



BIZZTRUST FOR ANDROID

PROTECTION OF SENSITIVE DATA AND SERVICES

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

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 as well as 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 resolves these problems and creates a framework for flexible network integration and management of remote devices. Fraunhofer SIT has achieved this by combining innovative container isolation and modern communication protocols that allow for central network integration, remote maintenance and device management. BizzTrust separates applications and data into security domains, executing personal applications in parallel and independently from business applications. 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. With the extended remote management, the business compartment of the employee's phone can be integrated into the enterprise event management infrastructure.

Features

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

*Fraunhofer Institute for Secure
Information Technology SIT*

*Contact:
Oliver KÜch
Rheinstraße 75
64295 Darmstadt, Germany*

*Telephone: +49 61 51 8 69-213
Fax: +49 61 51 8 69-224
oliver.kuech@sit.fraunhofer.de*

www.sit.fraunhofer.de