Sicherheit

In diesem Kapitel werden verschiedene Punkte erläutert, die im Zusammenhang mit der Sicherheit der Anwendung stehen.

- Überblick: Warum Sicherheit wichtig ist
- Die verschiedenen Sicherheitsmechanismen in Ihrer App
- Unterscheidung zwischen Zugangsdaten und Verschlüsselung: Zwei verschiedene Schutzmechanismen
- Passkeys: Die Zukunft der sicheren Anmeldung
- Grundlagen der Ende-zu-Ende-Verschlüsselung
- Ihre Sicherheit in Ihren Händen – mit einer optionalen Komfortlösung

Überblick: Warum Sicherheit wichtig ist

Ihre Daten sind wertvoll – und schützenswert

In der heutigen digitalen Welt sind unsere persönlichen Daten ein wertvolles Gut. Gerade im Gesundheitswesen sind diese Daten besonders sensibel und bedürfen eines besonderen Schutzes. Es geht um Ihre Privatsphäre, Ihre Krankheitsgeschichte, Ihre vertrauliche Kommunikation mit Ihrem Arzt oder Ihrer Ärztin. Stellen Sie sich vor, diese Informationen gerieten in falsche Hände. Die Folgen könnten gravierend sein – von Diskriminierung über Identitätsdiebstahl bis hin zu finanziellen Schäden. Deshalb ist Sicherheit für uns nicht nur ein leeres Versprechen, sondern eine absolute Notwendigkeit.

So sicher wie Ihr Zuhause

Jeder von uns schützt sein Zuhause. Wir schließen die Haustür ab, wenn wir gehen, und viele haben zusätzliche Sicherheitsvorkehrungen wie Alarmanlagen. Warum tun wir das? Weil wir unser Eigentum und unsere Privatsphäre schützen wollen. Genauso wichtig ist es, Ihre Gesundheitsdaten zu schützen. Stellen Sie sich unsere App wie ein sicheres Haus für Ihre medizinischen Informationen vor. Wir sorgen dafür, dass Unbefugte keinen Zutritt haben und Ihre Daten sicher aufbewahrt werden.

Was passieren könnte, wenn Daten in falsche Hände geraten

Was wären die Konsequenzen, wenn Ihre Gesundheitsdaten nicht geschützt wären?

- **Unbefugter Zugriff auf Ihre Krankheitsgeschichte:** Dritte könnten Einblick in Ihre medizinische Vorgeschichte erhalten und diese Informationen missbrauchen.

- **Offenlegung sensibler Informationen:** Persönliche Details über Ihren Gesundheitszustand könnten öffentlich werden und Ihre Privatsphäre verletzen.
- **Diskriminierung:** Informationen über bestimmte Erkrankungen könnten zu Benachteiligungen im Berufsleben oder bei Versicherungsabschlüssen führen.
- **Identitätsdiebstahl:** Ihre persönlichen Daten könnten für betrügerische Zwecke missbraucht werden.

Diese Beispiele verdeutlichen, warum der Schutz Ihrer Gesundheitsdaten von höchster Bedeutung ist.

Datensicherheit ist uns wichtig

Wir nehmen den Schutz Ihrer Daten sehr ernst. Unsere App wurde mit modernsten Sicherheitsstandards entwickelt, um Ihre Privatsphäre bestmöglich zu schützen. Wir verwenden anerkannte Verfahren zur Ende-zu-Ende-Verschlüsselung von Nachrichten sowie Authentifizierungs-Lösungen zum Schutz Ihres Benutzerkontos. So können Sie sicher sein, dass Ihre Kommunikation mit Ihrem Arzt oder Ihrer Ärztin vertraulich bleibt.

Die verschiedenen Sicherheitsmechanismen in Ihrer App

Wir nehmen den Schutz Ihrer Daten sehr ernst. Deshalb haben wir in unserer App verschiedene Sicherheitsmechanismen implementiert, die ineinandergreifen und ein Höchstmaß an Sicherheit gewährleisten. Im Folgenden erklären wir Ihnen die wichtigsten dieser Mechanismen.

Sichere Anmeldung: Ihr persönlicher Zugang

Der erste Schritt zur Sicherheit ist eine sichere Anmeldung. Wir bieten Ihnen verschiedene Möglichkeiten, sich in unserer App anzumelden:

- **Passwort:** Sie können ein sicheres Passwort verwenden, um Ihr Konto zu schützen. Bitte beachten Sie folgende Tipps für ein sicheres Passwort:
  - Verwenden Sie eine Kombination aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.
  - Verwenden Sie kein Passwort, das leicht zu erraten ist (z.B. Ihren Namen oder Ihr Geburtsdatum).
  - Verwenden Sie für jeden Dienst ein eigenes Passwort.
  - Ändern Sie Ihr Passwort regelmäßig.
- **Passkeys (Empfohlen):** Passkeys sind eine moderne und besonders sichere Methode zur Anmeldung. Sie nutzen die biometrischen Funktionen Ihres Geräts (z.B. Fingerabdruck oder Gesichtserkennung) oder einen Hardware-Sicherheitsschlüssel, um sich anzumelden. Passkeys sind deutlich sicherer als Passwörter, da sie nicht gestohlen oder erraten werden können. Erfahren Sie hier mehr zu Passkeys vom BSI: Anmelden ohne Passwort mit Passkey
- **Anmeldung mit Apple-ID/Google-ID (zukünftig):** In Zukunft werden wir auch die Anmeldung mit Ihrer Apple-ID oder Google-ID anbieten. Diese Dienste bieten bereits hohe Sicherheitsstandards und ermöglichen eine bequeme Anmeldung.

Ende-zu-Ende-Verschlüsselung: Ihre Nachrichten bleiben privat

Wir verwenden in unserer App standardmäßig die Ende-zu-Ende-Verschlüsselung mit dezentraler Schlüsselverwaltung. Das bedeutet:

- Ihre Nachrichten werden auf Ihrem Gerät verschlüsselt, bevor sie das Internet erreichen.
- Nur der Empfänger kann die Nachrichten mit seinem persönlichen Schlüssel entschlüsseln.
- Wir als Anbieter haben keinen Zugriff auf Ihre Nachrichten.

Optionale zentrale Schlüsselverwaltung (Komfortlösung): Zusätzlich bieten wir optional eine zentrale Schlüsselverwaltung an, um den Komfort zu erhöhen. Beachten Sie jedoch, dass dies einen Kompromiss in Bezug auf die maximale Privatsphäre darstellt.

Matrix-Protokoll: Eine sichere Basis für die Kommunikation

Die Ende-zu-Ende-Verschlüsselung unserer App basiert auf dem Matrix-Protokoll, einem offenen Standard für sichere und dezentrale Kommunikation. Das Matrix-Protokoll bietet folgende Vorteile:

- **Dezentralisierung:** Ihre Daten werden nicht zentral auf einem einzigen Server gespeichert, sondern können auf verschiedenen Servern verteilt sein. Dies erhöht die Ausfallsicherheit und schützt vor Zensur.
- **Ende-zu-Ende-Verschlüsselung:** Das Matrix-Protokoll unterstützt standardmäßig die Ende-zu-Ende-Verschlüsselung.
- **Offener Standard:** Der offene Standard ermöglicht es unabhängigen Experten, die Sicherheit des Protokolls zu überprüfen.

Erfahren Sie hier mehr zu Ende-zu-Ende-Verschlüsselung mit dem Matrix-Protokoll: Matrix und Element.io.

Zusätzliche Sicherheitsmaßnahmen

Neben den oben genannten Mechanismen setzen wir weitere Sicherheitsmaßnahmen ein, um Ihre Daten bestmöglich zu schützen:

- **Regelmäßige Sicherheitsupdates:** Wir aktualisieren unsere App regelmäßig, um bekannte Sicherheitslücken zu schließen.
- **Sichere Serverinfrastruktur:** Unsere Server sind durch modernste Sicherheitstechnologien geschützt.
- **Datenschutzkonforme Datenverarbeitung:** Wir verarbeiten Ihre Daten gemäß den geltenden Datenschutzbestimmungen (DSGVO).

Was Sie selbst für Ihre Sicherheit tun können

Auch Sie können einen wichtigen Beitrag zu Ihrer Sicherheit leisten:

- **Verwenden Sie ein sicheres Passwort oder Passkeys:** Befolgen Sie unsere Tipps für sichere Passwörter oder nutzen Sie die noch sichereren Passkeys.
- **Halten Sie Ihre App auf dem neuesten Stand:** Installieren Sie regelmäßig die neuesten Updates unserer App.
- **Seien Sie vorsichtig bei verdächtigen Nachrichten:** Klicken Sie nicht auf Links oder Anhänge in Nachrichten von unbekannten Absendern.
- **Schützen Sie Ihr Gerät:** Verwenden Sie eine Bildschirmsperre und installieren Sie eine Antivirus-App.

Fazit: Gemeinsam für Ihre Sicherheit

Wir setzen alles daran, Ihre Daten bestmöglich zu schützen. Durch die Kombination verschiedener Sicherheitsmechanismen und Ihre Mithilfe schaffen wir eine sichere Kommunikationsumgebung.

Unterscheidung zwischen Zugangsdaten und Verschlüsselung: Zwei verschiedene Schutzmechanismen

Oftmals werden die Begriffe "Zugangsdaten" und "Verschlüsselung" im Zusammenhang mit Sicherheit verwendet, aber sie bezeichnen zwei unterschiedliche Schutzmechanismen, die unterschiedliche Zwecke erfüllen. Es ist wichtig, den Unterschied zu verstehen, um die Sicherheit unserer App vollständig zu erfassen.

Zugangsdaten: Der Schlüssel zu Ihrem Konto

Ihre Zugangsdaten sind wie der Haustürschlüssel zu Ihrem Haus oder die PIN für Ihre Bankkarte. Sie ermöglichen Ihnen den Zutritt zu Ihrem persönlichen Bereich in unserer App. Ohne diese Zugangsdaten können Sie die App nicht nutzen und auf Ihre Daten zugreifen.

- **Was sind Zugangsdaten?** In unserer App können Ihre Zugangsdaten ein Passwort, ein Passkey oder zukünftig Ihre Apple-ID oder Google-ID sein.
- **Was schützen Zugangsdaten?** Ihre Zugangsdaten schützen Ihr Konto vor unbefugtem Zugriff. Sie verhindern, dass jemand anderes sich als Sie anmeldet und Ihre Nachrichten liest oder andere Aktionen in Ihrem Namen ausführt.
- **Analogie: Der Haustürschlüssel:** Stellen Sie sich vor, Ihre App ist Ihr Haus. Ihre Zugangsdaten sind der Haustürschlüssel. Nur mit dem richtigen Schlüssel können Sie das Haus betreten.

Verschlüsselung: Der Schutz Ihrer Nachrichten

Die Verschlüsselung hingegen schützt den Inhalt Ihrer Nachrichten selbst. Sie sorgt dafür, dass Ihre Nachrichten nur von Ihnen und dem Empfänger gelesen werden können, selbst wenn jemand Zugriff auf Ihr Konto erlangt oder die Nachrichten während der Übertragung abfängt.

- **Was ist Verschlüsselung?** Die Verschlüsselung wandelt Ihre Nachrichten in einen unleserlichen Code um. Nur mit dem richtigen Schlüssel können diese Nachrichten wieder in Klartext umgewandelt werden.
- **Was schützt die Verschlüsselung?** Die Verschlüsselung schützt den Inhalt Ihrer Nachrichten vor neugierigen Blicken. Selbst wir als Anbieter der App können Ihre Nachrichten nicht lesen, wenn sie verschlüsselt sind (bei der standardmäßig aktivierten dezentralen Schlüsselverwaltung).
- **Analogie: Der Safe im Haus:** Stellen Sie sich vor, Sie haben einen Safe in Ihrem Haus. Selbst wenn jemand mit dem Haustürschlüssel (Ihren Zugangsdaten) in Ihr Haus gelangt, kann er den Inhalt des Safes ohne den richtigen Code (den Verschlüsselungsschlüssel) nicht einsehen.

Der Unterschied im Überblick: Haustürschlüssel vs. Safe

Merkmal	Zugangsdaten (Haustürschlüssel)	Verschlüsselung (Safe)
Funktion	Ermöglicht den Zugang zum Konto	Schützt den Inhalt der Nachrichten
Schutz vor	Unbefugtem Zugriff auf das Konto	Unbefugtem Lesen der Nachrichten, auch bei Zugriff auf das Konto oder während der Übertragung
Analogie	Haustürschlüssel	Safe im Haus
Beispiel in der App	Passwort, Passkey, Apple-ID, Google-ID	Ende-zu-Ende-Verschlüsselung mit dem Matrix-Protokoll

Warum sind beide Mechanismen wichtig?

Sowohl Zugangsdaten als auch Verschlüsselung sind wichtig für die Sicherheit Ihrer Daten. Sie ergänzen sich gegenseitig und bieten einen umfassenden Schutz:

- **Zugangsdaten schützen vor unbefugtem Zugriff auf Ihr Konto.**

- **Die Verschlüsselung schützt den Inhalt Ihrer Nachrichten, selbst wenn jemand Zugriff auf Ihr Konto erlangt.**

Ohne Zugangsdaten könnten Sie die App nicht nutzen. Ohne Verschlüsselung wären Ihre Nachrichten nicht vertraulich.

Veranschaulichung mit einem Beispiel

Stellen Sie sich vor, jemand errät Ihr Passwort (Ihren Haustürschlüssel). Ohne Verschlüsselung könnte diese Person alle Ihre Nachrichten lesen. Mit Verschlüsselung hingegen wären die Nachrichten weiterhin geschützt, da die Person ohne den richtigen Verschlüsselungsschlüssel (den Code für den Safe) nichts damit anfangen könnte.

Fazit: Doppelt hält besser

Durch die Kombination von sicheren Zugangsdaten und starker Verschlüsselung bieten wir Ihnen ein Höchstmaß an Sicherheit und Privatsphäre.

Passkeys: Die Zukunft der sicheren Anmeldung

Passkeys sind eine neue und innovative Methode zur sicheren Anmeldung bei Apps und Websites. Sie bieten im Vergleich zu herkömmlichen Passwörtern eine deutlich höhere Sicherheit und sind dabei gleichzeitig einfacher zu verwenden.

Was sind Passkeys?

Stellen Sie sich Passkeys als digitale Schlüssel vor, die auf Ihrem Gerät gespeichert werden – sei es Ihr Smartphone, Tablet oder Computer. Anstatt sich ein komplexes Passwort merken zu müssen, authentifizieren Sie sich mit Ihrem Gerät selbst, z.B. per Fingerabdruck, Gesichtserkennung (Face ID) oder Geräte-PIN. Der Passkey bestätigt dann im Hintergrund Ihre Identität.

Wie funktionieren Passkeys?

Passkeys basieren auf der WebAuthn-Technologie, einem offenen Standard für sichere Authentifizierung. Wenn Sie sich mit einem Passkey anmelden, findet ein sicherer Austausch von kryptografischen Schlüsseln zwischen Ihrem Gerät und dem Dienst statt, bei dem Sie sich anmelden möchten. Dabei werden *keine* Passwörter über das Internet übertragen oder auf Servern gespeichert.

Die Vorteile von Passkeys gegenüber Passwörtern

- **Höhere Sicherheit:** Passkeys sind deutlich sicherer als Passwörter, da sie nicht gestohlen, erraten oder durch Phishing-Angriffe erbeutet werden können. Sie sind an Ihr Gerät gebunden und erfordern in der Regel eine biometrische Authentifizierung, was einen zusätzlichen Schutz bietet.
- **Kein Merken von Passwörtern:** Sie müssen sich keine komplexen Passwörter mehr merken oder diese verwalten. Die Authentifizierung erfolgt bequem und schnell über Ihr Gerät.
- **Schutz vor Phishing:** Da keine Passwörter übertragen werden, sind Sie vor Phishing-Angriffen geschützt, bei denen Betrüger versuchen, Ihre Passwörter abzufangen.

- **Einfache Nutzung auf verschiedenen Geräten:** Passkeys können über iCloud Keychain (Apple) oder Google Password Manager (Google) sicher zwischen Ihren Geräten synchronisiert werden, sodass Sie sich überall bequem anmelden können.

Passkeys im Vergleich zu Apple-ID/Google-ID

Sowohl Passkeys als auch die Anmeldung mit Apple-ID/Google-ID bieten eine komfortable und sichere Möglichkeit zur Anmeldung. Es gibt jedoch einige wichtige Unterschiede:

Merkmal	Passkeys	Apple-ID/Google-ID
Unabhängigkeit vom Anbieter	Unabhängig von einem bestimmten Anbieter. Funktioniert mit verschiedenen Diensten.	Abhängig vom jeweiligen Anbieter (Apple oder Google).
Gerätebindung	An das Gerät gebunden, kann aber über iCloud Keychain/Google Password Manager synchronisiert werden.	An das jeweilige Konto (Apple-ID oder Google-ID) gebunden.
Schutz vor Phishing	Bietet sehr guten Schutz vor Phishing.	Bietet Schutz vor Phishing, aber die Sicherheit hängt auch von der Sicherheit des Kontos ab.
Wiederherstellung bei Verlust	Bei Geräteverlust müssen die Passkeys über die Synchronisierung (iCloud/Google) wiederhergestellt werden.	Bei Verlust des Kontos muss das Konto wiederhergestellt werden (z.B. per Wiederherstellungs-E-Mail).
Zusätzliche Sicherheit	Kann mit zusätzlichen Sicherheitsmaßnahmen wie Hardware-Sicherheitsschlüsseln kombiniert werden.	Kann mit Zwei-Faktor-Authentifizierung (2FA) zusätzlich gesichert werden.

Vorteile der Nutzung von Apple-ID/Google-ID

- **Bequeme Anmeldung:** Die Anmeldung erfolgt schnell und unkompliziert mit Ihren bestehenden Kontodaten.
- **Single Sign-On (SSO):** Sie können sich mit Ihrer Apple-ID/Google-ID bei verschiedenen Apps und Websites anmelden, ohne jedes Mal neue Konten erstellen zu müssen.
- **Integration in das Ökosystem:** Die Nutzung ist nahtlos in das jeweilige Ökosystem (Apple oder Google) integriert.

Fazit

Passkeys stellen eine deutliche Verbesserung gegenüber herkömmlichen Passwörtern dar und bieten ein Höchstmaß an Sicherheit und Benutzerfreundlichkeit. Die Anmeldung mit Apple-ID/Google-ID bietet ebenfalls Vorteile in Bezug auf Komfort und Integration. Beide Methoden tragen dazu bei, Ihre Online-Sicherheit zu erhöhen. In unserer App unterstützen wir sowohl Passkeys als auch zukünftig die Anmeldung mit Apple-ID/Google-ID, um Ihnen die bestmögliche Erfahrung zu bieten.

Grundlagen der Ende-zu-Ende-Verschlüsselung

Was ist Ende-zu-Ende-Verschlüsselung? Eine sichere Reise für Ihre Nachrichten

Die Ende-zu-Ende-Verschlüsselung ist wie ein sicherer Umschlag für Ihre Nachrichten. Nur der Empfänger kann diesen Umschlag öffnen und den Inhalt lesen. Auf dem Weg vom Absender zum Empfänger ist der Umschlag verschlossen und somit vor neugierigen Blicken geschützt. Konkret bedeutet das: Ihre Nachrichten werden auf Ihrem Gerät verschlüsselt, bevor sie überhaupt das Internet erreichen. Nur der Empfänger kann diese Nachrichten mit seinem persönlichen Schlüssel wieder entschlüsseln.

Die Analogie mit dem Brief: Ein sicherer Transportweg

Stellen Sie sich vor, Sie schreiben einen wichtigen Brief.

1. **Verschließen des Briefs:** Sie stecken den Brief in einen Umschlag und verschließen ihn. Dies entspricht der Verschlüsselung Ihrer Nachricht auf Ihrem Gerät.
2. **Sicherer Transport:** Der Brief wird per Post verschickt. Während des Transports kann niemand den Inhalt des Briefes lesen, da der Umschlag verschlossen ist. Dies entspricht dem sicheren Transport Ihrer verschlüsselten Nachricht über das Internet.
3. **Öffnen durch den Empfänger:** Nur der Empfänger kann den Umschlag öffnen und den Brief lesen. Dies entspricht der Entschlüsselung der Nachricht auf dem Gerät des Empfängers mit seinem persönlichen Schlüssel.

Genau so funktioniert die Ende-zu-Ende-Verschlüsselung in unserer App.

Was bedeutet das für Sie? Absolute Privatsphäre

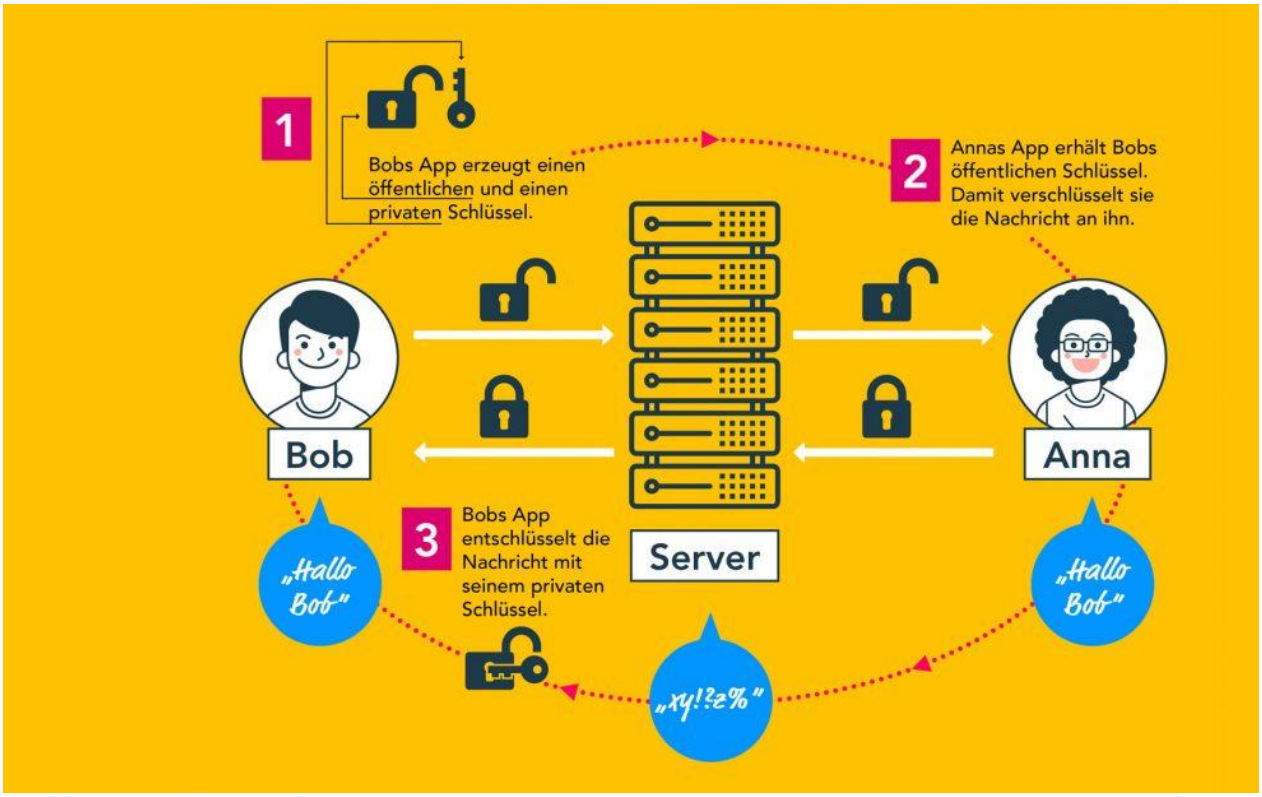
Die Ende-zu-Ende-Verschlüsselung bietet Ihnen ein Höchstmaß an Privatsphäre. Denn:

- **Nur Sie und der Empfänger können die Nachrichten lesen:** Selbst wir als Anbieter der App können Ihre Nachrichten nicht entschlüsseln.
- **Schutz vor Abhören:** Auch wenn jemand die Nachrichten während der Übertragung abfangen sollte, kann er sie nicht lesen, da sie verschlüsselt sind.
- **Vertrauliche Kommunikation:** Sie können sich darauf verlassen, dass Ihre Kommunikation mit Ihrem Arzt oder Ihrer Ärztin absolut vertraulich bleibt.

Der Unterschied zu herkömmlichen Kommunikationswegen: Wie Tag und Nacht

Herkömmliche Kommunikationswege wie unverschlüsselte E-Mails oder SMS sind wie Postkarten. Jeder, der die Postkarte in die Hände bekommt, kann sie lesen. Im Gegensatz dazu sind Ihre Nachrichten in unserer App wie in einem Tresor sicher verwahrt. Nur Sie und der Empfänger haben den Schlüssel zu diesem Tresor.

Der Weg einer verschlüsselten Nachricht



> Quelle: mobilsicher.de

Fazit: die Privatsphäre Ihrer Nachrichten ist uns wichtig

Die Ende-zu-Ende-Verschlüsselung ist ein wichtiger Baustein für die Sicherheit Ihrer Daten. Sie sorgt dafür, dass Ihre Kommunikation absolut vertraulich bleibt.

Ihre Sicherheit in Ihren Händen – mit einer optionalen Komfortlösung

Wir haben bereits erklärt, wie die Ende-zu-Ende-Verschlüsselung funktioniert und den Unterschied zwischen zentraler und dezentraler Schlüsselverwaltung erläutert. Nun möchten wir Ihnen eine optionale Komfortlösung vorstellen, die wir zusätzlich anbieten, und die damit verbundenen Vor- und Nachteile transparent darlegen.

Zentrale Schlüsselverwaltung vs. Dezentrale Schlüsselverwaltung: Zwei unterschiedliche Ansätze – mit einer optionalen dritten Option

Es gibt zwei grundlegende Arten, wie die Schlüssel für die Ende-zu-Ende-Verschlüsselung verwaltet werden können:

- **Zentrale Schlüsselverwaltung (wie bei WhatsApp):** Bei WhatsApp und ähnlichen Diensten werden bestimmte Schlüsselinformationen zentral auf den Servern des Anbieters gespeichert und verwaltet. Das bedeutet, dass der Anbieter technisch gesehen die Möglichkeit hätte, Nachrichten zu entschlüsseln. WhatsApp betont zwar, dies nicht zu tun, aber das Vertrauen in den Anbieter ist hier entscheidend. Es ist wie ein Bankschließfach in einer Bank. Die Bank hat zwar keinen direkten Zugriff auf den Inhalt jedes einzelnen Schließfachs, aber sie hat Zugriff auf den Tresorraum, in dem sich die Schließfächer befinden.
- **Dezentrale Schlüsselverwaltung (wie standardmäßig in unserer App):** In unserer App verfolgen wir standardmäßig einen anderen Ansatz: Die für die Verschlüsselung notwendigen Sicherheitsschlüssel werden *ausschließlich* auf Ihren Geräten generiert und gespeichert. Wir als Anbieter haben *keinen* Zugriff auf diese Schlüssel. Das bedeutet, dass wir Ihre Nachrichten *nicht* lesen können, selbst wenn wir es wollten. Es ist wie ein eigener Safe in Ihrem Haus. Nur Sie haben den Schlüssel.

- **Optionale zentrale Schlüsselverwaltung (Komfortlösung):** Wir verstehen, dass die Eigenverwaltung der Schlüssel, insbesondere auf mehreren Geräten, umständlich sein kann. Daher bieten wir optional die Möglichkeit einer zentralen Schlüsselverwaltung an. Wenn Sie diese Option wählen, werden bestimmte Schlüsselinformationen auf unseren Servern gespeichert.

Was bedeutet das konkret für Sie?

- **Höheres Maß an Privatsphäre (bei dezentraler Verwaltung):** Durch die standardmäßig aktivierte dezentrale Schlüsselverwaltung garantieren wir Ihnen ein Höchstmaß an Privatsphäre. Ihre Kommunikation bleibt absolut vertraulich, da niemand außer Ihnen und dem Empfänger Zugriff auf die entschlüsselten Nachrichten hat.
- **Komfort und Bequemlichkeit (bei optionaler zentraler Verwaltung):** Die optionale zentrale Schlüsselverwaltung bietet Ihnen mehr Komfort, insbesondere bei der Nutzung mehrerer Geräte oder bei einem Geräteverlust. Sie müssen sich nicht um die manuelle Sicherung und Wiederherstellung Ihrer Schlüssel kümmern.
- **Reduziertes Maß an Privatsphäre (bei optionaler zentraler Verwaltung):** Es ist wichtig zu betonen, dass bei der Nutzung der optionalen zentralen Schlüsselverwaltung ein geringfügig reduziertes Maß an Privatsphäre besteht. Da wir bestimmte Schlüsselinformationen speichern, hätten wir theoretisch die Möglichkeit, Nachrichten zu entschlüsseln. Wir verpflichten uns jedoch, dies *niemals* zu tun und Ihre Daten mit höchster Sorgfalt zu behandeln.

Vergleichstabelle: Die wichtigsten Unterschiede im Überblick

Merkmal	WhatsApp (Beispiel)	Unsere App (Standard)	Unsere App (Optionale Komfortlösung)
Schlüsselverwaltung	Zentral (auf den Servern des Anbieters)	Dezentral (auf den Geräten der Nutzer)	Zentral (auf unseren Servern)
Zugriff des Anbieters	Theoretisch möglich	Nicht möglich	Theoretisch möglich
Vertrauen in den Anbieter	Notwendig	Nicht notwendig	Notwendig
Sicherheit	Hoch, aber abhängig vom Vertrauen in den Anbieter	Höchstmöglich, unabhängig vom Anbieter	Hoch, aber abhängig von unserem Vertrauen
Komplexität für den Nutzer	Gering	Etwas höher (z.B. bei Geräteverlust/Neuinstallation)	Gering

Fazit: Ihre Wahl – Ihre Sicherheit

Wir bieten Ihnen die Wahl: Maximale Privatsphäre durch dezentrale Schlüsselverwaltung oder mehr Komfort durch die optionale zentrale Schlüsselverwaltung. Wir sind transparent bezüglich der Vor- und Nachteile beider Optionen und überlassen Ihnen die Entscheidung. Wir sind davon überzeugt, dass die standardmäßig aktivierte dezentrale Schlüsselverwaltung der beste Weg ist, um Ihre Privatsphäre bestmöglich zu schützen. Wir nehmen den Schutz Ihrer Daten sehr ernst und setzen alles daran, Ihnen eine sichere und vertrauliche Kommunikationsplattform zu bieten – egal für welche Option Sie sich entscheiden.