MobiVisor Messaging

Einführung

MobiVisor Messaging ist eine sichere und verschlüsselte Messenger-Application, die WhatsApp im Arbeitsbereich überflüssig macht. Die App bietet alle Basisfunktionen eines Messengers und darüber hinaus, wobei die gesamte Netzwerkkommunikation im Messenger über eine sichere Infrastruktur abgewickelt wird, die mit SSL/TLS verschlüsselt ist. Zudem werden alle Anwendungsdaten in verschlüsselten lokalen Speicherbereichen gespeichert.

Funktionen

Selbstverständlich können sich Benutzer gegenseitig auf sichere und verschlüsselte Weise Nachrichten zukommen lassen. Dies kann 1:1 erfolgen, jedoch können auch Gruppen innerhalb der Anwendung erstellt werden und somit Massennachrichten versendet werden.

Über die Messaging-Anwendung können Benutzer Dateien (Bilder, Dokumente, Audiodateien usw.) in verschlüsselter Form versenden. Hierbei werden die Nachrichten in der Anwendung mit dem 256-Bit-AES/CBC-Algorithmus unter Verwendung von 256-Bit (elliptische Kurve) Public-Private-Keys verschlüsselt.

Administration

Admin-Portal – Alle Nutzer des Messengers können zentral über ein Online-Portal verwaltet werden. Der Administrator kann dort Nutzer sperren, freigeben und einladen sowie die Nutzeraktivität einsehen. Über das Gerätenetzwerk können vom Administrator Benachrichtigungen (bspw. in Form von Push-Nachrichten) an alle im System registrierten Geräte gesendet werden.

MOBIVISOR

MobiVisor Messaging

Bündelung von Nutzern - Mitarbeitende können über das Administrations-Portal gewissen geschlossenen Bereichen zugeordnet werden (z.B. Marketing, Buchhaltung, Sales, usw.). Dies ermöglicht IOTIQ den Austausch von vertraulichen Inhalten einzuschränken und Datenlecks zu vermeiden.

Filter und Bulk Operations – Mit steigender Nutzerzahl wächst der Aufwand für Administratoren, weil häufig Tätigkeiten mehrfach ausgeführt werden müssen. MobiVisorMessenger verfügt über Filter und Bulk Operations, um die Nutzerverwaltung zu vereinfachen.

Funktionen

EMM-Integration – MobiVisor Messaging ist als Stand-Alone-Application verfügbar, die auch vollständig in unsere Enterprise Mobility Management-Lösung integriert werden kann. Die Messenger-App kann problemlos unternehmensweit konfiguriert werden und gewährleistet die Umsetzung von internen Sicherheitsrichtlinien für mobile Endgeräte.

Automatisierte Einrichtung – Der gesamte Registrierungs- und Rollout-Prozess ist vollautomatisiert, ohne dass Nutzeraktionen oder Supportaufwände nötig sind.

Nutzermanagement – Werden neue Mitarbeitende angestellt oder bisherige Mitarbeitende verlassen das Unternehmen, können problemlos Zugriffe durch den*die Administrator*in erteilt oder gesperrt werden.

Daten-Archivierung - Die Daten der Nutzenden einer Firma können über das Admin-Portal archiviert werden. Die Userchats werden auf der Gerätedatenbank gespeichert. Die Archivierung kann für spezifische Zeiträume und Nutzergruppen erfolgen. Das Archiv ist nur für autorisierte Personen zugänglich.

MOBIVISOR

MobiVisor Messaging

Einschränkungen - Es können gewisse Regeln für alle Nutzenden festgelegt werden, die die Verbreitung von Nachrichten via Copy & Paste oder das Versenden von weiteren Inhalten (wie Bildern, Videos, Dateien, usw.) verhindert. Die Einschränkungen können über das Admin-Portal individuell für Nutzende und Gruppen eingestellt werden. MobiVisor-Messenger wurde ausschließlich zur unternehmensinternen Kommunikation entwickelt.

Data Loss Prevention – Verlieren Mitarbeitende ihre Endgeräte oder sie wird gestohlen, können sensible Daten an die Öffentlichkeit kommen. Daher können in solchen Szenarien alle Daten und Inhalte von MobiVisor Messaging aus der Ferne (remote) gelöscht werden.

Infrastruktur

Private Cloud oder On-Premise – MobiVisor Messaging ist die passende Lösung unabhängig davon, welche IT-Infrastruktur vorhanden ist. MobiVisor-Messenger kann in unserer deutschen Cloud, On-Premise oder in einer privaten Cloud gehostet werden. Der Funktionsumfang wird von der Art des Hostings nicht beeinflusst.

Sicherheitsrichtlinien – In MobiVisor Messaging werden unsere strengen unternehmensweiten Sicherheitsrichtlinien angewendet, um den unbefugten Zugriff auf die Infrastruktur, Systeme und Datenzentren zu verhindern.

Skalierbarkeit – Für Unternehmen jeder Größe wird mit MobiVisor Messaging höchste Skalierbarkeit und Verlässlichkeit gewährleistet. Deshalb ist der Messenger sowohl für Kleinunternehmen als auch für sehr große Unternehmen geeignet.

MobiVisor Messaging

Datenschutz

Datenschutzrecht – MobiVisor Messaging ist das Produkt der IOTIQ GmbH mit Hauptsitz in Leipzig. Alle Daten und Inhalte werden ausschließlich auf deutschen Servern gespeichert. Damit wird das deutsche und europäische Datenschutzrecht (inkl. DSGVO) erfüllt.

Datenvermeidung – Für den Betrieb des Messengers werden so wenig Daten wie möglich verwendet. Nur wenn aus Sicherheits- oder Administrationsgründen die absolute Notwendigkeit besteht, wird auf personenbezogene Daten zugegriffen.

Integration und Anbindung – Alle Schnittstellen und APIs zu Drittanbietern wurden in MobiVisor Messaging selbst entwickelt. Dadurch können unkontrollierte Datenabflüsse verhindert werden.

Compliance

MobiVisor Messaging ist ein datenschutzkonformer Messenger für Unternehmen und Behörden. Der Datenverkehr erfolgt anonym ohne Telefonnummern und ohne Telefonbuchdaten. Die Datenverarbeitung erfolgt gemäß DSGVO, wobei der Schutz von personenbezogenen Daten von besonderer Bedeutung ist. Bei Auskunftsersuchen ist Transparenz wichtig. Deshalb liefern wir schnellstmöglich alle Informationen über die Verwendung von personenbezogenen Daten. Darüber hinaus haben Unternehmen die Möglichkeit, organisationsweite Richtlinien für den Zugriff und Austausch von Daten mit dem Messenger zu konfigurieren. Im Gegensatz zu herkömmlichen Messengern können Sie daher sicher sein, dass Sie bei der Nutzung von MobiVisor Messaging die Datenschutzbestimmungen einhalten.

MOBIVISOR

MobiVisor Messaging

Folgende Verordnungen und Gesetze werden von MobiVisor-Messenger erfüllt:

- Europäische Datenschutz-Grundverordnung (EU-DSGVO)
  - Schutz personenbezogener Daten
- Bundesdatenschutzgesetz (BDSG)
  - Umgang mit personenbezogenen Daten
- Telekommunikationsgesetz (TKG)
  - Verhinderung der Abhörung von Nachrichten
- Telemediengesetz (TMG)
  - Datenschutz beim Betrieb und die Herausgabe von Daten

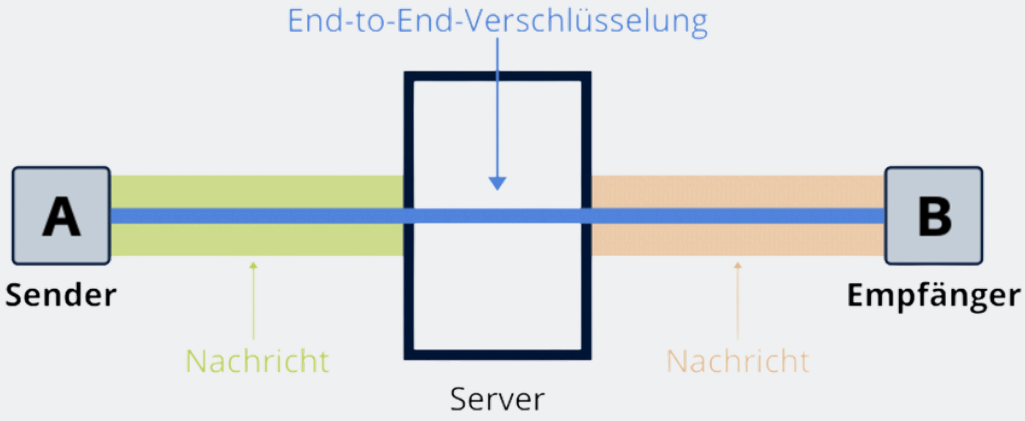
Mehr Informationen zum Datenschutz bietet unsere transparente Datenschutzerklärung. Darin wird detailliert über Art, Zweck und Umfang der Verarbeitung von personenbezogenen Daten informiert.

Technische Daten

Alle Verbindungen werden in MobiVisor Messaging über TLS aufgebaut. TLS-Zertifikate und Einstellungen verfügen über neueste Sicherheitsoptionen. MobiVisor Messaging erhält mit A+ die höchste Bewertung beim Qualys SSL Labs Test (SSL Server Test). Die Nachrichten verwenden eine End-to-End-Verschlüsselung. Bei der Verwendung von Push-Messaging-Diensten (Firebase Cloud Messaging, Apple Push Services) werden keine Inhalte gesendet, sondern nur ein Benachrichtigungs-Hinweis. Dadurch wird einem Datenverlust (auch wenn verschlüsselt) an Dritte vorgebeugt.

MobiVisor Messaging

End-to-End-Verschlüsselung:



256-bit public-private Keys werden generiert (entspricht **3072 bit RSA**).

$$AB_{shared} = createSharedSecret_{Curve25519}(A_{private}, B_{public})\ //\ 256\ bit$$

$$AB_{shared\_expandet} = HBKDF(AB_{shared})\ //\ 512\ bit$$

$$KEY_{encrypt} = AB_{shared\_expandet}[0-255]\ //\ Encryption\ Key$$

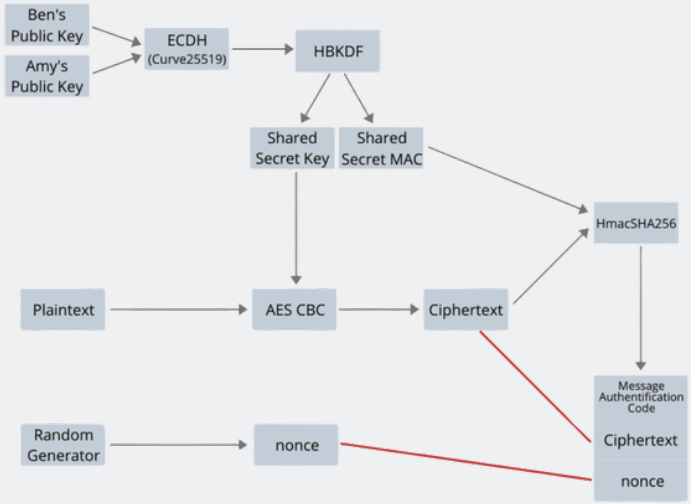
$$KEY_{mac} = AB_{shared\_expandet}[256-511]\ //\ Integrity\ Check$$

Verschlüsselung:

$$encryptedContent = AES_{CBC_{key}}(Plaintext)\ //\ AES256\ Block\ Encryption$$

$$Mac = HmacSHA256(encryptedContent)\ //\ Integrity\ Check$$

$$Message = \{\dots encrypted\ Content \mid mac \dots\}$$



MOBIVISOR

MobiVisor Messaging

Lokale Festplattenverschlüsselung:

Die Mitteilungen werden nicht im Volltext gespeichert. Sie sind verschlüsselt und können mit einer PIN abgerufen werden, die vom Benutzer erstellt wird.

key: zufällig generiert (256-bit)
PIN: benutzerdefiniert
pin_key= Scrypt(PIN)
encrypted_key=$encrypt_{pin\_key}$(key)

Nachrichten werden mit *key* verschlüsselt, *encrypted_key* wird auf der Festplatte gespeichert. Um die Nachrichten mit *key* zu öffnen, ist eine *PIN* erforderlich.

Encrypt-Funktion: 256-bit AES/CBC

Warum WhatsApp nicht ausreicht

WhatsApp-Nachrichten werden in der Cloud des Benutzers gesichert (wenn der Benutzer akzeptiert). Welche Standorte haben die Server? WhatsApp gehört Meta. Deshalb sind die Server ebenfalls im Besitz von Meta. WhatsApp ist für Endbenutzer konzipiert. Zukünftige Funktionen können gegen die Unternehmensrichtlinien verstoßen. Gleiches gilt für WhatsApp Business.