

Press Release

BlackBerry security under control – even during travelling

The new version of eperi Mobile PKI (BlackBerry) makes sure that unauthorized access does not occur, not even during worldwide travelling. The complete mobile data communication with the BlackBerry is secured through own PKI operations.

4th October, 2010 – One of the strongly discussed issues within the past months was the attempt of various states to get access to communication of BlackBerry devices. With the eperi Mobile PKI, however, enterprises and organizations gain total control of their BlackBerry device security. The entire data communication between mobile device and enterprise is encrypted through PKI (Public Key Infrastructure) methods. No matter to what country you are travelling, you can rely on security of your own PKI.

eperi Mobile PKI provides secured and efficient use of mobile devices within enterprises. For BlackBerry devices, it enables secured communication, even throughout international communication points, without having to sacrifice any part of user-friendliness or simplicity on administration.

Currently, an increasing number of states set their demands on RIM for access to mobile BlackBerry communication. With the public discussion on it, the necessity of an own independent security strategy becomes even more apparent. Get your mobile and your enterprise out of that risk by use of an additional protection feature, which is quickly and easily installed.

The Mobile PKI BlackBerry establishes a hybrid encryption (RSA1024, AES256) of the complete data traffic that remains entirely under enterprise control. eperi uses the standard interfaces of the system software to implement the necessary security functions. Thereby, secure communication for sensitive emails, calendar notes and addresses is guaranteed even for mobile operations.

The eperi mobile PKI provides roll-out of software and certificates over the air (OTA) and automatically. After release by the administrator, the software and private keys are transferred automatically and safely. A possibly available own PKI can be integrated and thus still be used. The certificates and private keys on the mobile device are stored in an own secured key store. Thereby, unauthorized access is entirely and reliably prevented during data transfer. On operation and maintenance, not a single user interaction is needed – just as it has to be.

Press Release

About eperi

eperi provides an innovative IT security solution for data in the cloud. Our securityRunTime is build as an open source solution. It is used by leading international enterprises.

The company was founded in 2003 and is located in Darmstadt, Germany. Since the beginning of 2014 we sign with our new name: eperi GmbH. With more than 10 years experience in software development we stand for information security that is trusted: eperi.de/en

Contact

Henriette Heidbrink
eperi GmbH
Uhlandstraße 9
64297 Darmstadt
Telefon +49 (6151) 95130 33
Fax +49 (6151) 95130 66
henriette.heidbrink@eperi.de
eperi.de/en

The screenshot displays the 'Security Administration (RCP)' application window. The main area shows a table of users with columns for UserID, First Name, Last Name, and Device Status. The 'user10' row is selected, and its properties are shown in a panel below the table.

UserID	First Name	Last Name	Device Status
user1	Alexander-Horst	Hanke	64 - Key installation successful
user10	Jens	Schmitt	64 - Key installation successful
user100	Lea	Tillmann	64 - Key installation successful
user101	Jennifer	Elele	32 - Key installation failed
user102	Jose	Ortkamp	02 - Installation successful
user103	John	Kostendieck	04 - Applying security rules failed
user104	Annette	Ambroster	64 - Key installation successful
user105	Jonas	Major	
user106	Melanie	Schauss	64 - Key installation successful
user107	Tim	Hanke	64 - Key installation successful
user108	Rebecca	Mueller	16 - Keys generated
user109	Felix	Balkowski	32 - Key installation failed
user11	Johanna	Gogolin	64 - Key installation successful
user110	Felix	Berthold	64 - Key installation successful
user111	Agathe	Hanke	

Properties

Properties: Roles Alias Certificates User Devices (Mobile PKI) Device contacts Installation Log

UserID: user10
Password: ***** Initialized
Last Name: Schmitt Active
First Name: Jens Send Init-Mail
Email: Schmitt@acme.com
 Hide Password

Current User: administrator

Mobile device administration in a graphical user interface showing the device status

Press Release



BlackBerry handheld with installed eperi Mobile PKI Solution – in this image an update notice email is displayed informing about a certificate update in the background.