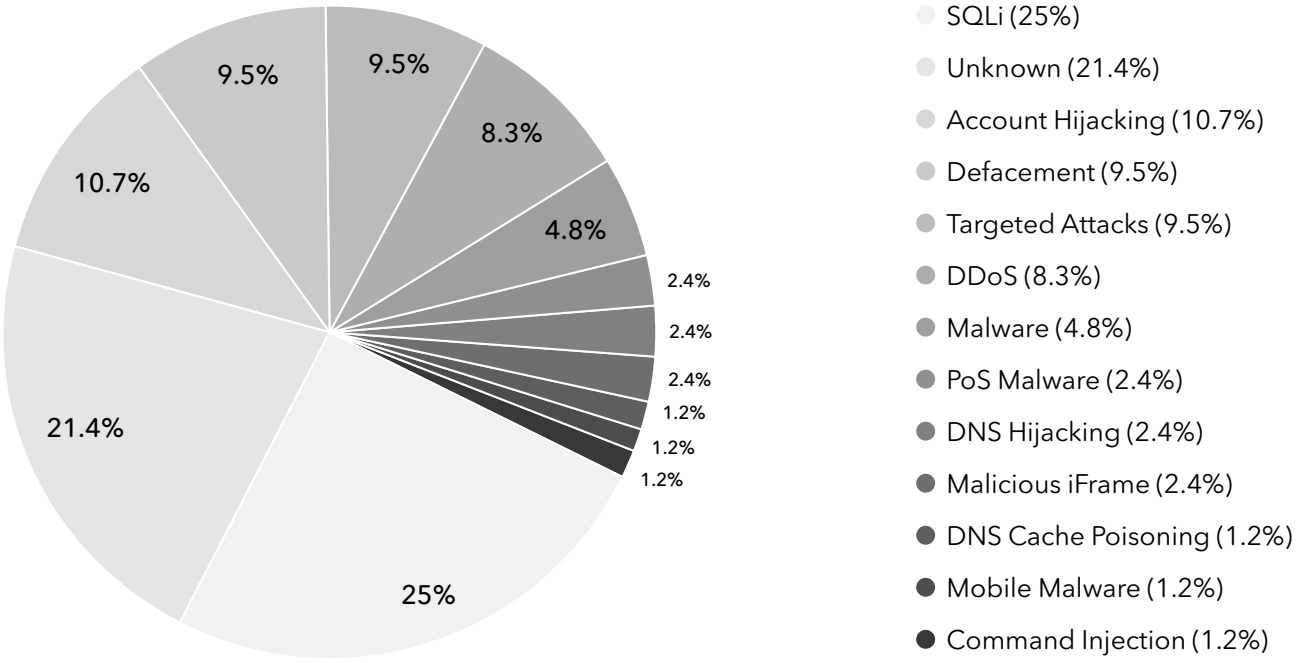
New Security Threats

Today's bank robbers are armed with computers, not guns. The goal of an attack is to steal personal information, like login credentials, account details and credit card numbers. Credentials are the holy grail for hackers and there are hundreds of millions of passwords and user-names traded on black markets.

The latest developments in hacking weapons have made them easier to use and more available to an ever-increasing number of Internet users.

To make matters even worse, hackers and their attacks become more sophisticated and when detected, cybercriminals can easily duck and rebuild their cyber-attack strategy.

Attack techniques[1] February 2015



Common threats include phishing emails and websites looking to steal credentials (username and password).

Man in the middle (MITM) attacks

Many hacking attempts happen in the form of a so called man in the middle (MITM) attack. A man in the middle attack is when a trespasser injects himself into a "conversation" between a user and an application, either to spy or to mimic one of the parties, making it look as if a normal exchange of information is going on. This type of attack is relatively easy to stage for an attacker, by using proxy devices like Wi-Fi routers, hubs and switches that essentially routes communication to a rogue service.

Man in the middle attacks are difficult to protect against and very hard for the ordinary end user to spot. Technologies like DNSSEC give some protection but is not broadly used yet. Though intrusion Detection Systems (IDS) are becoming more advanced, they will do nothing if the attack is launched outside the IDS protected environment.

Gone phishing

Another common way hackers use to steal password protected information is by phishing attacks. During a phishing attack, specific tools are used to include links in fake emails that asks the recipient to reset a password. The link leads to a website that at first glance looks legitimate. When the recipients click on the link and unsuspectingly types their passwords into the sketchy site, the hacker has it.

According to Symantec one in 131 emails contained malware in 2017, which is the highest rate in five years. The only method to counter this kind of malicious attacks is to remove the need for passwords altogether, which is what Covr does.

A multi-factor authentication system needs to be easy to install, tangible, intuitive for any user, flexible for customer adaptation and have a low per-user cost.

Covr overview

Covr uses:
– PKI, Public Key Infrastructure
– Encrypted channel - 2048 Bit
– Checksum to see if someone tampered with the information
– Automatic RSA between security server and device
– Application in phone to marry with hardware

In today's dynamic market, where electronic transactions are constantly taking place, there is a need for a system that ensures the security of each individual transaction and in which both sender and receiver can recognize that the transaction is requested and approved. The cryptography technology of today grants some of the requested functionality based on asymmetric cryptography. However, this technology only enables verification of the sender and only the intended recipient can read the transaction. Covr includes the use of PKI and other technologies to create a complete end-to-end authorization and authentication solution.

Covr offers both security and usability, giving end users control over their transactions and their identity in a way that enhances the perceived as well as the real security level when, for example, engaging in electronic commerce.

Similar efforts and implementations have been made with Kerberos, PKI, security devices, one-time passwords, etc. However, all of these technologies have weaknesses and because they have historically been technology-driven, they also lack usability.

Covr lets users authorize transactions themselves by using PKI technologies together with a messaging system to receive the request for authorization. The PKI systems that are used are compatible with all digital private keys and public certificates, the new identity cards used in the Baltic region, standard online certificates, etc.

By using the new automatic RSA algorithm we never send any information over the Internet. The device will know what's going on automatically. This patent-pending solution can be used for any highly secure channel between any devices. We use it from security server to phone and it is coming in a desktop version.

By using PKI as a base, the product's infrastructure is "future proof". All types of transactions and logins can be authorized in real time with the product. The advantages for the organization implementing the solution are decreased costs and increased security. To minimize the technical risks, Covr uses proven technology. Users benefit from a user-friendly and legible security model that is easy to comprehend.

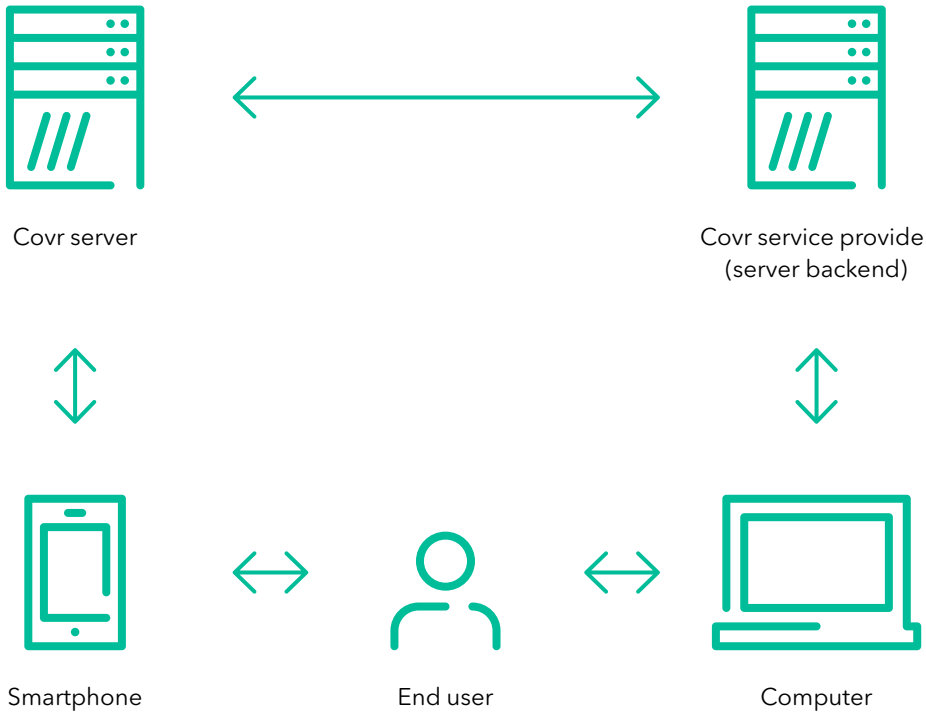
The authorization process is as simple as using the cell phone to answer an authorization request. One of the big advantages with Covr is that the user is not only authenticated, but is also able to grant or reject transactions and logins. This also makes it easy to implement scenarios where multiple persons are required to grant access or allow a given transaction. A big advantage for users is that they no longer have to trust the back-end system's auditing, but can and must audit and authorize their transactions themselves.

Technical overview

The Covr system uses a method of authentication where multiple channels and several factors of identification are used as a foundation for security.

In ”traditional” network security data/information is transported over the same channel on which security techniques are used to authenticate an established identity. In such a system, any potential perpetrator that can compromise and neutralize security measures, will also have access to sensitive data within the same communication channel.

The below picture depicts a typical Covr setup

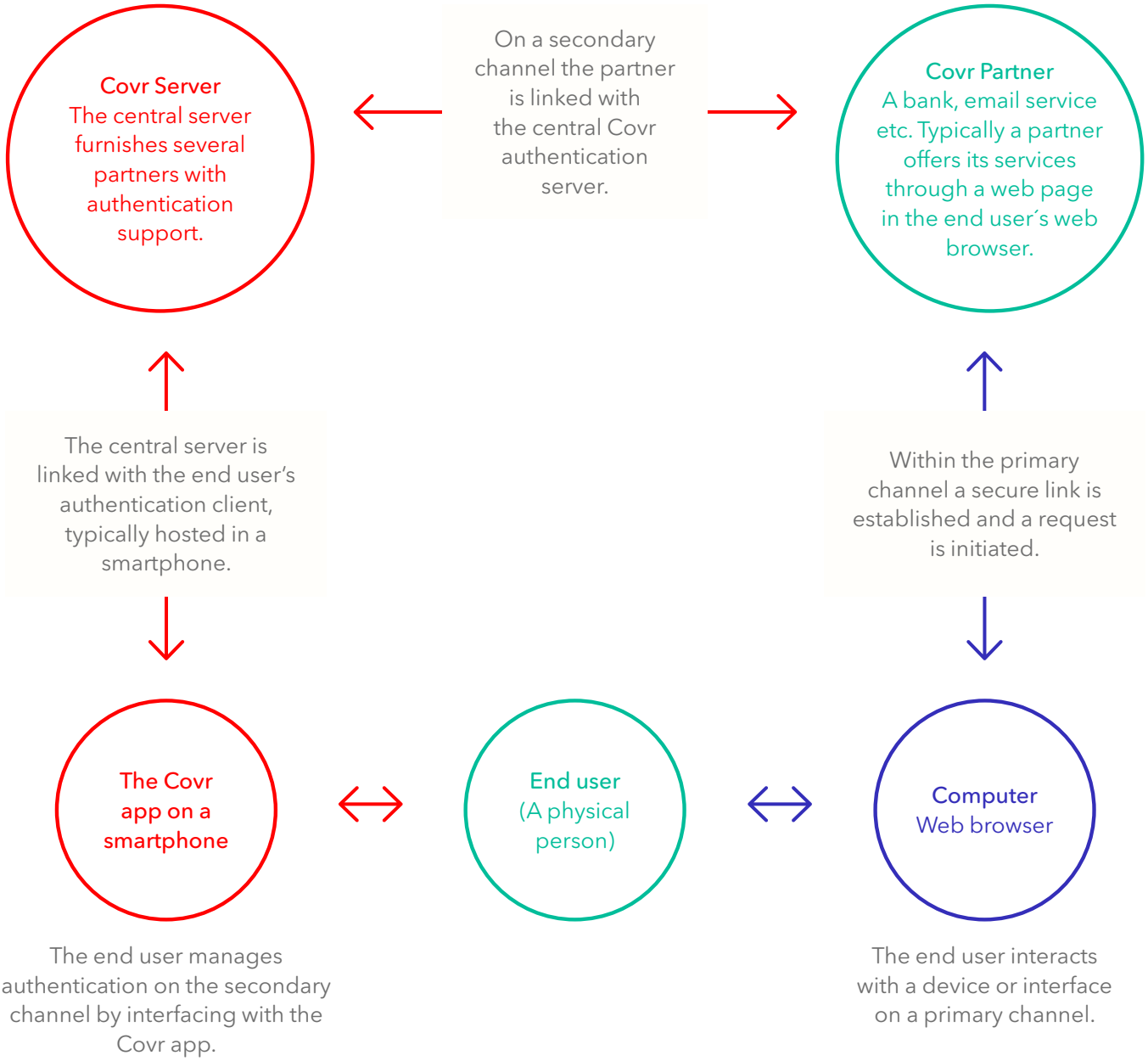


The main players in this setup are the end user and the Covr partner (e.g. a bank/email service/cloud provider/hospital/ gaming site, etc.). As will be shown in more detail on next page, these two players are in contact over two channels for the purpose of ensuring that they both are who they claim to be.

Detailed schematic breakdown

The components of the Covr system are linked in a communication process with several steps and rules.

- Primary communication channel
- Secondary communication channel
- Entitles communication with both channels



Process description

For an arbitrary authentication session, a sequence of steps are carried out between each component, as seen in the following diagram with descriptions below.

1. (primary channel) - The end user attempts to perform an action like transferring money from an account, logging into an email service, verifying his or her identity with an authority, etc. The party requiring this authentication is defined in the system as the partner. This is essentially a Covr customer which provides Covr's services to their end users.

2. (primary channel) - In the case of a bank, the user prepares a monetary transaction via the bank's web page, which is displayed in the web browser. The user then submits the request, knowing that a Covr verification will occur. This step is what happens upon submitting the request. The web browser issues the request over a secured network channel (HTTPS) to the bank's server.

3. (secondary channel) - The partner contacts Covr's central server and requests authentication of the end user. Along with the request it sends its own ID (which was stored earlier in the Covr database), the end user's ID (which is known to Covr by user registration). The partner also passes along a prompt message which is to be presented to the end user through the secondary channel (e.g. displayed on the mobile device).

4. (secondary channel) - The central server verifies the ID of the partner (the partner must have previously registered with Covr). The central server already has the user's ID and unique identification of the end user's client hardware from when the end user previously registered with Covr.

The Covr server generates a unique key from the current timestamp (i.e. the time when the server received the request) and the unique identification data. Currently this unique data is the IMEI number of the end user's mobile device, which is unique to every device ever produced. The key is hashed using MD5 and SHA1 algorithms.

5. (secondary channel) - The Covr server contacts the Covr app, which is typically located on the end user's smart phone (but could also be any secondary device). It requests authentication from the app software, and passes along the timestamp mentioned in step 4. It also passes along the prompt message originally issued by the partner to be shown to the end user.

6. (secondary channel) - The Covr app prompts the user to verify identity by requesting a pin code.
If identification is successful it now generates its own key (which the Covr server also did in step 4), based on the timestamp received from the server and its own IMEI number.

7. (secondary channel) - The Covr app contacts the server to verify its authenticity. It passes along the key/id information.

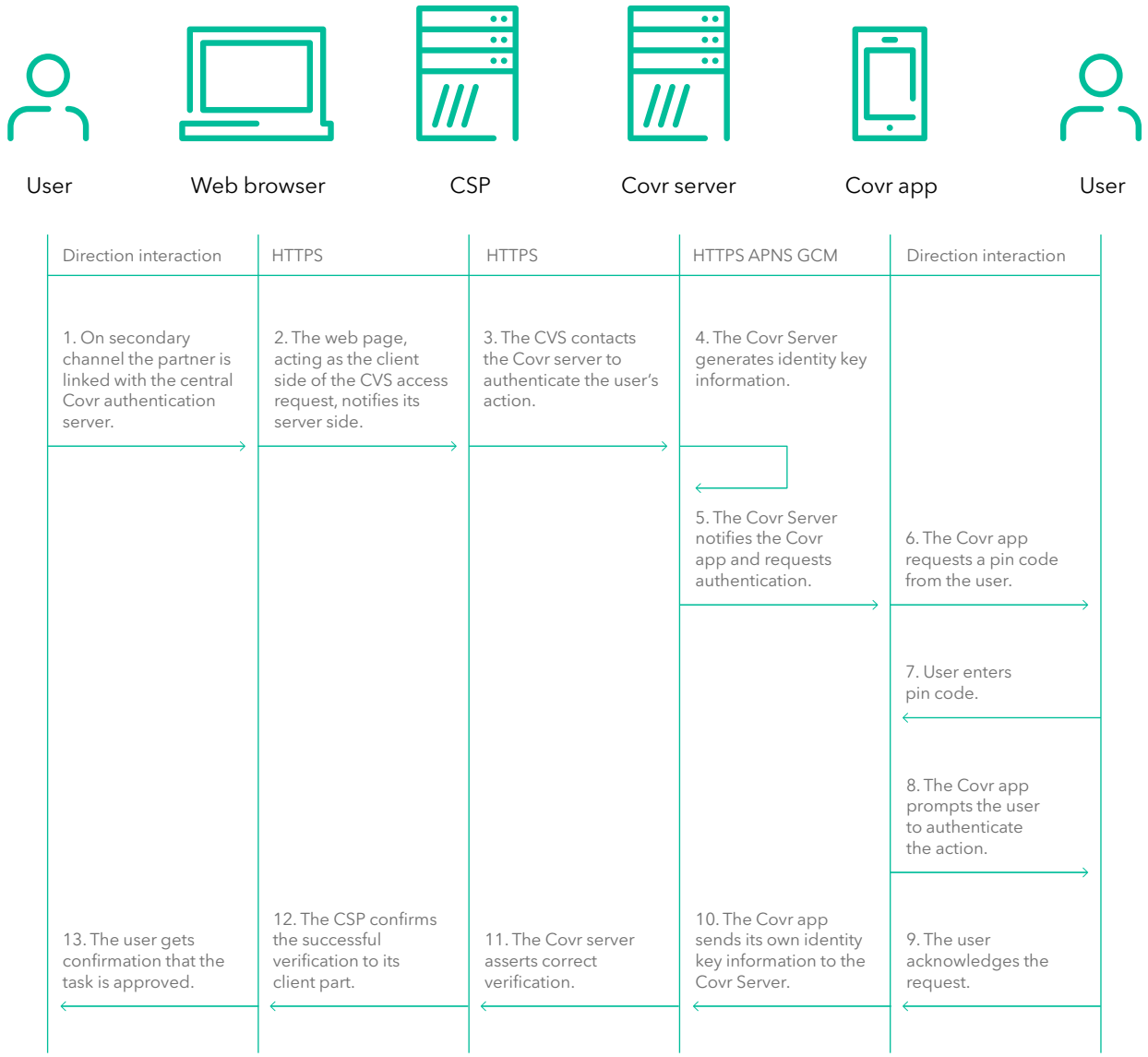
8. (secondary channel) - The server makes sure the keys that it generates match the client's, and then responds to the partner, notifying it of the result.

9. (primary channel) - The partner responds, either granting or denying the client part permission to perform the requested action.

10. (primary channel) - The user is given (typically) visual confirmation of either successful or failed authentication.

Process description

The below picture depicts the process



The authentication process

The below picture depicts the authentication process

Secure and gating identification handshake
The system verifies the identity of the end user separately and prior to sending anything or committing to a transaction. No data in any form is handled until an identity handshake has been concluded.

Data which is known solely to the Covr system and the user's app environment is used together with time stamping to generate key information which references the correct user and the time of the authentication session. Only the time information part of this encrypted key is then passed over the communication link.

Both parties can in this manner generate identical keys for the handshake, and the time information enables the system to create a limited window of exposure, within the key itself, before the handshake expires and indefinitely renders the key useless.

In a sense, this method resembles the PKI model of sending partial keys over a communication link. However, in this case the public fragments passed over the network are significantly less sensitive and useless for e.g. staging a MITM attack, even without any form of certificate support system.

Underlying PKI
Even though the system utilizes proprietary methods of secure transfer and identification, the underlying data transport is also secured by traditional PKI measures.

Communication Protocols

Infrastructure
1. Server-side API
2. Back office administration console
3. Mobile clients for iOS and Android
4. Partner plugins via JavaScript integration

Communication channels for data
1. Between mobile clients and API
2. Between Back Office frontend and API
3. Between partner web plug-in and API

API Security
The API security mechanism is based on a standard session-based security mechanism and Java security mechanism. It has the following components:

1. Single entry point for authentication and authorization. It is "post/auth," which requires different parameters for different system roles (see below). This method should be required for unauthorized users to enter the system.

2. Session-based API methods after entering via "post/auth" we receive the user's roles and store them in the user session. Therefore all other requests should be done within this session, otherwise it is considered an unauthorized request and it will be rejected. We consider a user session expired after 15 mins.

3. Role-based access control model on services: we have different services and methods for each role, which are always checked before running methods of services.

4. Ownership-checking mechanism: This forbids access to data of other users. For example, the end user only has access to his/her requests, partners, configuration, etc., and cannot obtain information from other end users. Admin, however, has access to all system data.

Unique Identification
Covr's unique proprietary algorithm is comprised of seven input parameters which generate a unique ID for the user and his/her mobile device.

Communication between mobile clients and API
Mobile clients are used by end users for interacting with Covr's system. These clients only interact with our API model. They receive/accept and transmit the authorization of requests.

Covr's API is the communication mechanism for mobile clients and it uses API security principles, which are described above. Authentication and authorization for end users (mobile clients) is based on a consumer key, which is generated on the device.

Mobile clients use two additional communication channels:
1. End users authenticate their phone numbers and link to partners using SMS. The SMS that Covr sends to the end user contains a PIN code. This code expires in five minutes if it is not used.

2. Push notifications are used for accepting or rejecting authorization requests. Covr sends different types of messages and requests the ID. The data sent does not contain any information about the specifics of the request (name of action, description, partner, etc.). This data will be sent to the mobile client via API after successful authorization.

Communication between a mobile device and our API is only permitted after a user enters their 6-digit PIN code or use their devices Touch-ID to gain access to the mobile app.

Areas of application

Below is a small selection of application areas for the Covr Security system.

Transaction security
The transaction of resources such as money transfers are effectively secured by Covr. The correct owner of a resource is always instantly asked for verification.

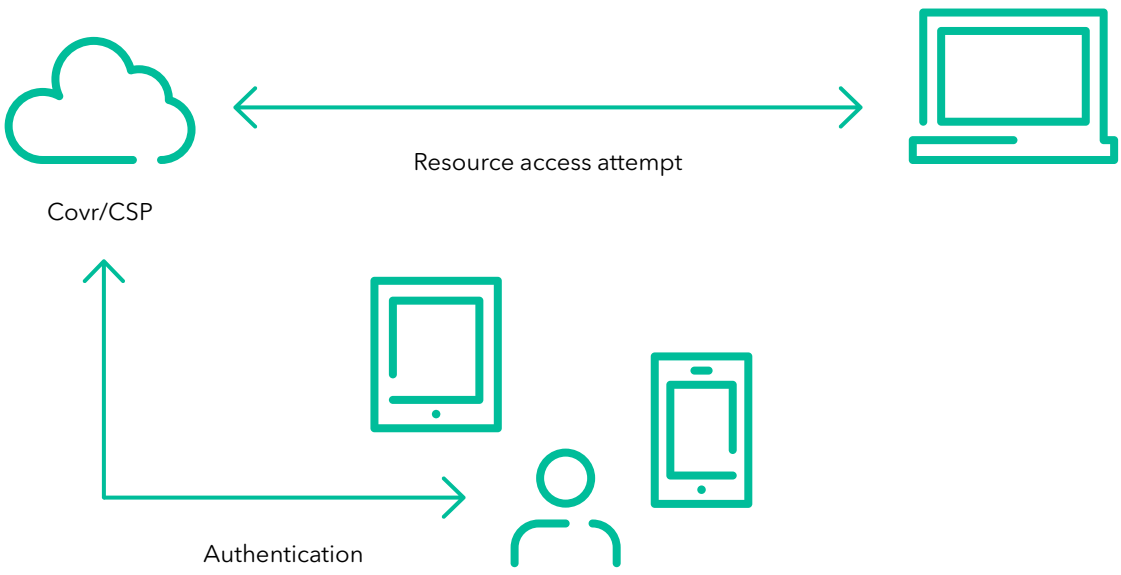
Service login
Covr can be used for any system where login procedures need to be secured beyond regular credentials. Covr also simplifies account management since there are no passwords to be forgotten, lost or retrieved.

Controlled and secured resource access
Access to sensitive data such as documents or images can be limited to selected stakeholders, and the system inherently allows for confirmation of such access on a per-resource basis.

Workflow approvals
When managing documents, invoices, etc., Covr can be used to facilitate approval processes enabling stakeholders to digitally "sign off" without the need for more elaborate technologies, such as encrypted PFX signing.

Multi-user authentication
A system may utilize Covr authentication in a manner where several individuals can be prompted for identification before a particular action is allowed. This both enables an additional level of security and allows for arbitrary authentication requests, where any one of the members in a group of users can acknowledge an action.

Multi-user authentication



Brief summary of Covr's benefits

What really differentiates Covr is the decentralized system architecture that certifies a strong connection at all times. Because the client side is operated entirely by software, the user is exempted from having to handle special hardware.

- Covr's reliable security channel for two-way communication is created between you and each user and, as a side effect, prevents less secure access points like password-based credential interfaces
- The transactional method of identity handshakes enables immediate intervention in any situation where sensitive resources are handled
- The integration is scalable and often a one-time step task
- Rollout doesn't need manual system administration
- The user registration process is tailored to be lightweight is handled entirely by the user
- The essential ambition of the Covr system is not necessarily to protect entry points, but rather to minimize their existence

Finally, people will continue to give their banking platform permission to swop to the best solution without having to make an active decision, and they will take for granted that their credentials are totally safe and protected. Covr comes fully prepared and has all the requirements for this new reality.

Summary
From the perspective of a Covr partner, the system offers a range of improvements over many traditional security measures. The architecture is inherently decentralized while still enabling partners to maintain a strong connection with their end users. It also facilitates management tools for handling such relationships.

There is no need for users to handle special hardware as the client side is operated entirely by software. The transactional method of identity handshakes enables immediate intervention in any situation where sensitive resources are handled. Integration is scalable and often a one-time step. Any subsequent rollout would not require manual system administration. The user registration process is tailored to be lightweight and manageable solely by the user.

A reliable security channel for two-way communication is formed between the partner and each user and, as a side effect, this seals the system off from less secure access points such as password-based credential interfaces.

The essential ambition of the system at its core is not necessarily to protect entry points, but rather to minimize their existence.

Terms and definitions

MITM
Man-in-the-middle attack - An attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other.

DNSSEC
Domain Name System Security Extensions - A suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks.

IDS
Intrusion Detection System - A device or software application that monitors network or system activities for malicious activities or policy violations

MFA
Multi-Factor Authentication - A method of computer access control which a user can pass by successfully presenting several separate authentication stages.

PKI
Public Key Infrastructure - A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

SHA1
Secure Hash Algorithm 1 - A cryptographic hash function designed by the United States National Security Agency and is a U.S. Federal Information Processing Standard published by the United States.

PFX
Personal Information Exchange certificate - A digital certificate format used in digital document signing functionality.

Partner
A Covr customer whose end users perform secure tasks using the Covr app.