Rohde & Schwarz Cybersecurity

R&S®TRUSTED MOBILE

Mobile devices such as smartphones and tablets have become an indispensable part of everyday work. This means that more and more sensitive business data is stored on these mobile devices, resulting in considerable security risks:

- Data loss, e.g. through apps and malware
- Data manipulation, e.g. through Trojans
- Unauthorized company access, e.g. through lost or stolen devices

None of the current commercial security mechanisms such as mobile device management (MDM) or container-based security solutions offer sufficient protection against these risks. Adequate security measures are crucial for the use of mobile devices in enterprises.

Product flyer
version 04.00

ROHDE&SCHWARZ
Make ideas real

Security-hardened Android without backdoors

R&S®Trusted Mobile is based on a hardened security kernel that safeguards your device against attacks like zero-day exploits by employing additional state-of-the-art security mechanisms, security services and granular access control. The Rohde&Schwarz Cybersecurity concept, which extends to R&S®Trusted Mobile, allows monitoring and, if necessary, blocking of all data streams. R&S®Trusted Mobile supports smart cards to protect your long-term cryptographic keys. R&S®Trusted Mobile is compatible with Android, so all common Android apps can be used.

Secure access to company resources

Following the Rohde&Schwarz Cybersecurity concept, the smartphone is split into two virtual environments. This separation between "Restricted" and "Open" enables secure access to business resources. Applications inside the "Restricted" environment can exchange data and access enterprise resources such as emails, contacts, calendar and intranet through a secure VPN tunnel. Optionally, the "Restricted" environment can access the internet through the secure company infrastructure. All data that is exchanged by smartphones and corporate network is protected against unauthorized access by secure encryption.

With its security features, R&S®Trusted Mobile is the ideal platform for applications that offer secure, encrypted voice or text communication. It also supports publicly available app stores in the "Open" environment. In this way, the user has full flexibility and the security of the company network is ensured.

Product variants

R&S®Trusted Mobile is provided in the following variants according to security requirements:

- **R&S®Trusted Mobile – Restricted,** for official use only (RESTRICTED)
- **R&S®Trusted Mobile – Pooling,** for multi-user scenarios
- **R&S®Trusted Mobile – Enterprise,** for companies and authorities

Core features

- Hardened security kernel
- Separation of private data, applications and company resources (e.g. separated contact list, to prevent apps such as unsecure messengers from accessing company contact data)
- Optional secure element (obligatory for RESTRICTED information)

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
- All external interfaces can be restricted or disabled (e.g. limit USB capabilities or enable "No Spy Mode" to deactivate microphone and camera)

Central management

The included management system offers both EMM/MDM functionality and an enterprise app store. Following central company guidelines, it can be used exclusively or in combination with conventional app stores.

- Management functionality for central organization of the corporate network
- Device, policy and configuration management
- Full public key infrastructure with automated distribution of software certificates
- OTA distribution of all updates to all or specific devices at the touch of a button
- 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" environments on a single device
- Automatic installation of apps via enterprise app store
- Compatible with all Android apps
- Central management (MDM)

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

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

PD 3607.5802.32 | Version 04.00 | February 2020 (mh)
R&S®Trusted Mobile
Data without tolerance limits is not binding | Subject to change

3607580232

3607.5802.32 04.00 PDP 1 en