ROHDE&SCHWARZ

Make ideas real

NATIVE DATA PROTECTION FOR USE ON iPHONES AND iPADS WITH 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.

Indigo is a new security solution developed by the device manufacturer and approved by the German Federal Office for Information Security (BSI, Bundesamt für Informationssicherheit) for commercial off-the-shelf iPhones and iPads. Even in the case of mixed use (private and business), the 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 all-in-one 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, we at Rohde & Schwarz Cybersecurity supply everything for your Indigo project from a single source to ensure a tailored high-security communications infrastructure.

PROTECTED AREA
PRIVATE AREA

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

SOLUTION COMPONENTS

Apps for highly secure work

The pre-installed default system apps mail, calendar and contacts provide native support for 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 Indigo, e.g. for VPN and wireless connections, activation of separation

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 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 Indigo 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, 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:

- Indigo is a native security solution for iPhones and iPads on device level
- No complementary apps or third party software needed
- Highly secure use according to RESTRICTED standard (VS-NfD)
- Solution is suitable for EU directive NIS2
- GDPR compliant
- Planning security due to 6-year manufacturer's warranty for Indigo
- 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

For whom is the product suitable as a security solution?

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.

Implementation & system integration:

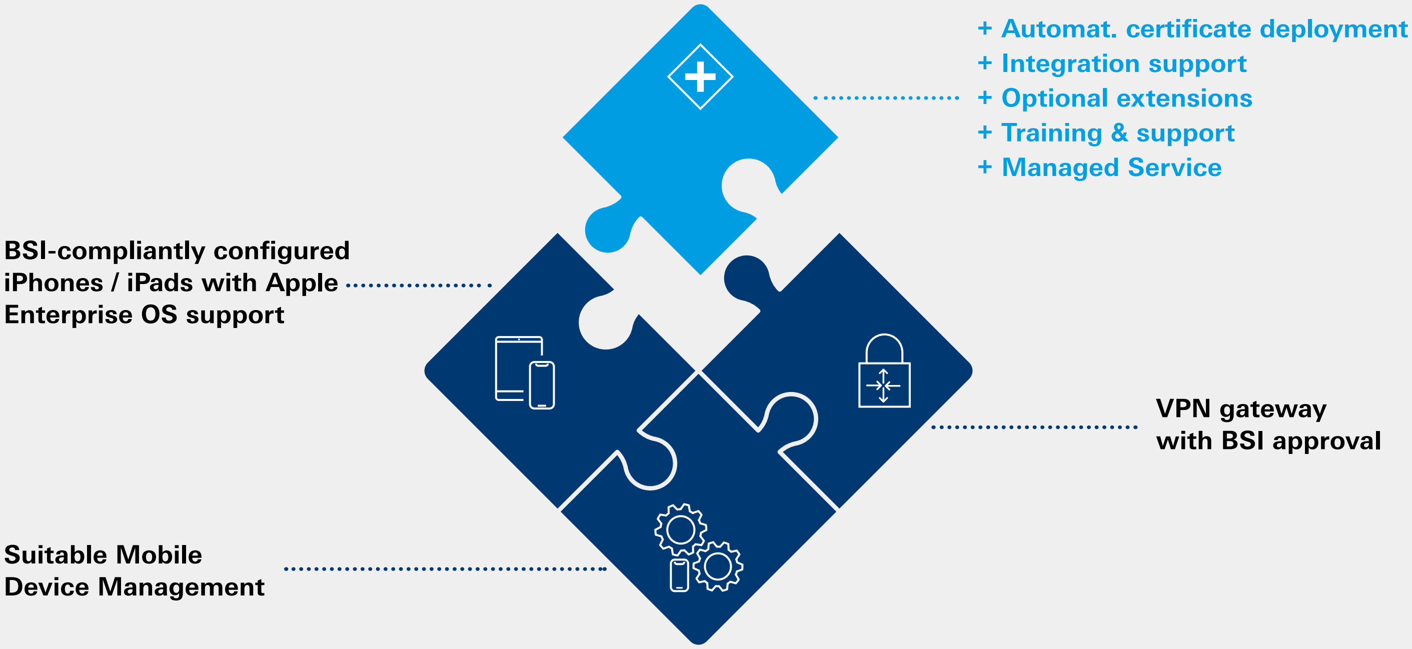
- Kick-off + on-site reconciliations as required
- Integration concept for client environment
- SW installation MDM server
- Integration support VPN gateway incl. management system
- Integration in Apple Business Manager, among others Device Enrolment Program
- Test operation, briefing of the customer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

Managed Service:

- 24/7 operation of all 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


+ Automat. certificate deployment
+ Integration support
+ Optional extensions
+ Training & support
+ Managed Service
BSI-compliantly configured iPhones / iPads with Apple Enterprise OS support
VPN gateway with BSI approval
Suitable Mobile Device Management

You have questions?

We look forward
to receiving your email:

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
www.rohde-schwarz.com/cybersecurity

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

PD 3608.9276.32 | Version 01.00 | October 2023 (NP)
Native data protection for use on iPhones and iPads with Indigo
Data without tolerance limits is not binding | Subject to change

3608927632

3608.9276.32 01.00 PDP 1 de