Rohde & Schwarz Cybersecurity

R&S®TRUSTED MOBILE

Mobile Geräte wie Smartphones und Tablets sind unverzichtbarer Bestandteil des beruflichen Alltags. Dies bedeutet, dass über diese mobilen Endgeräte immer mehr sensible firmeninterne Daten verfügbar sind. Durch die Mobilität entstehen aber auch ganz neue Gefahren:

- Ungewollte Datenabflüsse, z. B. durch Apps und Schadsoftware
- Datenmanipulationen, z. B. durch Trojaner
- Unerlaubte Unternehmenszugriffe, z. B. durch verlorene oder gestohlene Geräte

Alle bisherigen kommerziellen Sicherheitsmechanismen wie MDM- oder containerbasierte Sicherheitsanwendungen bieten hier keinen ausreichenden Schutz. Doch wenn adäquate Sicherheitsmaßnahmen Voraussetzung für den Einsatz mobiler Geräte in Unternehmen sind, ist R&S®Trusted Mobile die Lösung.

Produkt-Flyer
Version 04.00

ROHDE&SCHWARZ
Make ideas real

Gehärtetes Android ohne Hintertüren

R&S®Trusted Mobile ist ein gehärtetes Android ohne Backdoor. Die Grundlage bildet ein gehärteter Sicherheitskern, der durch zusätzliche Sicherheitsmechanismen, -dienste und feingranulare Zugriffsregeln vor Angriffen wie Zero-Day-Exploits schützt. Das Rohde&Schwarz Cybersecurity-Sicherheitskonzept, welches auf R&S®Trusted Mobile Anwendung findet, ermöglicht die Kontrolle sämtlicher Datenflüsse – und falls erforderlich, deren Blockierung. R&S®Trusted Mobile unterstützt die Verwendung von Smartcards zum Schutz von Langzeitschlüsseln optimal. R&S®Trusted Mobile ist Android kompatibel, so dass übliche Android-Apps verwendet werden können.

Sicherer Zugriff auf Unternehmensressourcen

Im Rahmen des Sicherheitskonzepts von Rohde&Schwarz Cybersecurity ist das Smartphone in zwei virtuelle Bereiche getrennt. Diese Trennung zwischen „Restricted“ und „Open“ ermöglicht den sicheren Zugriff auf Unternehmensressourcen: So können Anwendungen aus dem „Restricted“-Bereich nur über einen sicheren VPN-Tunnel auf Ressourcen des Unternehmens wie E-Mail, Kontakte, Kalender und Intranet zugreifen und untereinander Daten austauschen. Optional kann auch der „Restricted“-Bereich über die sichere Unternehmensinfrastruktur auf das Internet zugreifen. Durch eine sichere Verschlüsselung aller Daten, die zwischen dem Smartphone und dem Unternehmensnetzwerk ausgetauscht werden, sind sie vor unberechtigtem Zugriff geschützt.

R&S®Trusted Mobile ist mit seinen Sicherheitsfunktionen die ideale Plattform für Applikationen, die zum Beispiel gesicherte, verschlüsselte Sprachkommunikation oder Messenger-Dienste anbieten. Je nach Anwendungsbereich des Kunden unterstützt R&S®Trusted Mobile auch öffentlich zugängliche App-Stores direkt im „Open“-Bereich. Dadurch bleibt die volle Flexibilität für den Benutzer erhalten und die Sicherheit des Unternehmensnetzwerkes ist gewährleistet.

Varianten

R&S®Trusted Mobile wird entsprechend der Sicherheitsbedürfnisse in den folgenden Varianten angeboten:

- **R&S®Trusted Mobile – NfD,** für VS-NfD-Anwendungen
- **R&S®Trusted Mobile – Pooling,** für Multi-User-Szenarien
- **R&S®Trusted Mobile – Enterprise,** für Unternehmen und Behörden

Basiseigenschaften

- Gehärteter Sicherheitskern
- Trennung von privaten Daten und Anwendungen sowie Unternehmensressourcen (z. B. getrennte Adressbücher, damit Apps, wie z. B. WhatsApp, nicht auf Firmenkontaktdaten zugreifen können)
- Optionales Secure-Element (bei VS-NfD obligatorisch)

Sicherheit

- Gehärteter Sicherheitskern mit Mandatory Access Control und Type Enforcement
- Zentrale Kontrolle der installierten Apps
- Zertifikatbasiertes VPN über IPsec-Tunnel zu Unternehmensressourcen
- ECDH und ECDSA bis 512/521 Bit (Software oder Smartcard)
- Device-Verschlüsselung mittels AES-XTS 256 Algorithmus
- Alle Schnittstellen nach außen können auf Wunsch eingeschränkt oder deaktiviert werden (z. B. limitierte USB-Nutzung oder „No Spy Mode“ zur Deaktivierung des Mikrofons und der Kamera)

Zentrales Management

Das hauseigene Managementsystem bietet sowohl EMM/MDM-Funktionen, als auch einen Enterprise App-Store. Über diesen können, gemäß zentraler Richtlinien, Android-Apps ausschließlich oder in Kombination mit einem herkömmlichen App-Store installiert werden.

- Managementfunktionen zur zentralen Organisation des Unternehmensnetzwerkes
- Device-, Konfigurations- und Policy-Management
- Vollständige PKI mit automatischer Verteilung von Softwarezertifikaten
- Verteilung sämtlicher Updates auf alle oder einzelne Geräte per Knopfdruck
- Anbindung an Verzeichnisdienste (LDAP, AD)
- Unterstützung von existierenden CAs
- Zentrale Auswahl, Zertifizierung und Verteilung von Unternehmens-Apps.

Komfort

- Trennung in „Restricted“- und „Open“-Bereich auf dem gleichen Gerät
- Apps über Enterprise App-Store automatisch installierbar
- Kompatibel mit Android-Apps
- Zentrales Management (MDM)

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
Info: +49 30 65884-222
E-Mail: cybersecurity@rohde-schwarz.com
www.rohde-schwarz.com/cybersecurity

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

R&S® ist eingetragenes Warenzeichen der Rohde&Schwarz GmbH&Co. KG
Eigennamen sind Warenzeichen der jeweiligen Eigentümer
PD 3607.5802.31 | Version 04.00 | September 2019 (sch)
R&S®Trusted Mobile
Daten ohne Genauigkeitsangabe sind unverbindlich | Änderungen vorbehalten
© 2016 - 2019 Rohde&Schwarz Cybersecurity GmbH | 81671 München

3607580231

3607.5802.31 04.00 PDP 1 de