ROHDE&SCHWARZ
Make ideas real

NATIVER DATENSCHUTZ FÜR DEN EINSATZ MIT iPHONES UND iPADS DURCH R&S MOBILE CONNECTIVITY

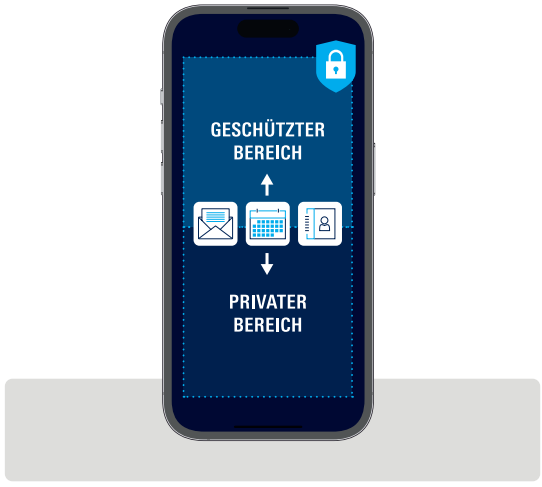
Komplettlösung für den zuverlässigen Schutz sensibler Unternehmensdaten bei der Nutzung von Mobilgeräten

Immer mehr Unternehmen ermöglichen ihren Mitarbeitern mobiles Arbeiten - vorausgesetzt, sie verfügen über eine Internetverbindung und ein mobiles Endgerät. Diese neue Flexibilität stellt IT-Verantwortliche bei der Gewährleistung von Datensicherheit und -schutz vor große Herausforderungen. Hier sind geeignete Technologien und Rahmenbedingungen notwendig.

Die Technologie Indigo von Apple ist eine neue, vom Gerätehersteller entwickelte und vom BSI geprüfte Sicherheitslösung für handelsübliche iPhones und iPads. Die R&S Mobile Connectivity-Lösung erfüllt auch bei gemischter dienstlicher und privater Nutzung höchste Anforderungen an Datensicherheit und Datenschutz bis hin zum staatlichen Geheimschutz. Gleichzeitig ist sie besonders benutzerfreundlich, da sie bei der Verarbeitung sensibler Unternehmensdaten erstmalig auch die Nutzung der vorinstallierten Standard-Apps für E-Mail, Kalender und Kontakte ermöglicht.

Herkömmliche Lösungen arbeiten meist mit Containern und komplizierten Authentifizierungsprozessen, die bestehenden Workflows im Weg stehen. Sicherheit wird dann von den Nutzern schnell als Belastung empfunden. Mit der neuen R&S Mobile Connectivity-Lösung können Nutzer ihr iPhone nativ, das heisst wie gewohnt, nutzen, ohne dass die Gefahr besteht, dass sensible Daten abfließen. Das zentrale Managementsystem ermöglicht außerdem eine flexible und unabhängige Administration sämtlicher Geräte und Zertifikate inkl. Rollout.

Gemeinsam mit unserem strategischen Partner agilimo Consulting liefern wir, die Rohde & Schwarz Cybersecurity für Ihr Projekt alles aus einer Hand für eine zugeschnittene und hochsichere Kommunikationsinfrastruktur.



BSI-bestätigte Plattformsicherheit, die weit über die bisheriger MDM-Lösungen hinausgeht

Maximale Benutzerakzeptanz durch Nutzung der Standard-Apps für E-Mail, Kalender und Kontakte - keine Containerlösung

Nutzung handelsüblicher Apple-Mobilgeräte, Weiterverkauf nach Nutzungsende möglich

R&S MOBILE CONNECTIVITY-LÖSUNGSKOMPONENTEN

Apps für hochsicheres Arbeiten

Die vorinstallierten Standard-System-Apps Mail, Kalender und Kontakte bieten native Unterstützung für Indigo. Optionale Erweiterungen sind z.B. ein abgesicherter Intranet-Browser und ein sicherer Messenger, der auch Audio/Video-Anrufe und -Konferenzen unterstützt.

Mobilgeräte „as a Service“

Wir bieten das gesamte Life-Cycle-Management der Mobilgeräte an:

- Beschaffung
- Konfiguration / Staging
- Rollout
- Schutzbrief
- Verwaltung / Abrechnung
- Rückführung
- Zertifizierte Datenlöschung

Mobile Device Management

Zentrale Endgeräte-Verwaltung:

- Registrierung von Mobilgeräten im Apple Business Manager als betreute Geräte im „Supervised Mode“
- Verwaltung über MDM-Schnittstelle, wobei die Geräteregistrierung beim MDM automatisch erfolgt
- Durchsetzung zentraler Konfigurations- und Sicherheitsvorgaben für Indigo, z.B. für VPN- und Drahtlosverbindungen, Aktivierung der Separation, etc.

Steuerung per Fernzugriff:

- Konfiguration von Geräten auf Ebene von Gerät, Gerätegruppe, Nutzer oder Nutzergruppe
- Organisationsweite Installation von Apps
- Durchsetzung von Unternehmensrichtlinien im Umgang mit Mobilgeräten, Daten und Apps und Einhaltung überwachen
- Löschung oder Sperrung von Geräten per Fernzugriff
- Bestandsaufnahme von Geräten, Softwareversionen, installierten Apps etc.

VPN-Gateways

Die eingesetzten **R&S®Trusted VPN Gateways** sind IPsec-basierte Verschlüsseler zur Sicherung der Vertraulichkeit und Integrität von Daten bei der Übertragung über IP-Netze mit BSI-Geheimschutz Zulassung. Die Layer-3-Verschlüsselung ist durch die Anzahl und die Variante der Gateways skalierbar.

Zentrales VPN-Managementsystem mit Indigo-Erweiterung

Der **R&S®Trusted Objects Manager** ist das zentrale Managementsystem zur Verwaltung und Konfiguration der VPN-Gateways. Es ermöglicht u.a. eine flexible Nutzer- und Rechteverwaltung und enthält eine integrierter PKI/CA sowie eine optionale Schnittstelle zu LDAP-Verzeichnisdiensten, z.B. AD.

Eine spezielle Erweiterung für die R&S Mobile Connectivity-Lösung ermöglicht die automatisierte Verteilung der Mobilgeräte-Zertifikate bei:

- Rollout der Lösung inkl. Verifikation der Gerätezuordnung zu einem Benutzer in der Organisation
- Sperrung einzelner Zertifikate im Fall von Geräteverlusten
- Austausch von Zertifikaten nach Sicherheitsvorfällen
- Automatischen Sperrungen, wenn Mitarbeiter ausscheiden und Erneuerung von Zertifikaten
- Keine weitere, externe PKI/CA benötigt, aufgrund zentraler, automatisierter Verteilung
- Deutliche Reduzierung von Administrationsaufwendungen

Vorteile für Organisationen mit besonderem Schutzbedarf:

- Die R&S Mobile Connectivity-Lösung ist eine native Security-Lösung für iPhone und iPads auf Geräteebene
- Keine ergänzenden Apps oder dritte Software zwingend nötig, aber möglich
- Hochsichere Nutzung nach VS-NfD-Standard
- Lösung ist geeignet für NIS2 EU-Richtlinie
- DSGVO konform
- Planungssicherheit durch 5 Jahre Bereitstellung von Security-Patches nach End-of-Sale eines Modells
- Hohe Einsparpotenziale durch längere Nutzung der Geräte
- Private Nutzung der Endgeräte möglich Arbeiten in einer modernen und gewohnten (Geräte-)Umgebung

Für wen ist die R&S Mobile Connectivity-Lösung geeignet?

Privatwirtschaft

- Energieversorger
- Rüstung
- Kritische Infrastruktur
- Bankwesen
- Gesundheits-einrichtungen
- Firmen mit hohem Schutzbedarf

Öffentlicher Sektor

- Behörden
- Verwaltung (Bund, Länder, Kommunen)
- Polizei
- Einsatzkräfte
- DRK, THW, etc.

Implementierung & Systemintegration:

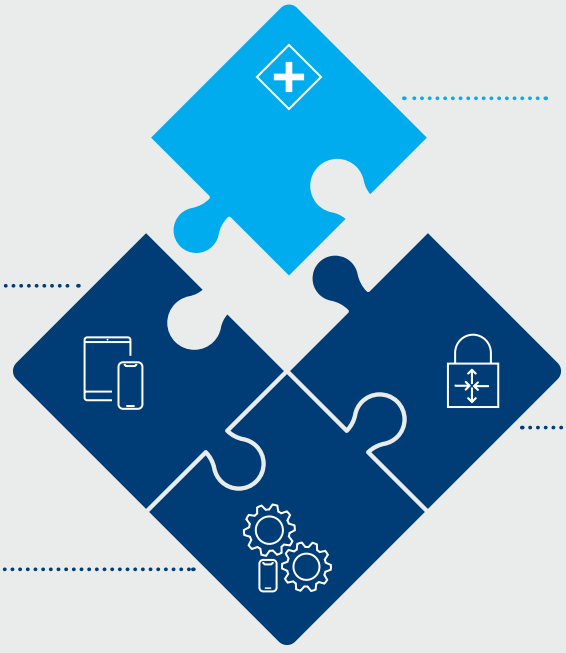
- Kick-off + Abstimmungen vor Ort nach Bedarf
- Integrationskonzept Kundenumgebung
- SW-Installation MDM-Server
- Integrationsunterstützung VPN-Gateways inkl. Managementsystem
- Integration in Apple Business Manager, u.a. Device Enrolment Program
- Testbetrieb, Einweisung der Kunden-administratoren und Abnahme
- Dokumentation der Indigo-konformen Mobilgeräte-Konfiguration

Managed Service:

- 24/7 Betrieb aller Indigo-relevanten Systeme
- Monitoring sämtlicher Teilsysteme
- Remote Patch-Management/-Installation und System Upgrades

Support:

- Dokumentation und Training für 1st Level Support/ Service Help Desk des Kunden
- 2nd Level Support für Betrieb von MDM und VPN-Gateway
- Ggf. Koordinierung von 3rd Level Support durch Hersteller



+ Automat. Zertifikatsverteilung
+ Alternatives Routing
+ Optionale Erweiterungen
+ Training & Support
+ Managed Service

BSI-konform konfigurierte iPhones / iPads mit Apple Enterprise OS Support

VPN-Gateway mit BSI-Zulassung

Geeignetes Mobile Device Management

Sie haben Fragen?

Wir freuen uns über
Ihre Kontaktaufnahme
per E-Mail an

cybersecurity@rohde-schwarz.com

oder telefonisch unter +49 30 65884-222

Rohde&Schwarz Cybersecurity GmbH
Mühldorfstraße 15 | 81671 München
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 3608.9276.31 | Version 02.00 | April 2024 (dh)

3608927631
3608.9276.31 02.00 PDP 1 de