R&S®Trusted Mobile
Security for Smartphones and Tablets

The Android platform R&S®Trusted Mobile provides companies and public institutions with security for smartphones and tablets.

Mobile devices like smartphones and tablets have become essential tools in both our private and professional lives. But mobile devices are also especially liable to get lost or stolen, allowing third parties to access sensitive business data or even the entire company network. The use of mobile devices therefore leads to considerable security risks. Attacks like zero-day exploits target the company's core to gain access to sensitive information or cryptographic keys. Until now, all current commercial security mechanisms like MDM- or container-based security solutions were unable to offer sufficient protection against such attacks.

Adequate security measures are crucial for the use of mobile devices in companies.

Separation of data and apps in an "Open" and a "Restricted" area

R&S®Trusted Mobile is based on a hardened security kernel that provides protection against attacks such as zero-day exploits by employing additional state-of-the-art security mechanisms, security services and finely granular access rules. Optionally, R&S®Trusted Mobile supports smart cards for the protection of long-term keys.

R&S®Trusted Mobile is completely compatible with Android and therefore allows the use of any Android app in both security areas.

ROHDE&SCHWARZ
Cybersecurity

Product Flyer | 03.00

Secure access to corporate resources

The separation between a “Restricted” and an “Open” area enables secure access to business resources. Applications inside the “Restricted” area can exchange data with each other and access company resources such as e-mails, contacts, calendars and the intranet via a secure VPN tunnel. Optionally, the “Open” area can access the intranet via a corporate firewall that filters dangerous content. All data that is exchanged by smartphones and corporate network is protected against unauthorized access by secure encryption.

R&S®Trusted Mobile also encrypts telephone calls to the headquarters and to company-owned smartphones and is compatible with the Rohde&Schwarz Cybersecurity voice and chat solution. The flexibility of a smartphone is always maintained. In the “Open” area, users can install their preferred apps (e.g. via Google Play Store), without affecting the security of the corporate network.

The R&S®Trusted Objects Manager is used as a management component and offers not only EMM and MDM functions but also an enterprise app store that is controlled by a central rules management. Android apps can be installed exclusively via the enterprise store or in combination with a conventional app store.

Basic Features

- Hardened security kernel for Android 6
- Separation of private data and apps from business resources
- Encryption of all data on mobile devices
- Optional smart card support

Security

- Hardened security kernel with mandatory access control and type enforcement
- Central management of installed apps
- Certificate-based VPN via IPsec-Tunnel to company resources
- ECDH and ECDSA up to 512/521 Bit (software or smart card)
- Device encryption with AES-XTS 256 algorithm
- “No Spy Mode” deactivates microphone and camera

Central Management

- R&S®Trusted Objects Manager (TOM) as central management of corporate network
- Device, policy and configuration management
- Full public key infrastructure with automated distribution of software certificates
- OTA distribution of all updates possible
- Connection to directory services (LDAP, AD)
- Support of existing CAs
- Central selection, certification and distribution of corporate apps

Comfort Features

- Separation of “Restricted” and “Open” on a single device
- Installation of apps via enterprise app store
- Compatible with all Android apps

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
Info: +49 30 65884-222
Email: cybersecurity@rohde-schwarz.com
www.cybersecurity.rohde-schwarz.com

Rohde&Schwarz GmbH&Co. KG
www.rohde-schwarz.com

PD 3607.5802.32 | Version 03.00 | Mai 2018 (sch)
R&S®Trusted Mobile

3607580232

3607.5802.32 03.00 PDP 1 en