Secure COM
by Virtual Solution

SecureCOM

Data Sheet

Virtual Solution AG

May 2021

Version 1.0

SecureCOM by Virtual Solution

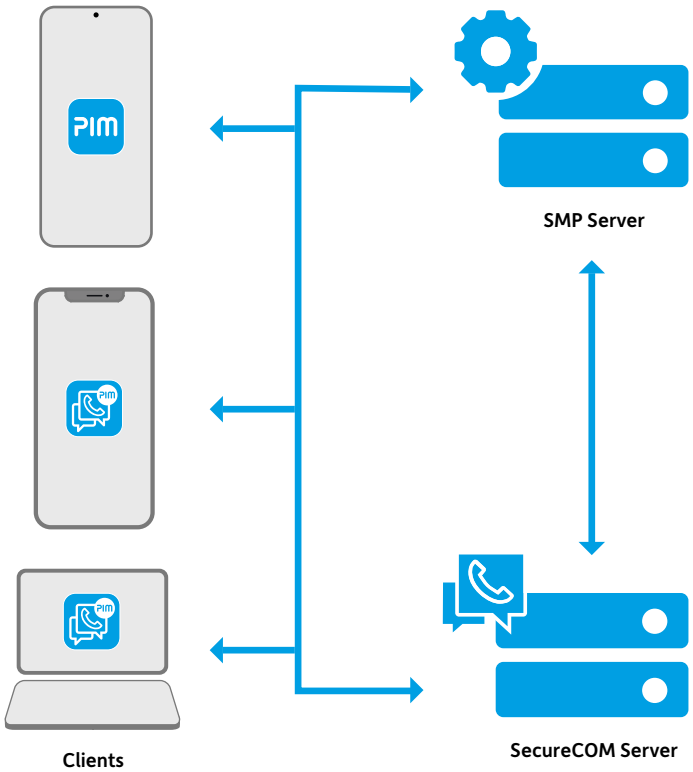
What is SecureCOM?

SecureCOM provides you with everything you need for secure instant messaging for business and work.
The messenger enables employees to exchange information both quickly and securely, while also facilitating encrypted telephony.
SecureCOM is just as intuitive to handle as users of messengers in the private environment have come to expect.
All essential, business-critical functions are available.
In addition, there are functions specifically designed for authorities, for instance a map-based location display of employees on duty in the field. Users communicate via their preferred smart phones or tablets, or, alternatively, use the messenger on their PCs. SecureCOM is available for all common mobile and desktop operating systems.

A version of SecureCOM is also provided as an integrated component of the communication application SecurePIM. Within a protected container, this application grants users secure access to emails, calendar, photos and documents, and allows them to share this content directly in the chat, without having to exit the application. This not only increases the security of their data but is also highly convenient for users.

Components

+ SecureCOM Client for mobile devices and desktop
+ SecureCOM Server (cloud or onpremises)
+ Management Portal SMP for user administration



SecureCOM by Virtual Solution

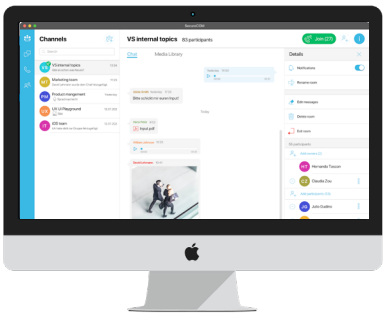
SecureCOM Client

The functions provided by SecureCOM are

+ End-to-end encrypted messages (text, speech, video, multimedia, files)
+ End-to-end encrypted messages with self-destruct option
+ End-to-end encrypted voice and video calls
+ End-to-end encrypted teleconferences
+ End-to-end encrypted group chat
+ End-to-end encrypted location sharing
+ End-to-end encrypted real-time location sharing
+ Private SecureCOM address book

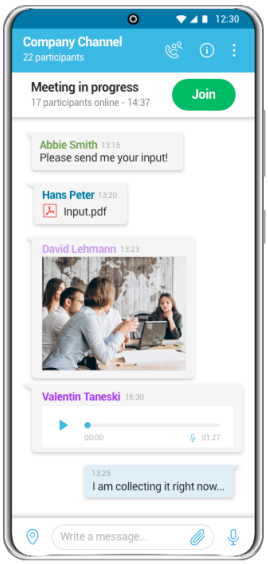
The SecureCOM App is available for both iOS and Android devices. The rollout process is quick and easy, as the employees simply download the app from the Apple® App Store or Google Play™ and register themselves in the SecureCOM App using their personal credentials. Depending on the security requirements for software deployment, other options are also available for rolling out SecureCOM, for instance directly from the SecureCOM Messenger server, via a mobile device management system, from a self-operated web server or from app stores.

The SecureCOM desktop version is available for Windows, MacOS and Linux. The desktop apps can simply be downloaded from the Virtual Solution website or the Virtual Solution customer and partner portal, and then rolled out to the employees using the usual software distribution process.



The clients are available in English and German.

The SecureCOM client is based on the SecureCOM Crypto Core, which utilizes cryptographic functions, such as encryption and hash algorithms, which have been evaluated by the German Federal Office for Information Security (BSI) and form part of the BSI-approved SecurePIM Government SDS communication service.



SecureCOM
by Virtual Solution

Details of the cryptographic functions provided by SecureCOM

+ X25519 scalar multiplication function (DiffieHellman), based on the Curve25519 elliptical curve
+ XSalsa20 stream cipher for data encryption in combination with private key encryption
+ Poly1305 message authentication code function employed for verification
+ Blake2b cryptographic hash function used for hashing and key derivation
+ Ed25519 deployed as algorithm for the digital signature

These specifications apply to

+ All messages
+ All private keys and the secure channel status
+ All contacts
+ PIN code and other critical data required to execute the application

All data is stored exclusively on the client side. This ensures that only the application itself, and no other external application, has access to it.

SecureCOM Server

The SecureCOM Server is responsible for providing the app and administration functions, as well as setting up secure communication and data forwarding services. It enables the provisioning and administration of users, management of devices, the establishment of connections and the exchange of messages and data for encrypted end-to-end communication between the clients.

The main objective of the SecureCOM Server is to provide the clients with secure, encrypted end-to-end messaging, data and speech functionality, which is administrated on the server.

The core functions are

+ Administration
+ User management
+ Device management
+ TLS Pinning
+ Auditing
+ Provisioning of the clients
+ Secure channel setup of the clients
+ Address book for the clients

The SecureCOM Server acts as the key component connecting the endpoints with each other and, if required, also stores their data on the server. The SecureCOM Server is also the source of data for location and geo mapping.

All services offered by the SecureCOM Messenger platform are securely contained within the platform's boundaries. The services provided by the platform function without being connected to any public service. The system is fully designed to ensure that absolutely no data is passed on to external or public services.

The SecureCOM Server can either be run from the cloud or on-premises.

SecureCOM
by Virtual Solution

SecureCOM Features and Functions

Chat

+ 1:1 Chat
+ Group chat up to 10 persons
+ Share text messages
+ Share photographs, either taken with the secure camera or – if authorized – from the photo storage on the device
+ Share emojis
+ Record and send audio messages
+ Share documents – from the device storage, only if authorized by IT
+ Share location markers, for which various icons are available for purposes of differentiation
+ Share the live location within groups
+ Self-destruct mechanism for messages
+ Respond to individual messages
+ Forwarding of messages
+ Copying of messages
+ Deletion of messages (individual, all or expired)
+ Marked as delivered
+ Message status and read receipt

Calls and Conferences

+ 1:1, groups and channels
+ Audio calls
+ Video calls
+ Screen sharing (desktop and Android versions)
+ Support for Bluetooth headsets
+ *Push to talk*: In conference calls the participants are muted and can only speak, or rather be heard, while pressing down on the corresponding icon
+ Integration in iOS Phone App, allowing SecureCOM calls to be listed there (only for iOS)
+ Full-screen mode for presentations
+ Share front and rear camera views in video calls
+ Option to configure the number of microphones simultaneously active during conferences

Channels

+ Channels for up to 255 persons
+ The creator is the default owner - others can also be designated as owners
+ Meetings with audio or video transmission
+ Share text messages
+ Share photographs, either taken with the secure camera or – if authorized – from the photo storage on the device
+ Share emojis
+ Record and send audio messages
+ Share documents – from the device storage, only if this has been authorized
+ Share location markers
+ Share the live location
+ Copying of messages
+ Deletion of messages
+ Self-destruct mechanism for messages
+ Message status and read receipt

Contacts

+ Company address book
+ Overview over media shared with a contact
+ History of communication with a contact
+ Mark contacts as external
+ QR code for exchanging contacts and keys
+ User status in profile picture (visible in all modules)

Security

+ End-to-end encryption
+ No storage of data on servers
+ Optional PIN entry
+ Setting of time-period for automatic locking
+ A secure keyboard is used to safeguard against key logging (only Android)
+ Displays contact names in push notifications (only Android)
+ Select which persons are authorized to contact the user
+ Device overview
+ Complete event log
+ Deletion of app data (various setting options)

SecureCOM by Virtual Solution

Management Portal (SMP)

SecureCOM users are managed in the SMP.

The portal offers the following functions

+ The user account can be created, edited and deleted in the SMP. The admin simply needs to enter the first name, surname and email address* of the user. At this email address, the user receives a welcome email containing a link to a webpage where the user needs to set his/her own password for SecureCOM.
  Once the user has created this password, he/she receives an activation email with details about where SecureCOM can be obtained and how to proceed with the installation and registration.
  This email also contains the activation token which the user requires to activate SecureCOM.
+ Depending on the registration status, the SMP administrator has the option of resending the welcome email or the activation email. This assists the user with registering SecureCOM, should the email not be received or get lost.
+ The SMP administrator can initiate the resetting of the SecureCOM password on behalf of a user.
  The user receives an email with a link to a webpage on which the user has to set the new password.
  This password is then used to log in to SecureCOM.

Technical Prerequisites

Mobile devices

+ iOS: Currently all operating systems from iOS 14 or higher are supported
+ Android: Android devices running a Google-certified Android operating system - Android Version 7.0 or higher

Desktop

+ Windows 10 (1909) and later
+ MacOS 10.15.5 and later
+ Ubuntu Linux 18.04 LTS and later

SecureCOM Server

+ Intel Core i7 (Recommended: XEON), 2.4GHz or faster/ higher, 4 cores
+ 16GB RAM
+ 512GB SSD physical memory
+ The optimum number of redundant nodes in the system is 5:
  + 2 nodes are set up as SecureCOM Servers in a high-availability cluster mode, which is connected to the internet (or another network within which communication is taking place). Both of these nodes also perform the SecureCOM push service for on-premises installation.
  + 3 nodes are set up as ActorDB data storage in a private network

Network

+ Audio calling (Mobile/Desktop) 20 kbps per audio channel
+ Video calling (Mobile) 200 kbps per video stream
+ Video calling (Desktop) 500 kbps per video stream
+ Screen sharing (Desktop) 1 mbps per video stream

*An email address is mandatory for generating a SecureCOM account. The first name and surname should be added, as these details will be used in the SecureCOM address book. The user has the opportunity to change the first name and surname on the self-service page.

Service und Support

Security experts at Virtual Solution and our channel partners are standing by to provide you with service and support of the highest quality.

Integration Services

Highly experienced security specialists at Virtual Solution and our channel partners are on hand to provide additional training and integration services for SecureCOM.

Product-related Update and Upgrade Support

The SecureCOM App, the Management Portal and the SecureCOM Server are improved continuously. Updates and upgrades are included in the licence.

SecureCOM
by Virtual Solution

About Virtual Solution

Virtual Solution is a software vendor specializing in secure mobile applications, with its headquarters in Munich and a development office in Berlin.

The company develops and markets the SecurePIM and SecureCOM applications, as well as the SERA security architecture for iOS and Android. SecurePIM enables mobile working which is both encrypted and user-friendly. Authorities are able to communicate using smartphones and tablets, while maintaining the levels of confidentiality required for information which is categorized as CLASSIFIED/VS-NFD.

For companies, SecurePIM ensures compliance with the General Data Protection Regulation (GDPR) when working from mobile devices, reducing the risk of committing GDPR violations and the loss of company data.

Virtual Solution was founded in 1996 and employs a staff of around 90 people. All products offered by Virtual Solution bear the trust mark *IT Security made in Germany* awarded by the TeleTrusT IT Security Association, founded to promote trust in information and communication technology in Germany.

P-21.0089_SCOM_Datasheet_EN_en/uk_v1_05/21

Virtual Solution

Virtual Solution AG
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.virtual-solution.com