CeBIT: CyphWay ? One device for all scenarios

CeBIT: CyphWay - One device for all scenarios
Smartphones and tablets allow easy and convenient sending of images and information anywhere. But when it comes to sensitive data, security is important. Their widespread use makes tablets and smartphones a lucrative target for spies. CyphWay, developed at the Fraunhofer Institute of Optronics, System Technologies and Image Exploitation (IOSB) closes this vulnerability. The core of CyphWay is a trusted hardware module, which encapsulates and protects safety-critical components, such as encryption, decryption, and key management, and ensures optimal protection of sensitive data.
Ever new cases of hacker attacks, data leaks, and espionage demonstrate the lack of data security when sending and receiving between workplace and cloud, between enterprise server and tablet, or from smartphone to smartphone. In many areas this prevents police, government agencies, and companies from taking full advantage of fast, mobile data communication. A business owner, for example, may want to send sensitive contract data to their company, for which they require a line that is secured against eavesdropping. A police officer who has taken a photo of the crime scene with a cellphone is not allowed to send the image to colleagues with standard communication technology. He may do this only if unauthorized access to the data can be excluded at the highest level of security. The experts for secure communication architectures at Fraunhofer IOSB are working on a highly secure communication solution that can be used with all available devices.
CyphWay provides data encryption and decryption
CyphWay - a small add-on device - provides a maximum-security channel for data transmission. "The safety systems of CyphWay have a modular structure. This allows for easy adjustment of the safety system to different application scenarios, explains project leader Dr. Andreas Jakoby of Fraunhofer IOSB. One module, for example, specializes in the encryption and decryption of data. Another module provides a secure connection between the add-on device and the communication hardware used. This allows CyphWay to be connected both to stationary hardware - such as a desktop PC or a server environment - and to a tablet or smartphone via a wireless connection.
The cryptographic functions of CyphWay can be used for secure provision of data on a cloud, mobile access to corporate data, or secure telephone conferences. The connection between a smartphone or other mobile device and CyphWay can be established, for example, through an encrypted Bluetooth channel. For secure sending of photos taken with a cellphone camera, the image file is first transferred to the add-on device, where it is encrypted before being sent back to the cellphone as a secured file.
Tampering is futile
"Secured with strong cryptographic systems, the file can safely be sent to another mobile device or a server. Should it fall into the wrong hands, the transmitted information cannot be read and is useless to the data thief, explains Jakoby.
At the recipient of the protected information the file is also processed by the security module of their CyphWay device and can then be viewed and edited on screen. Because the data encryption and decryption takes place entirely on the additional device, the encryption processes cannot be bypassed. Unauthorized access to and tampering with the add-on device are not possible.

Fraunhofer-Institut für Informations- und Datenverarbeitung IITB
Fraunhoferstraße 1
76131 Karlsruhe
Telefon: +49 (0) 7 21 / 60 91-0
Telefax: +49 (0) 7 21 / 60 91-4 13
Mail: juergen.beyerer@iitb.fraunhofer.de
URL: http://www.iitb.fraunhofer.de

<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=558055" width="1" height="1">

Pressekontakt

Fraunhofer-Institut für Informations- und Datenverarbeitung IITB

76131 Karlsruhe

iitb.fraunhofer.de
juergen.beyerer@iitb.fraunhofer.de

Firmenkontakt

Fraunhofer-Institut für Informations- und Datenverarbeitung IITB

76131 Karlsruhe

iitb.fraunhofer.de
juergen.beyerer@iitb.fraunhofer.de

Weitere Informationen finden sich auf unserer Homepage