keypasco

Your DeviceID – as unique as your DNA

How it Works

The secret behind the solution

There are many well-proven authentication solutions in the market. But the absolute majority of services are still using static passwords for login, followed by repeated frauds and scandals.

So why continue on a dead end street? To make our connected world safe, it is about time to step up and do things in a different way.

With features like DeviceID, location, and a unique Risk Engine, the Keypasco Solution can raise the level of security for you and your customers. The groundbreaking technology even offers you a way to secure ALL of your customers without affecting the user experience – **let us tell you how it works!**

Security By Your Own Device!

Over the years, reports have been pouring in about leaked account information, stolen passwords, credit card fraud, and other troublesome and costly incidents, all due to poor security solutions.

By challenging traditions and making things easier and more adapted to human behaviour, we believe we can put an end to the problems. This is why we created the Keypasco Solution.

The Keypasco Solution began with a simple idea. We have all heard of fraudsters fooling people to give up their username and password. But, what if your username and password only worked on your own device? Then this type of fraud would disappear!

We then added location as a security factor, so you must not only have the right device, it must also be in the right place. Today Keypasco offers a unique patented security solution based on the end-user's own device.

No distributed credentials = nothing to steal!

Traditionally ALL authentication solutions use distributed credentials, like password or a unique key, stored in a token or a mobile app.

But – credentials can, and will be stolen. That is why the patented Keypasco Solution does not rely on distributed credentials!

Traditional Digital Identity

Distributed credentials = username + password and unique key

- Hardware tokens
- SMS OTP, mobile software OTP token

Keypasco Digital Identity = DeviceID

- Device properties
- Location and proximity
- External personal device as part of device properties – Internet of Things

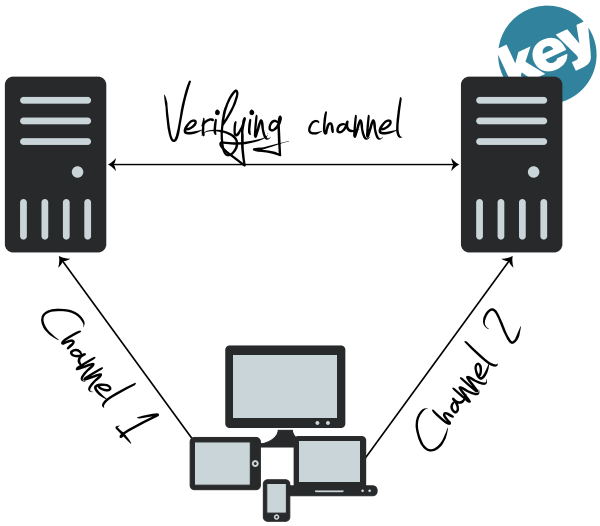
The Keypasco Solution

How it works

The solution consists of:

- The Keypasco server
- One or several devices
- A two-channel structure
- The Risk Engine

1. The DeviceID properties on the end-user's device are scanned and stored at the Keypasco server. Any personal device may form part of the digital identity
2. The first channel sends information between the end-user's device and the service provider
3. The second channel sends information between the end-user's device and the Keypasco server
4. To verify the authentication the service provider checks with the Keypasco server to confirm:
   - Device authentication
   - Geographical location
   - Proximity
   - Risk Engine analysis
5. Then, it is decided whether the authentication is successful or not



Our patented features

- **DeviceID and two-channel authentication:** Bring the user's own device as unique authentication device through a two-channel structure. ***Security by Your own device!***
- **Proximity:** The user's own devices / wearables in close position to each other as unique identity to enhance security.
- **Keypasco PKI Sign:** A unique solution for PKI in a mobile device without the need for a Secure Element. By using Keypasco PKI Sign no private key is stored at any one place, but it is still PKI compliant, making the solution extremely safe.
- **Dynamic URL:** This allows for single sign-on with one single trusted security app linking multiple Internet content providers on one side and multiple ID providers on the other.

The Keypasco server – Borgen™

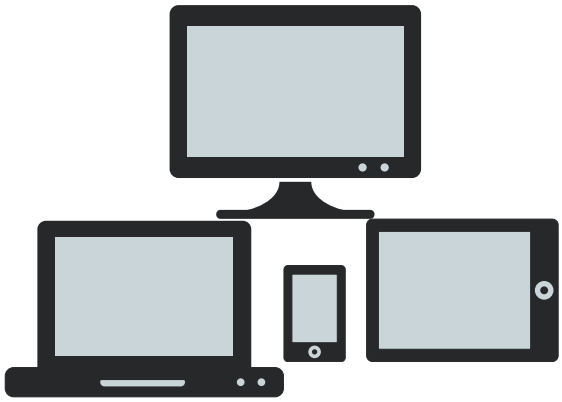
Keypasco authenticates the end-user by identifying and associating their device(s) and location(s) to an anonymous user-ID within the Keypasco server. No personal data is ever stored in either the client or on the server. The server is self-scalable to handle any volume.

- Cloud based / on premise
- Self-scalable
- Web-based graphical user interface
- Administration of multiple Internet Content Providers
- Administration of Licenses
- ICP Customer Support
- Billing management
- Integrity – no personal information stored

Keypasco clients – Vakten™

On the client side there are multiple choices and combinations of how to use the Keypasco Solution.

We support all major operating systems and platforms.



Vakten™ Mobile SDK

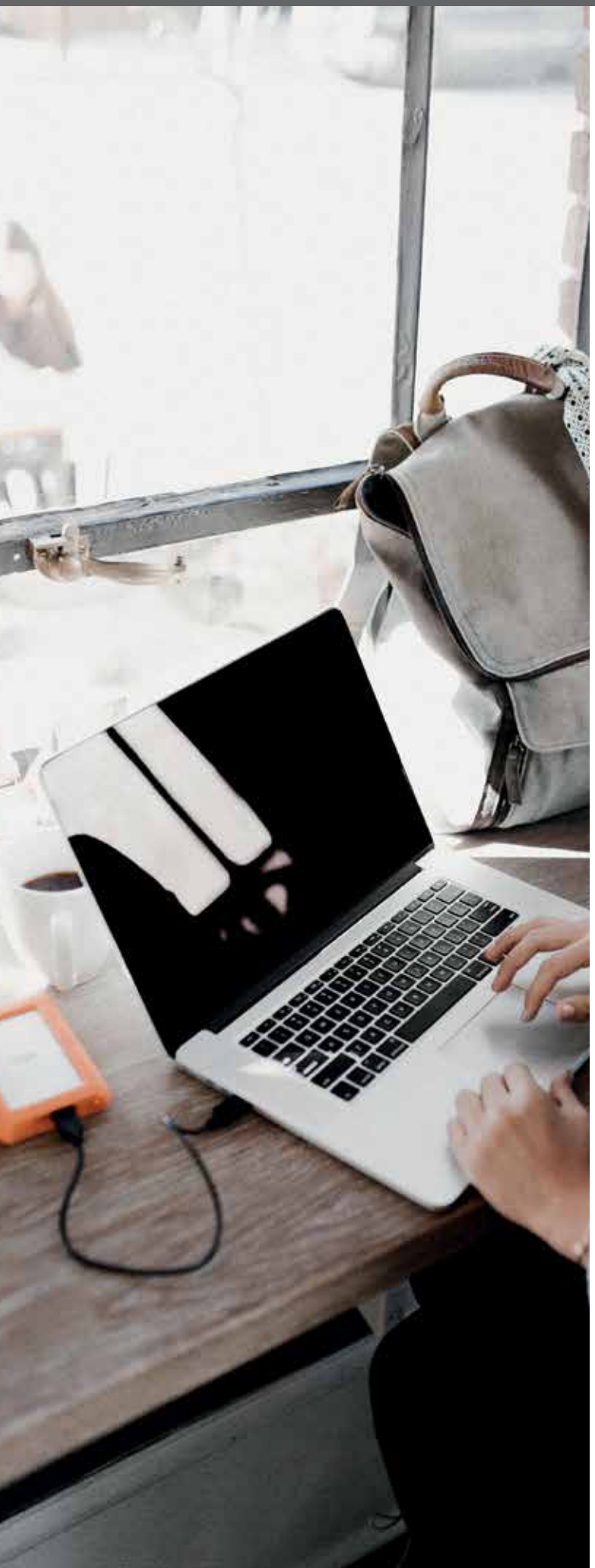
Integrate the Keypasco Mobile SDK in to your own application. Combined with our silent Generic enrolment, the Keypasco Solution immediately starts to protect you and your customers without any visible change for the end-user.

- Perfect for your smartphone and tablet applications
- Easy to install and integrate our SDK into your app
- Instant security with 100% customer coverage
- No end-user interaction required with silent Generic enrolment
- Simple and straight-forward yet powerful API
- Identifies the device and its location
- Confirms secure verifications and signatures through the Out-of-Band verification channel
- Possible to use the Keypasco PKI Sign as signing method

Mobile SDK

DeviceID

- Device attributes
- Exact ID with device properties
- Debugger, malicious code, jailbroken / rooted detection
- Geolocation, GPS
- Extra features, e.g. Proximity



Vakten™ Mobile app

The Keypasco Vakten app is a generic authentication application. If you do not have your own app, this is an easy way to increase security for you and your customers.

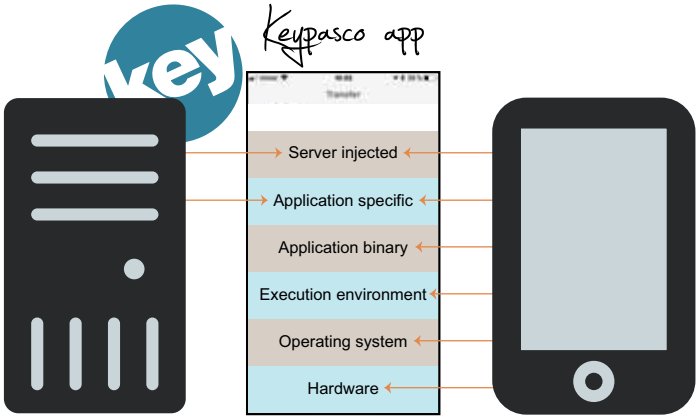
The Keypasco application – Vakten™

- When you do not want to develop your own app
- Use it for secure login, transaction signing and money transfer etc.
- Skip online passwords! Use the mobile's biometric identification instead
- The same app can be used for multiple online services and providers
- Keypasco branded, or with your company's logo

Six layers of protection

The Keypasco Mobile SDK and app has a 6-layers structure for protection, making our mobile solution extremely secure and flexible.

From each layer we gather a large amount of properties. A single property may not be unique but put together the properties will create a unique DeviceID.



Vakten™ Desktop

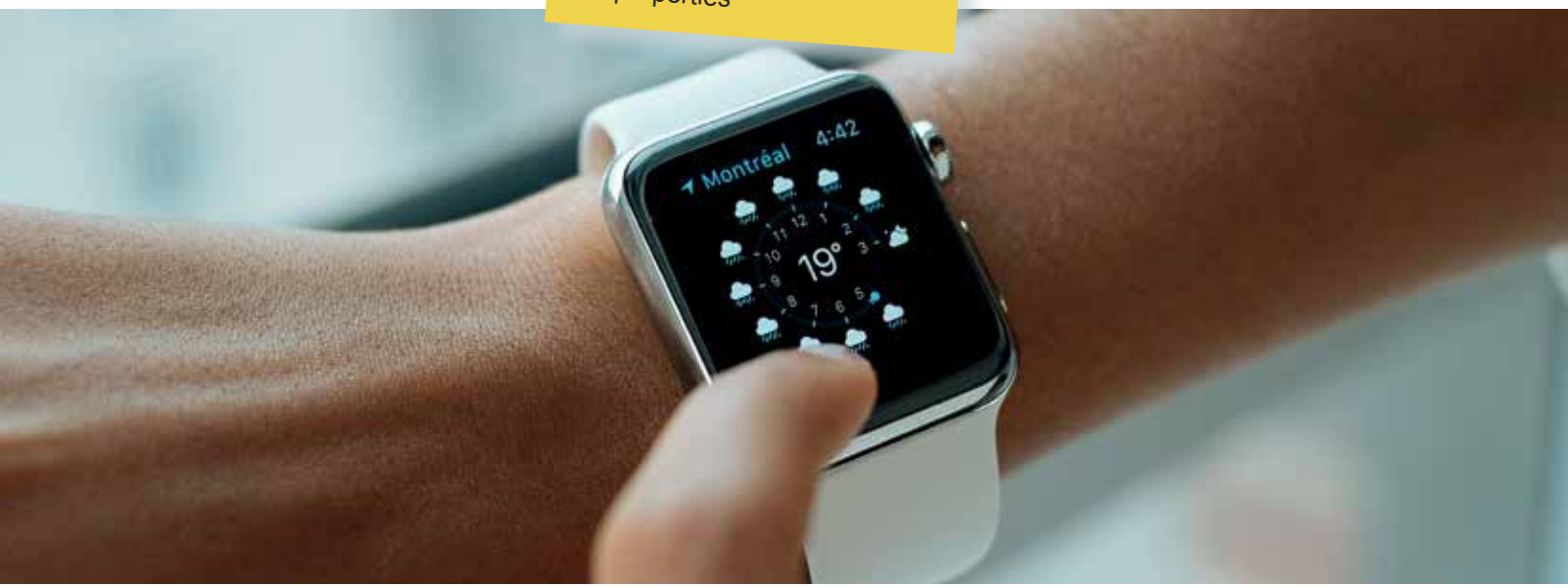
Our desktop client is installed on the end-user's desktop computer for identification of the device and location. It also provides the functionality of secure verifications and signatures. The desktop client can be used to secure web solutions as well as desktop applications.

Browser properties

- JavaScript based solution
- Device attributes; Fonts, screen resolution etc.
- Browser plugins; Flash, Silverlight etc.
- IP address, geolocation, HTML5 detection
- Exact ID using device properties

Vakten™ Browser

With Vakten Browser, there is no installation required instead it is executed in the background each time the end-user enters your website. With the Browser client, the Keypasco Solution can verify the device and location. An excellent complement to the mobile solution.

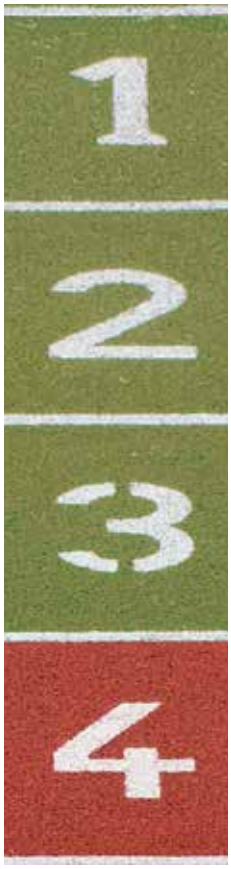


The Keypasco Risk Engine

The unique Risk Engine, based on the Keypasco DeviceID technology, operates in the background to continuously improve the security for you and your customers.

- Powered by smart data mining of device properties
- Working in the background
- Gathered and measured sources – device, user, behaviour, system etc.
- Provides the rule engine with factors like – time, location, behaviour etc.
- Keep track of devices being jailbroken / rooted etc.
- Blacklist of users and devices not compliant with set rules
- Customizable rules and decision-making according to your needs
- Precise decisions with extremely low false positive / negative ratio

As the Keypasco Solution is used, the Risk Engine is fed with more and more information, which leads to better and better conclusions and increased security. We call this "Smart Data Mining".



By analysing the aggregated information, the Risk Engine can score the situation in four levels (as a minimum):

Green1 – CHANGE

This is the best situation and the user is 100% correct. Most transactions, more than 99.4%, are Green1.

Green2 – REDO

You can allow the user to do things they have done before. Typical reason: known device in a new and far off location.

Green3 – LOOK

You can allow the user to check the account balance. Typical reason: new device in new location. (Yes, we can recognize the user, without knowing the username, even if the device is new.)

Red – DENY

We advice against login or sign. Typical reason: wrong device – hacker / unauthorized person.

How it Works

Keypasco PKI Sign

Keypasco has invented a unique patented solution for PKI in a mobile device, without the need* for a secure element. With the Keypasco PKI Sign no private key is stored at any one place, but it is still PKI compliant, making the solution extremely safe.

This is a customisable and hardware independent solution for secure authentication and signing. The end-user's private key is divided into three parts: a client part, a server part, and a secret (PIN/fingerprint).

The private key only exist if the user:

- Wants to make a signature
- Has his mobile
- Is in the correct location
- Provides the secret

**However, if you have a secure element we use it.*

GeoOTP

For times when a user uses an online terminal in combination with an offline smartphone, we have created a solution called GeoOTP.

Our app / mobile SDK has a feature for generating a GeoOTP. For the user, it is like a regular OTP, but with more functionality in the background. So even in the case of an offline mobile, we can track the location and which device it came from. We can also check the proximity between the offline mobile, and the online terminal where the GeoOTP was used.

Proximity

The idea behind proximity is to further increase security. With proximity you can add more devices to the "same" device.

These other devices should be in proximity with the main device. For example, you can decide that your smart watch must be in proximity with your mobile to be able to login.

Generic enrolment

We have learned that the enrolment process can be difficult. No one wants to bother the end-user with complicated procedures, even if it is to increase security. To solve this, we offer a way to associate devices without affecting the end-user.

In the majority of cases, it is the right account owner who logs in to an online service. By associating the account to the first device used to access the service, the account can be locked and then only accessible to that user from this specific device.

In cases where an incorrect user locks an account, there was already a problem. Now, with their account locked, the correct user is likely to contact you to resolve the issue. Over time, all cases will be resolved and fraud will go down. This is a way to enrol your existing customers with a minimum of end-user involvement.

Strict enrolment

Certain types of services may require an extra high level of security. It may for example be appropriate with a stricter enrolment for services such as: Finance, e-Government, credit card protection, and Mobile Payment services. We then apply a stricter enrolment with user identification.

Generic enrolment

- Automatic enrolment in background
- No end-user interaction
- Provided through browser and / or mobile app
- Easy to integrate with your current solution
- Instantly protects all of your customers after implementation