BIZZTRUST FOR ANDROID
PROTECTION OF SENSITIVE DATA AND SERVICES

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Oliver Küch
Rheinstraße 75
64295 Darmstadt, Germany

Phone +49 6151 869-213
Fax +49 6151 869-224
oliver.kuech@sit.fraunhofer.de
www.bizztrust.de

In many enterprises smartphones are part of the corporate culture, but often these devices do not fulfill the necessary security requirements. With BizzTrust for Android, Fraunhofer SIT and Sirrix have developed a solution that protects sensitive enterprise services and data without restricting functionality and users.

Business users increasingly use employer-issued smartphones for personal as well as business applications (apps). However, in current devices little infrastructure is available to facilitate remote management and enforce enterprise security policy. Moreover, the use of smartphones for personal and business purposes increases the exposure to unknown software and unauthorized parties, putting the enterprise's data and services at risk.

Challenges
In dual-use scenarios, the employer should usually take care of the security and management of the smartphone, but often it is not in the interest of the employee to give the employer full control over partly personal data on the smartphone. Similarly, it is not in the interest of the employer that the IT department is potentially responsible for the private data on the employee's phone. In addition to this conflict of interest, usability poses the biggest challenge: The centralized security management of the employee's smartphone should not restrict functionality to the point where it is easier to use two separate phones.

Solution
BizzTrust for Android offers a revolutionary solution by smartly and securely separating the application areas into business and private, basing on the consequent use of an extended security kernel. Previous security solutions did not provide adequate protection against root exploits and malware. Private and business applications can be used in parallel and independently; both areas contain their own data records and access authorization. Furthermore, the flexible remote maintenance protocols make it possible to analyze the software status of a remote device and to enforce update or remediation procedures realizing an enterprise's security policy. Fraunhofer SIT and Sirrix combine innovative container isolation and modern communication protocols that allow for central network integration, remote maintenance and device management.

Features
- Protection of business data
- No restrictions for private use
- Secure enterprise communication (encryption)
- Supports bring-your-own-device strategy
- Remote management and update
- Automatic policy enforcement

TeleTrusT
Winner of the TeleTrusT
Innovation Award 2012

Investments into your future

HESSEN