# ))·((CYBERUSLABS
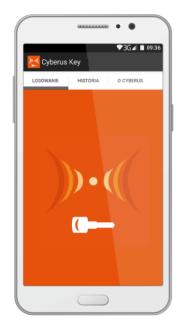
SECURE WORLD



# CYBERUS KEY

## A Solution for PSD2 (Directive (EU) 2015/2366)

## in regard of
## Requirements for Banks & TPPs Cooperation.

CYBERUS KEY    EXO5

**CYBERUS KEY – A Solution for PSD2 Requirements for Banks & TPPs cooperation.**

The PSD2 directive enables bank customers, both individual and businesses, to use third-party providers (TPP) to manage their finances. Customers will be able using even such operators like Google to pay their bills or making P2P transfers. TPPs will be able also to analyze customer spending, while customers continue to have their money kept in the bank account. Banks will be obligated to provide these third-party providers access to their customers' accounts through open APIs (application program interface). This will enable TPPs to provide financial services using banks' data and infrastructure.

The directive's aim is to improve present EU rules for electronic payments. EU directive establishes also rules concerning among others:

Strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud;

The directive came into effect on January 12, 2016. EU member states must incorporate it into their national regulations by January 13, 2018.

**The impacts**

The new directive brings key changes that include:

1) Third-party payment initiation: Payment Initiation Service Providers (PISP) will be able to initiate online payments from the payer's bank account.

2) Security of online payments and account access through the introduction of new security requirements for electronic payments and account access.

Banks will be required to open-up their infrastructure to third parties by offering APIs under the XS2A (access to account) rule. They will be forced to grant them access to their customers' online account/payment services in a regulated and secure way.

·With PSD2, the Directive will allow retailers to 'ask consumers for permission to use your bank details. Once you give permission, the retailer will receive the payment directly from your bank without intermediaries

·The direct connection between retailers and banks will be enabled using Application Programming Interface (API)

·A strong customer authentication system

Third party access to accounts (XS2A), the use of API's to connect merchant and the bank directly and the ability to consolidate account information in 1 portal.

At the same time the TPPs must ensure that the highest levels of security are implemented also on their side as they will be handling payments of banks customers.

**CyberusKey** offers a possibility to play a role of the platform connecting banks and TPPs. It is one of the main features of the **CyberusKey**.

The idea behind the system to:

- enable secure login to user account

- enable secure transaction

- secure anonymous online operation while operator has a full information about the payee

- provide with time, date and geolocation information about account login and transaction

**CyberusKey** is an identification platform that answers the requirements of the PSD2 directive. System enables banks' customer to access the account and make any online transaction.

A crucial part of the system is a CyberusKey Authentication Server (CAS). The installation of **CyberusKey** within banks IT infrastructure ensures the safety of users' data that the bank is responsible for. But **CyberusKey** does much more than that.

For every bank customer being registered to the service an anonymous profile is created on the CyberusKey Authentication Server (CAS). Only this server and only the data and user profile stored on it is being used for the logon/ transaction confirmation purposes. That means that no actionable user's credentials are being used to perform any of the above mentioned operations. The only elements that **CyberusKey** uses are:

- one-time-code that uses One-Time-Pad methodology generated by the HSM

- app and smartphone unique ID and profile data

That allows to keep actionable users credential within the bank's infrastructure and not to transmit them outside of it and still being able to perform online transactions, without the risk of unauthorized parties being able to intercept those information and misuse it or even steal the credentials.

**Cyberus Labs sp z o.o.**     ul. Królewska 65a/1       www.cyberuslabs.com        NIP: 9442248670
30-081 Kraków, Polska     kontakt@cyberuslabs.com    KRS: 0000565252

CYBERUS KEY     EXO5

Why is this so important in case of the PSD2 directive? One of the biggest fears of the banks will be sharing their users' data with TPPs. Another is creating a common platform that uses API to connect with TPPs.

**CyberusKey** is an answer for this. It is an already existing platform with a ready API that offers a possibility of an anonymous Single-Sign-On solution. Contrary to the present SSO solutions that transmit user credentials, the sign-on process with use of the **CyberusKey** is anonymous. Only a one-time-code and user profile is being used for this operation.

How does this solve problem of PSD2 requirements? Every TPP that wants to make transactions for the banks customer needs to be integrated with the use of API with bank. **CyberusKey** system gives a solutions or banks and TPPs working together and perform online transactions without sharing customer credentials or any data between banks and TPP during this process. In case of implementing **CyberusKey** in the bank it is enough that bank's users are also **CyberusKey** enabled TPPs users or vice versa. TPPs that will adopt **CyberusKey** will have its own separate data base of the customers that are at the same time customers of the bank behind its own firewall.

In this case, when making a transaction for a customer with its bank there is NO user's information/credentials shared between the entities. However – at this same time both operators will receive information about the transaction. That eliminates the biggest threat of any online transaction- user's credentials and payment details being transferred online.

*Source:* http://ec.europa.eu/finance/payments/framework/index_en.htm

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366

http://eur-lex.europa.eu/legal-content/EN/LSU/?uri=CELEX:32015L2366

http://fintechnews.ch/moneytransfer/eus-payment-services-directive-psd2-what-it-is-and-why-it-matters/6959/

https://www.evry.com/en/news/articles/psd2-the-directive-that-will-change-banking-as-we-know-it/