

PRONEXTOR

Mobile Encryption System

The patented system for data protection and data transport

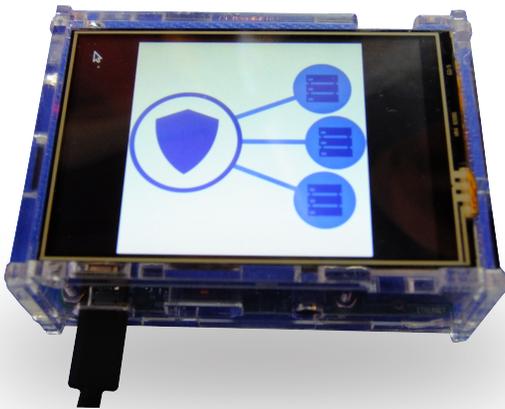


THE ULTIMATE SECURITY FOR YOUR DATA

- ✓ The Mobile Encryption System (MES) is a device similar to a smartphone that is connected to a PC and ensures that an hacker cannot read or steal the passwords for the encrypted data. MES is based on a patented process.
- ✓ No matter which current encryption method you use today, the encryption and decryption is performed on your PC or laptop.
- ✓ As a result the secret key is at least temporarily stored on your computer. In addition, the key must be entered into the system by the user. These two vulnerabilities can be used by potential attackers to get the key.



OUR PATENTED METHOD SOLVES THIS PROBLEM ENTIRELY



Demonstrator

- ✓ Connection to external storage media such as USB memory sticks, hard drives, SSDs or SD cards, mobile devices such as mobile phones or tablets, digital cameras etc.
- ✓ No external access over networks.
- ✓ Full control of the data, including ongoing visualization of the access (detection of attacks such as Ransomware).
- ✓ Optional: Creation of log files, setting of limits (access type, amount, time of access).

PRONEXTOR

Mobile Encryption System

The patented system for data protection and data transport

The mobile encryption system of the future. As easy to handle as an USB memory stick, robust and secure. Even if you lose it, your data remains protected from unauthorized access. You can use it on your PC, Mac or Linux system, on mobile devices with Android or iOS, on televisions, projectors and many other devices.

WHAT DATA CAN BE PROTECTED?

In general, everything that can be stored digitally can be secured by MES.

FOR WHOM WAS MES DEVELOPED?

Basically everyone wants to have his data available everywhere while at the same time preventing unauthorized access to it. Both private and business data is exposed to various dangers such as theft, manipulation, deletion or encryption.

Private applications

- ✔ Personal files such as photos, documents or copies of ID cards, access credentials to services on the network, social networks or corporate networks.
- ✔ Financial data from eBanking applications, shops such as Amazon or eBay and Paypal booking slips.
- ✔ Password lists and PIN codes for services outside the internet or complete backups of your computer or mobile device.

Business Applications

- ✔ Fulfilment of the storage obligations.
- ✔ Data confidentiality is maintained, even in the event of theft Comment deleted.
- ✔ Protection of research and development data until it is commercialized, publicated or patented.
- ✔ Transport of reports, presentations or lectures that can be directly processed from MES.
- ✔ Project data such as quotations, applications or reports that should only be available to a limited number of employees.



Demonstrator

The Team

Christian Kollmitzer

Expert for IT Security
AIT Austrian Institute of
Technology / Department
Mobile Safety & Security

Thomas Köck

Business economist
Bausparkasse der österreichischen
Sparkassen / CEO Founder of Inno
vationlab firefly solutions GmbH