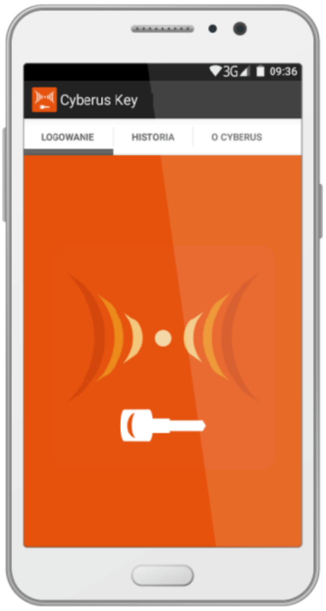
CYBERUSLABS

SECURE WORLD



CYBERUS KEY

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

in regard of
PSD2 Strong Customer Authentication Requirements

Cyberus Key is a protected patent-pending technology.

CYBERUS KEY and PSD2 Strong Customer Authentication Requirements

PSD2 (Directive (EU) 2015/2366) and strong customer authentication rules.

The PSD2 directive refers to “strong customer authentication” several times. A strong customer authentication is now a core of the technical security standards for payment services in Europe.

__PSD2__ defines “Strong Customer Authentication” as authentication based on the use of two or more elements categorized as:

Knowledge – something only the user knows

Possession – something only the user possess

Inherence – something the user is

Each are independent, so the breach of one does not compromise the reliability of the others.

CyberusKey uses smartphone as a universal key to any ***CyberusKey*** enabled online service/website.

System provides a strong customer authentication required be EU directive with:

a) using a smartphone – something user possess

b) implementing solutions for securing a ***CyberusKey*** with:

- PIN code - something only the user knows,
- biometric technology chosen by the operator – something the user is

It is, however, very important to remember that biometric technologies should be used as a second factor authenticator and not the first one.

In case of biometric credentials being stolen users loses a chance to login with use of biometric technologies to their account forever. If biometric is used as a second factor it can easily be replaced with PIN. For higher security requirements ***CyberusKey*** can integrate within one system multiple layers of authentication factors, depending on the operator's needs.

Liability

States if the:

“Payments service provider of the Payer does not require multi-factor authentication the payer will not incur any financial losses”

“Payee or payment service provider of the payee do not accept multi-factor authentication, then they need to refund any losses to the payer’s payment service provider

CyberusKey provides easy to install for the operator but also simple to use and secure for its customers 2 factor authentication login and transaction confirmation system. ***CyberusKey*** provides ease of use and security in one solution. Until today operators had to engage separate operators and systems in their infrastructure to be able to provide 2 factor authentication that was:

- not ensuring customers security

- was easy to hack and steal customers’ credentials (passwords)

- was many times compromised (like SMSs)

- inconvenient and costly (SMS services, hardware tokens)

- difficult to use and remember (passwords)

Right of Recourse

if any payment service providers fail to provide strong customer authentication they should compensate the other payment service providers where:

•Unauthorised payments are made

•Non-execution, defective or late execution of payment transactions are made.

Authentication

Countries will need to ensure that payment service providers implement strong customer authentication where the payer:

•Accesses the payment account online

•Initiates an electronic payment

•Carries out any action through a remote channel which may result in the risk of payment fraud

From the above regulations emerges strong need of a one integrated 2 factor authentication system that is easy to install within banks IT infrastructure and is also simple to use and secure for banks customers.

CyberusKey is such system. It not only delivers in one integrated system all the features that at present are being delivered by various systems that need to be integrated later with banks IT system. **CyberusKey** :

1) is easy to install within any internal bank's IT infrastructure (ready API)

2) uses one-time code that is being used for every login or transaction confirmation

3) one time code is generated by Hardware Security Module (HSM) and is based on the only unbreakable encryption system called One-Time-Pad or Vernam Cypher

4) creates anonymous profile of every registered banks customer stored on the CyberysKey Authorization Server (CAS) that is installed behind bank's firewall to ensure security

5) uses only one-time-code and anonymous user profile to perform online transactions (login and transaction confirmation)

6) no customers' actionable credentials are being used or transmitted during any operation

7) for all transactions uses out-of-band communication to ensure full security

8) transaction information includes date, time and geolocation information that are available to the bank and customer. They also may be transferred to fraud engines of the bank and by delivering precise information of made transactions form and analyze customer behavior patterns that will be used to trigger early warning signals preventing fraudulent operations.

9) out-of-band communication also prevent **CyberusKey** users from performing unauthorized transactions. Even when cybercriminals would be able to infect browser and change the transactions details they will be passed in this changed form to customer who will be able to reject it, fully aware of the fraud attempt.

10) provides integrated 2 factor authentification system

CyberusKey gives the banks the comfort that in the simplest way provides full security not only for the banks customers as required by the EU PSD2 directive but also gives bank the secure tool to protect against financial loses and to comply with EU regulations

Sources: 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://www.sepaforcorporates.com/payments-news-2/wtf-psd2-say-2fa/