SecureCOM
by Virtual Solution

# SecureCOM

## Datenblatt

Virtual Solution AG

September 2020

Version 1.0

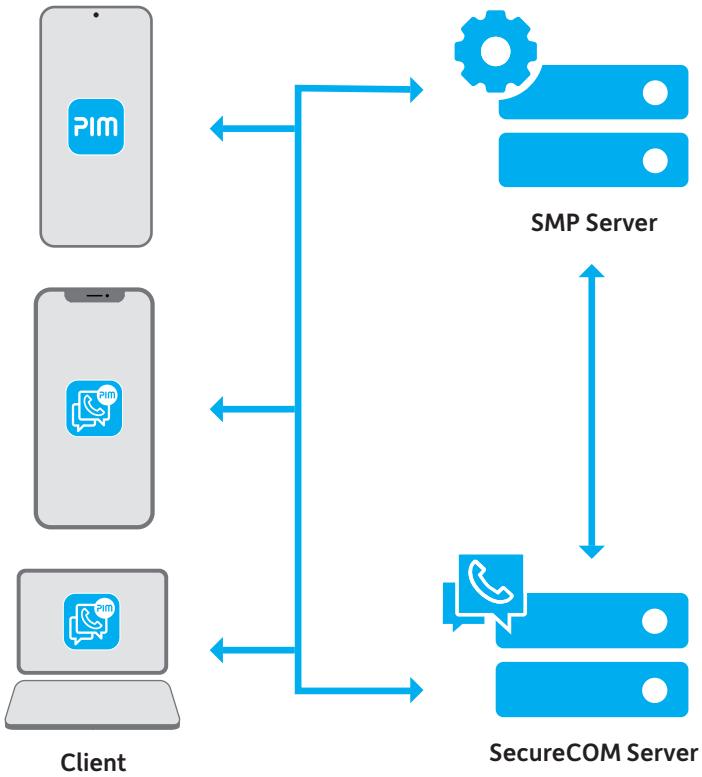
# Was ist SecureCOM?

Mit SecureCOM haben Sie alles, was Sie für sicheres geschäftliches und dienstliches Instant Messaging brauchen. Der Messenger ermöglicht Mitarbeitern einen schnellen und sicheren Austausch von Informationen und Dokumenten sowie verschlüsselte Telefonie. SecureCOM lässt sich genauso intuitiv bedienen, wie es die Anwender von Messengern aus ihrem privaten Umfeld gewöhnt sind. Alle wichtigen, geschäftskritischen Funktionen sind vorhanden. Darüber hinaus gibt es spezifische Funktionen für Behörden, wie z.B. kartenbasierte Standortanzeige von Einsatzkräften. Die Nutzer kommunizieren über ihr bevorzugtes Smartphone oder Tablet, oder benutzen den Messenger auf ihrem PC. SecureCOM steht für alle gängigen Mobil- und Desktop-Betriebssysteme zur Verfügung.

SecureCOM gibt es auch als in die Kommunikationsanwendung SecurePIM integrierte Variante: Die Anwender haben damit innerhalb eines geschützten Containers sicheren Zugriff auf Mail, Kalender, Fotos, Dokumente und können diese Inhalte direkt im Chat teilen, ohne die Anwendung verlassen zu müssen. Das erhöht nicht nur die Sicherheit Ihrer Daten, sondern ist auch für Anwender komfortabel.

## Komponenten

+ SecureCOM Client für Mobilgeräte und Desktop
+ SecureCOM Server (Cloud oder On-premise)
+ Management Portal SMP zur Benutzerverwaltung



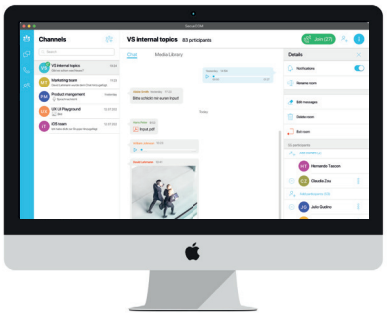
# SecureCOM Client

## Die Funktionalitäten von SecureCOM sind:

+ Ende-zu-Ende verschlüsselte Nachrichten (Text, Sprache, Video, Multimedia, Dateien)
+ Ende-zu-Ende verschlüsselte Nachrichten mit Selbstzerstörungsoption (Text, Multimedia, Dateien)
+ Ende-zu-Ende verschlüsselte Sprach- und Videoanrufe
+ Ende-zu-Ende verschlüsselte Telefonkonferenzen
+ Ende-zu-Ende verschlüsselter Gruppenchat
+ Ende-zu-Ende verschlüsselte Standortfreigabe
+ Ende-zu-Ende verschlüsselte Echtzeit-Standortfreigabe
+ Privates SecureCOM Adressbuch

Die SecureCOM App ist sowohl für iOS als auch Android Geräte erhältlich. Der Rollout der App geht schnell und einfach, denn Mitarbeiter laden sich die App entweder über den Apple® App Store oder Google Play™ herunter und registrieren sich mit ihren Zugangsdaten in der SecureCOM App. Abhängig von den Sicherheitsanforderungen an die Softwareverteilung, gibt es noch weitere Möglichkeiten SecureCOM auszurollen, z.B. direkt vom SecureCOM Messenger Server, über ein Mobile Device Management System oder über selbst betriebene Webserver oder App Stores.

Die SecureCOM Desktop-Version gibt es für Windows, MacOS und Linux. Die Desktop Apps können einfach über die Virtual Solution Webseite bzw. im Virtual Solution Kunden- und Partnerportal heruntergeladen werden und über den üblichen Prozess der Softwareverteilung an die Mitarbeiter ausgerollt werden.



Die Clients stehen auf Deutsch und Englisch zur Verfügung.

Der SecureCOM Client ist auf dem SecureCOM Crypto Core aufgebaut. Dieser verwendet kryptographische Funktionen, wie Verschlüsselungs- und Hash-Algorithmen, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) evaluiert wurden und Bestandteil der vom BSI zugelassenen Kommunikationslösung SecurePIM Government SDS sind.

### Details zu den kryptografischen Funktionen in SecureCOM:

+ X25519 skalare Multiplikationsfunktion (Diffie-Hellman), basierend auf der Curve25519 elliptischen Kurve
+ XSalsa20 Stream Cipher zur Datenverschlüsselung unter Verwendung von Verschlüsselung mit privatem Schlüssel
+ Poly1305 Nachrichten-Authentifizierungscode-Funktion wird zur Verifizierung verwendet
+ Blake2b kryptographische Hash-Funktion für Hashing und Schlüsselableitung
+ Ed25519 als Algorithmus für die digitale Unterschrift

### Diese werden eingesetzt für:

+ Alle Nachrichten
+ Alle privaten Schlüssel und den sicheren Kanalstatus
+ Alle Kontakte
+ PIN-Code und andere kritische Daten, die zur Ausführung der Anwendung erforderlich sind

Sämtliche Daten werden ausschließlich auf der Client-Seite gespeichert. Dadurch hat nur die Anwendung selbst und keine andere externe Anwendung Zugriff darauf.

## SecureCOM Server

Der SecureCOM Server ist für die Bereitstellung, Verwaltung und sichere Kommunikationseinrichtung und Datenweiterleitung zuständig. Er ermöglicht die Bereitstellung und Verwaltung der Benutzer, die Geräteverwaltung, den Verbindungsaufbau und den Nachrichten- und Datenaustausch für die verschlüsselte Ende-zu-Ende-Kommunikation zwischen den Clients. Der Hauptzweck des SecureCOM-Servers besteht darin, den Clients eine sichere, verschlüsselte Ende-zu-Ende-Nachrichten-, Daten- und Sprachfunktionalität zur Verfügung zu stellen, die auf dem Server verwaltet wird.

### Die Kernfunktionen sind:

+ Administration
+ User Management
+ Geräteverwaltung
+ TLS Pinning
+ Auditing
+ Bereitstellung der Clients
+ Secure Channel Setup für die Clients
+ Adressbuch für die Clients

Der SecureCOM Server fungiert als Kernkomponente, die die Endpunkte verbindet und bei Bedarf auch die Daten auf dem Server für diese speichert. Der SecureCOM Server ist auch die Quelle der Standort- und Kartierungsdaten. Alle Dienste der SecureCOM Messenger-Plattform sind innerhalb der Plattformgrenzen sicher eingeschlossen. Die Dienste der Plattform funktionieren ohne Verbindung zu irgendeinem öffentlichen Dienst. Das Systemdesign ist vollständig darauf ausgelegt, dass keinerlei Daten an externe oder öffentliche Dienste weitergegeben werden.

Der SecureCOM Server kann entweder in der Cloud oder On-premise betrieben werden.

# Funktionalitäten von SecureCOM

## Chat

+ 1:1 Chat
+ Gruppenchat bis zu 10 Personen
+ Teilen von Textnachrichten
+ Teilen von Bildern, die entweder mit der sicheren Kamera gemacht werden oder – falls freigegeben – aus dem Fotospeicher des Geräts genommen werden können
+ Teilen von Emojis
+ Aufnehmen und verschicken von Audio-Nachrichten
+ Teilen von Dokumenten – aus dem Gerätespeicher nur, wenn dies freigegeben ist
+ Teilen von Standortmarkierungen, für die verschiedene Icons zur Unterscheidung verfügbar sind
+ Teilen des Live-Standorts
+ Selbstzerstörungsmechanismus für Nachrichten
+ Weiterleiten von Nachrichten
+ Kopieren von Nachrichten
+ Löschen von Nachrichten (Einzelne, alle oder abgelaufene)
+ Als zugestellt markiert

## Anrufe

+ Audio-Anrufe
+ Video-Anrufe
+ Bildschirm teilen (Desktop-Version)
+ Unterstützung von Bluetooth-Headsets
+ „Drücken um zu sprechen“: In Konferenzschaltungen ist man stummgeschaltet und kann nur reden bzw. gehört werden, wenn man das entsprechende Icon gedrückt hält
+ Integration in iOS Phone App, so dass dort SecureCOM Anrufe aufgeführt werden (nur iOS)

## Channels

+ Channels für bis zu 255 Personen
+ Ersteller ist Besitzer. Er kann andere ebenfalls zu Besitzern ernennen
+ Besprechungen mit Audio- oder Videoübertragung
+ Teilen von Textnachrichten
+ Teilen von Bildern, die entweder mit der sicheren Kamera gemacht werden oder – falls freigegeben – vom Gerät genommen werden können
+ Teilen von Emojis
+ Aufnehmen und verschicken von Audio-Nachrichten
+ Teilen von Dokumenten – vom Gerätespeicher nur, wenn dies freigegeben ist
+ Teilen von Standortmarkierungen
+ Kopieren von Nachrichten
+ Löschen von Nachrichten

## Kontakte

+ Unternehmensadressbuch
+ Überblick über mit einem Kontakt geteilte Medien
+ Historie mit einem Kontakt
+ Externe Kontakte markieren
+ QR Code für den Kontakt- und Schlüsselaustausch

## Sicherheit

+ Ende-zu-Ende Verschlüsselung
+ Keine Speicherung von Daten auf Servern
+ Optionale PIN-Eingabe
+ Sperren nach einer festgelegten Zeit
+ Verwenden einer sicheren Tastatur als Schutz vor Key Logging (nur Android)
+ Zeigen von Kontaktnamen in Push Notifications (nur Android)
+ Einstellen, wer einen kontaktieren kann
+ Geräteüberblick
+ Vollständiges Event Log
+ Appdaten löschen (verschiedene Einstellmöglichkeiten)

# Management Portal (SMP)

Für SecureCOM können im SMP die Nutzer verwaltet werden.

### Folgende Funktionen stehen zur Verfügung:

+ Das Benutzerkonto kann im SMP erstellt, bearbeitet und gelöscht werden. Der Admin muss Vor- und Nachname und E-Mail-Adresse* des Benutzers eingeben. Mit dieser E-Mail-Adresse erhält der Benutzer eine Begrüßungs-E-Mail, die einen Link zu einer Selbstbedienungsseite enthält, auf der der Benutzer sein Passwort für SecureCOM festlegen muss. Nachdem der Benutzer dieses Passwort gesetzt hat, erhält er eine Aktivierungs-E-Mail mit Informationen darüber, woher SecureCOM bezogen werden kann und wie mit der Installation und Registrierung fortzufahren ist. Diese E-Mail enthält auch ein Aktivierungs-Token, das der Benutzer zur Aktivierung von SecureCOM benötigt.
+ Der SMP-Administrator kann je nach Registrierungsstatus des Benutzers die Begrüßungs-E-Mail oder die Aktivierungs-E-Mail erneut senden. Dies hilft dem Benutzer bei der Registrierung von SecureCOM, falls die E-Mail nicht empfangen wurde oder verloren gegangen ist.
+ Der SMP-Administrator kann eine Rücksetzung des SecureCOM-Passworts für den Benutzer auslösen. Der Benutzer erhält eine E-Mail mit einem Link zu der Seite mit dem Resetpasswort, auf der er nun ein neues Passwort festlegen muss. Dieses Passwort wird dann für die Anmeldung bei SecureCOM verwendet.

# Technische Voraussetzungen

### Mobilgeräte:

+ iOS: Aktuell werden alle Betriebssystemversionen ab iOS 13 unterstützt
+ Android: Android Gerät mit einem von Google zertifizierten Android Beriebssystem ab Android Version 7.0

### Desktop:

+ Windows 10
+ MacOS 10.x
+ Ubuntu Linux 18.04 und neuer

### SecureCOM Server:

+ Intel Core i7 (Empfohlen: XEON), 2.4Ghz oder schneller/höher, 4 Cores,
+ 16GB RAM
+ 512GB SSD physischer Speicher
+ Die optimale Anzahl redundanter Systemknoten beträgt 5:
  + 2 Knoten werden als SecureCOM Server im Hochverfügbarkeits-Cluster-Modus eingerichtet, der mit dem Internet (oder einem anderen Netzwerk, in dem Kommunikation stattfindet) verbunden ist. Beide Knoten führen auch den SecureCOM Push-Dienst für On-Premise Setups aus
  + 3 Knoten als ActorDB-Datenspeicher in einem privaten Netzwerk

*E-Mail-Adresse ist obligatorisch, um ein SecureCOM-Konto zu generieren. Vor- und Nachname sollten hinzugefügt werden, da diese Informationen im Adressbuch von SecureCOM verwendet werden. Der Benutzer hat die Möglichkeit, den Vor- und Nachnamen auf der Selbstbedienungsseite zu ändern.

## Service und Support

Sicherheitsexperten von Virtual Solution und Ihrer Vertriebspartner stehen zur Verfügung, um Service und Support in höchster Qualität zu leisten.

## Integrationsservice

Die erfahrenen Sicherheitsspezialisten von Virtual Solution und Ihrer Vertriebspartner stehen auch für zusätzliche Trainings und Integrationsdienstleistungen im Rahmen der Einführung von SecureCOM zur Verfügung.

## Produktbezogener Update und Upgrade Support

Sowohl die SecureCOM App als auch das Management Portal und der SecureCOM Server werden fortlaufend verbessert. Updates und Upgrades sind im Jahresabonnement enthalten.

# Über Virtual Solution

Virtual Solution ist ein auf sichere mobile Anwendungen spezialisiertes Softwareunternehmen mit Sitz in München und Entwicklungsstandort in Berlin.

Das Unternehmen entwickel t und vertreibt die Applikationen SecurePIM, SecureCOM und die Sicherheitsarchitektur SERA für iOS- und Android.
SecurePIM ermöglicht verschlüsseltes und benutzerfreundliches mobiles Arbeiten. Behörden können mit Smartphones und Tablets auf Geheimhaltungsstufe „VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH“ ( „VS – NfD“) kommunizieren.

Für Unternehmen stellt SecurePIM die Anforderungen der Datenschutzgrundverordnung (DSGVO) auf mobilen Geräten sicher und senkt damit die Risiken strafbewährter DSGVO-Verstöße und des Verlustes von Unternehmensdaten.

Virtual Solution wurde 1996 gegründet und beschäftigt rund 90 Mitarbeiter. Alle Produkte der Virtual Solution tragen das Vertrauenszeichen „IT-Security made in Germany“ des TeleTrust-IT-Bundesverbandes IT-Sicherheit e.V.

P-20.0085_SCOM_Datenblatt_de/de_v1_09/20

SecureCOM
by Virtual Solution

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