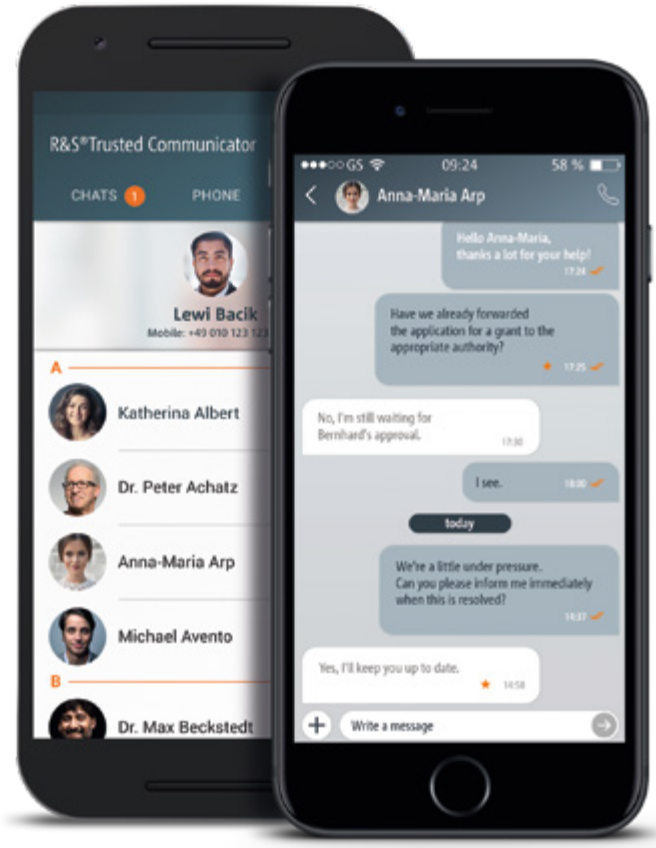
R&S®Trusted Communicator

For iOS and Android: secure messaging and voice encryption



Messaging applications have become indispensable in everyday life. Private sector and public sector organizations do not want to do without them. However, security aspects are often neglected. Phone calls should be tap-proof as well. Data protection (privacy) is another major issue with many conventional applications. Here, custom configuration is only possible to a limited extent.

R&S®Trusted Communicator is a communications and collaboration platform that delivers highly secure messaging along with voice encryption in a single app. The solution provides encryption of all data, plus you can easily implement it in your own public key infrastructure (PKI). It is thus ensured that employees and staff always communicate with the person(s) they really want to. Man-in-the-middle attacks are thwarted. R&S®Trusted Communicator protects your sensitive data and messages using end-to-end encryption. We offer you state-of-the-art cryptographic technology and a single user interface for iOS and Android – customized for the user's platform. R&S®Trusted Communicator also perfectly complements our Android based R&S®Trusted Mobile platform.

Security by design

With R&S®Trusted Communicator, security is built in already at the development stage. Secure exchange of confidential information is the theme that rules all aspects and phases of the application. R&S®Trusted Communicator was created for cryptographic agility to counter the challenges of quantum computing. This means that cryptographic algorithms and standards can be updated promptly without requiring critical changes to digital certificates, for example. This protects you against the risk of obsolescence, i.e. that cryptographic algorithms may no longer provide adequate security in the future.

ROHDE&SCHWARZ
Cybersecurity

Multi-platform client for multi-user voice and chat communications

R&S®Trusted Communicator combines secure instant messaging and encrypted telephony in a single app. You can send all types of information – text messages, emojis, file attachments, your location data – with end-to-end encryption and only readable by authorized persons.

You can start multi-user chats at any time and make conference calls whenever you wish. Phone calls are also encrypted locally on your smartphone, using the AES 256 encryption algorithm, and decrypted only after arriving on the smartphone of your contact.

Separate telephone directory for compliance with data protection (privacy) standards

Many messenger apps access all data in the telephone directory – including private contacts – with the consequence that addresses as well as metadata (location data, etc.) from your smartphone or tablet end up on external servers. This is different with R&S®Trusted Communicator. The app manages contacts from diverse sources and accesses a secured, encrypted telephone directory that is separated from your private contacts.

Supports NATO SCIP and SNS cryptographic standards

R&S®Trusted Communicator has the SCIP crypto protocol integrated in the standard version. Support of the SNS protocol is also possible; this protocol is based on TETRA-BOS cryptography and extends NATO SCIP.

Management using MDM and EMM tools

R&S®Trusted Communicator can be administered with all common mobile device management (MDM) and enterprise mobility management (EMM) appliances that support the AppConfig standard. We also offer our own management appliance called R&S®Trusted Objects Manager.

Optimized user interface for trust and acceptance

All processes are optimized to match the target user platform. As a result, iOS and Android users will immediately feel at home with R&S®Trusted Communicator, just as with familiar communications and collaboration apps.

Additional option: your own compatible infrastructure system

The R&S®Trusted Communications Server gateway provides you with an infrastructure system compatible with R&S®Trusted Communicator in case you have no compatible system of your own.

Features

Secure phone calls:	**Push notification services and power consumption:**
▪ Extension to maintain super wideband attribute (27 kbit) ▪ AES256-GCM for integrity protection ▪ SIPS based on TLS 1.2+	▪ Support of push notification services (iOS/Android) ▪ Stealth push notification: activities remain with the user ▪ Optimized power consumption thanks to push notifications
Secure chatting/messaging:	**Mobile device management (MDM):**
▪ End-to-end encryption using AES-256 – XMPP-OTR protocol ▪ Sending text messages, file attachments, geolocation data ▪ Multi-user chats: no inherent limit restricting number of users ▪ Message broadcasting by privileged users (moderators)	▪ AppConfig support: AppConfig for MDM/EMM based configurations ▪ R&S®Trusted Objects Manager support
Secure contacts:	**Cryptographic capabilities:**
▪ Managing contacts, e.g. from active directory, using R&S®Trusted Objects Manager or MDM/EMM appliance ▪ Local contacts remain in secure telephone directory ▪ Automated cross-check of contacts – no personal data stored in backend	▪ Cryptographic agility ▪ Implementation of latest encryption algorithms ▪ SCIP protocol: meets approval requirements ▪ SNS protocol: certification by German Federal Office for Information Security (BSI) pending

Rohde&Schwarz Cybersecurity GmbH
Muehldorfstrasse 15 | 81671 Munich, Germany
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 5215.8058.32 | Version 01.00 | June 2018 (sch)
R&S®Trusted Communicator

5215805832

5215.8058.32 01.00 PDP 1 en