R&S®Trusted Mobile

Niveau de sécurité supérieur pour vos smartphones et tablettes

La plateforme Android R&S®Trusted Mobile offre aux entreprises et aux institutions publiques une sécurisation des smartphones et des tablettes.

En entreprise aussi, smartphones et tablettes sont devenus partie intégrante du quotidien. La perte ou le vol de ces appareils nomades est, elle aussi, chose courante et peut aboutir à l'accès de personnes non autorisées à vos données sensibles, voire à l'ensemble du réseau de l'entreprise. Ce risque fait de l'utilisation des appareils mobiles le maillon faible de tout concept de sécurité d'entreprise. Les cyberattaques de type zero-day choisissent souvent pour cibles des réseaux d'entreprise afin d'accéder à des données sensibles ou aux clés cryptographiques. Jusqu'à présent, aucune des solutions de MDM ou de conteneurisation présentes sur le marché n'assure une protection à la hauteur de ces menaces.

Des mesures de sécurité adéquates sont indispensables dans le cadre de l'utilisation d'appareils mobiles dans les entreprises.

Classement « Restricted » ou « Open » des données et applications

La pièce maîtresse de R&S®Trusted Mobile est son noyau de sécurité renforcé par des mécanismes de sécurité d'avant-garde, des services sécurités ainsi que des règles d'accès à granularité fine assurant la meilleure protection contre les attaques de type zero-day. R&S®Trusted Mobile est, en option, compatible avec les Smartcards afin de protéger les clés privées.

Entièrement compatible avec Android, R&S®Trusted Mobile permet l'installation de toute application Android dans chacun des deux compartiments de sécurité.

ROHDE&SCHWARZ
Cybersecurity

Dépliant produit | Version 01.00

Accès sécurisé aux données d'entreprise

La séparation entre une zone « Restricted » et une zone « Open » permet un accès sécurisé aux ressources de l'entreprise. Les applications de la zone « Restricted » peuvent échanger des données entre elles et accéder aux ressources de l'entreprise telles que les e-mails, les contacts, les calendriers et l'intranet via un tunnel VPN sécurisé. En complément, l'espace « Open » peut accéder à l'intranet via un pare-feu d'entreprise qui filtre les contenus dangereux. Toutes les données échangées par les smartphones et le réseau de l'entreprise sont protégées contre tout accès non autorisé par un cryptage sécurisé.

R&S®Trusted Mobile assure aussi le chiffrement des appels téléphoniques vers le bureau central et les smartphones de l'entreprise, et est compatible avec la solution Rohde&Schwarz Cybersecurity voice and chat. La flexibilité d'un smartphone est toujours préservée. Dans l'espace « Open », les utilisateurs peuvent installer leurs applications prédéfinies (par exemple via Google Play Store), sans affecter la sécurité du réseau de l'entreprise.

En parallèle, R&S®Trusted Objects Manager propose des fonctionnalités de gestion des périphériques, des fonctionnalités EMM et MDM et un App-Store d'entreprise. Ce dernier permet de mettre à disposition aux utilisateurs des applications répondants à des exigences définies en amont par l'administrateur. Les applications sont accessibles depuis l'App-Store d'entreprise ou par le biais des plateformes d'applications habituelles.

Caractéristiques principales

- Noyau de sécurité renforcé pour Android 6
- Séparation des données d'entreprise et des données et applications privées
- Chiffrement intégral des données du périphérique
- En option : prise en compte des Smartcards

Sécurité

- Noyau de sécurité renforcé avec Contrôle d'accès obligatoire (MAC) et Type Enforcement
- Contrôle centralisé des applications installées
- Tunnel VPN IPsec avec certificat pour l'accès aux données d'entreprise
- Chiffrement ECDH et ECDSA jusqu'à 512/521 bits (sur logiciel ou Smartcard)
- Chiffrement des périphériques par algorithme AES-XTS 256
- « No Spy Mode » pour désactiver le micro et la caméra

Gestion centralisée

- R&S®Trusted Objects Manager (TOM) pour la gestion centralisée du réseau d'entreprise
- Outil de gestion MDM et de gestion des configurations et des procédures de sécurité
- Infrastructure à clés publiques (PKI) intégrale avec distribution automatique des certificats logiciels
- Mises à jour OTA (Over the Air) possibles sans restriction
- Liaison aux services d'annuaire (LDAP et AD)
- Prise en charge des autorités de certification existantes
- Sélection, certification et distribution centrale des applications d'entreprise

Ergonomie

- Division en compartiments « Restricted » et « Open » sur un seul et même périphérique
- Applications délivrables depuis l'App-Store d'entreprise
- Compatible avec toutes les applications Android

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Allemagne
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 3607.5802.33 | Version 01.00 | mai 2018 (sch)
R&S®Trusted Mobile
Données sans tolérance : sans obligation | Sous réservé de modification

3607580233

3607.5802.33 01.00 PDP 1 fr