



# NATIVE DATA PROTECTION FOR USE ON iPHONES AND iPADS WITH R&S®COMSEC SUPPORTING INDIGO

## All-in-one-solution for the reliable protection of sensitive company data when using mobile devices

More and more companies are enabling their employees mobile work – provided they have an internet connection and a mobile device. This new flexibility means that IT managers face major challenges in ensuring data security and data protection. This requires suitable technologies and framework conditions.

Apple's indigo technology is a new security solution developed by the device manufacturer and approved by the German Federal Office for Information Security (BSI, Bundesamt für Informations-sicherheit) for commercial off-the-shelf iPhone and iPad devices. Even in the case of mixed use (private and business), the R&S®ComSec supporting indigo solution fulfills the highest demands on data security and data protection up to the level of nationally classified information. At the same time, it is particularly user-friendly, since, for the first time, it allows using pre-installed standard apps for email, calendar and contacts for processing sensitive corporate data.

Traditional solutions usually work with containers and complicated authentication processes that impede existing workflows. Then, security is quickly perceived as a burden by the users. With the new R&S®ComSec supporting indigo solution, users can use their iPhone natively, i.e. as usual, without the risk of sensitive data being leaked. The central management system also allows flexible and independent administration of all devices and certificates, including rollout.

Together with our strategic partner agilimo Consulting, we at Rohde & Schwarz Cybersecurity supply everything for your project from a single source to ensure a tailored and high-security communications infrastructure.



**BSI-approved platform security**  
that by far outperforms previous MDM solutions



**Maximum user acceptance**  
through the use of standard apps for email, calendar and contacts – no container solution



**Use of commercial off-the-shelf Apple mobile devices**, resale possible after end of use

# R&S® COMSEC SUPPORTING INDIGO SOLUTION COMPONENTS

## Apps for highly secure work

The pre-installed default system apps mail, calendar and contacts provide native support for Apple indigo. The optional extensions are, e.g., a secured intranet browser and a secure messenger, which also supports audio/video calls and conferences.

## Mobile devices "as a service"

We offer the entire lifecycle management of the mobile devices:

- ▶ Procurement
- ▶ Configuration / staging
- ▶ Rollout
- ▶ Service pack
- ▶ Administration / settlement
- ▶ Return of the products
- ▶ Certified secure data deletion

## Mobile Device Management

Central endpoint device management:

- ▶ Registration of mobile devices in Apple Business Manager as supervised devices in "supervised mode".
- ▶ Management via MDM interface, where device registration with the MDM takes place automatically
- ▶ Enforcement of central configuration and security specifications for Apple indigo, e.g. for VPN and wireless connections, activation of separation, etc.

Control via remote access:

- ▶ Configuration of devices on the level of device, device group, user or user group
- ▶ Organization-wide installation of apps
- ▶ Monitoring the enforcement and compliance of corporate policies regulating the handling of mobile devices, data and apps
- ▶ Deletion or locking of devices via remote access
- ▶ Inventory of devices, software versions, installed apps, etc.

## VPN gateways

**R&S®Trusted VPN Gateways** used are IPsec-based encryptors for securing confidentiality and integrity of data when transferring data via IP networks with BSI authorization for Communications and Information Systems (CIS). The layer-3 encryption is scalable through the amount and the variant of the gateways.

## Central VPN management system with Apple indigo extension

**R&S®Trusted Objects Manager** is the central management system for management and configuration of the VPN gateways. It allows, among other things, flexible user and rights management and contains an integrated PKI/CA as well as an optional interface to LDAP directory services, e.g. AD.

A dedicated extension for the R&S®ComSec supporting indigo solution allows the automated deployment of mobile device certificates when:

- ▶ Rolling out the solution including verification of device assignment to a user in the organization
- ▶ Revocation of single certificates in the case of device failures/losses
- ▶ Exchange of certificates after security incidents
- ▶ Automated blocking when employees leave and renewing of certificates
- ▶ No further, external PKI/CA required, thanks to automated central deployment
- ▶ Significant reduction of administrative expenses



## Benefits for organizations with special security needs:

- ▶ The R&S®ComSec supporting indigo solution is a native security solution for iPhone and iPad on device level
- ▶ No complementary apps or third party software absolutely necessary, but possible
- ▶ Highly secure use according to RESTRICTED standard (VS-NfD)
- ▶ Solution is suitable for EU directive NIS2
- ▶ GDPR compliant
- ▶ Planning security due 5-year provision of security patches after end-of-sale of a model
- ▶ High saving potential due to prolonged use of the devices
- ▶ Private use of endpoint devices possible, working in a familiar and state-of-the-art (device) environment

## Implementation & system integration:

- ▶ Kick-off + on-site reconciliations as required
- ▶ Integration concept for client environment
- ▶ SW installation MDM server
- ▶ Integration support VPN gateway incl. management system
- ▶ Integration in Apple Business Manager, among others Device Enrolment Program
- ▶ Test operation, briefing of the customer administrators and acceptance
- ▶ Documentation of the Apple indigo-compliant mobile device configuration

## Who is the R&S®ComSec supporting indigo solution suitable for?

### Private sector

- ▶ Energy suppliers
- ▶ Armament
- ▶ Critical infrastructure
- ▶ Banking sector
- ▶ Healthcare facilities
- ▶ Companies with high security needs

### Public sector

- ▶ Authorities
- ▶ Administration (Federal government, states, communities)
- ▶ Police
- ▶ Emergency personnel
- ▶ German Red Cross (DRK), Technical Relief Service (THW) etc.

## Managed Service:

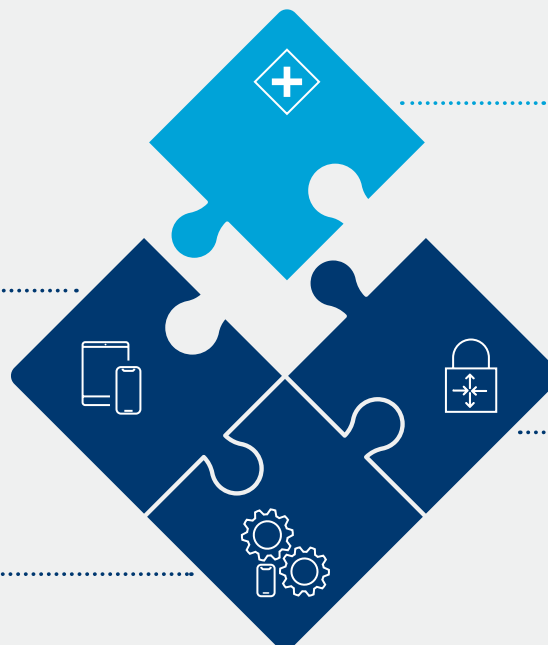
- ▶ 24/7 operation of all Apple indigo-relevant systems
- ▶ Monitoring of all subsystems
- ▶ Remote patch management/installation and system upgrades

## Support:

- ▶ Documentation and training for 1st level support/ service help desk of client
- ▶ 2nd level support for operation of MDM and VPN gateway
- ▶ If needed, coordination of 3rd level support through manufacturer

**BSI-compliantly configured iPhone / iPad devices with Apple Enterprise OS support**

**Suitable Mobile Device Management**



**+ Automat. certificate deployment**  
**+ Alternative routing**  
**+ Optional extensions**  
**+ Training & support**  
**+ Managed Service**

**VPN gateway with BSI approval**

**You have questions?**



We look forward  
to receiving your email:

[cybersecurity@rohde-schwarz.com](mailto:cybersecurity@rohde-schwarz.com)

Or call us: +49 30 65884-222

**Rohde & Schwarz Cybersecurity GmbH**

Muehldorfstrasse 15 | 81671 Munich, Germany

Info: +49 30 65884-222

Email: [cybersecurity@rohde-schwarz.com](mailto:cybersecurity@rohde-schwarz.com)

[www.rohde-schwarz.com/cybersecurity](http://www.rohde-schwarz.com/cybersecurity)

**Rohde & Schwarz GmbH & Co. KG**

[www.rohde-schwarz.com](http://www.rohde-schwarz.com)

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG

Trade names are trademarks of the owners

PD 3608.9276.32 | Version 03.00 | July 2024 (dh)

R&S®ComSec supporting indigo

Data without tolerance limits is not binding | Subject to change

© 2024 Rohde & Schwarz Cybersecurity GmbH | 81671 Munich, Germany