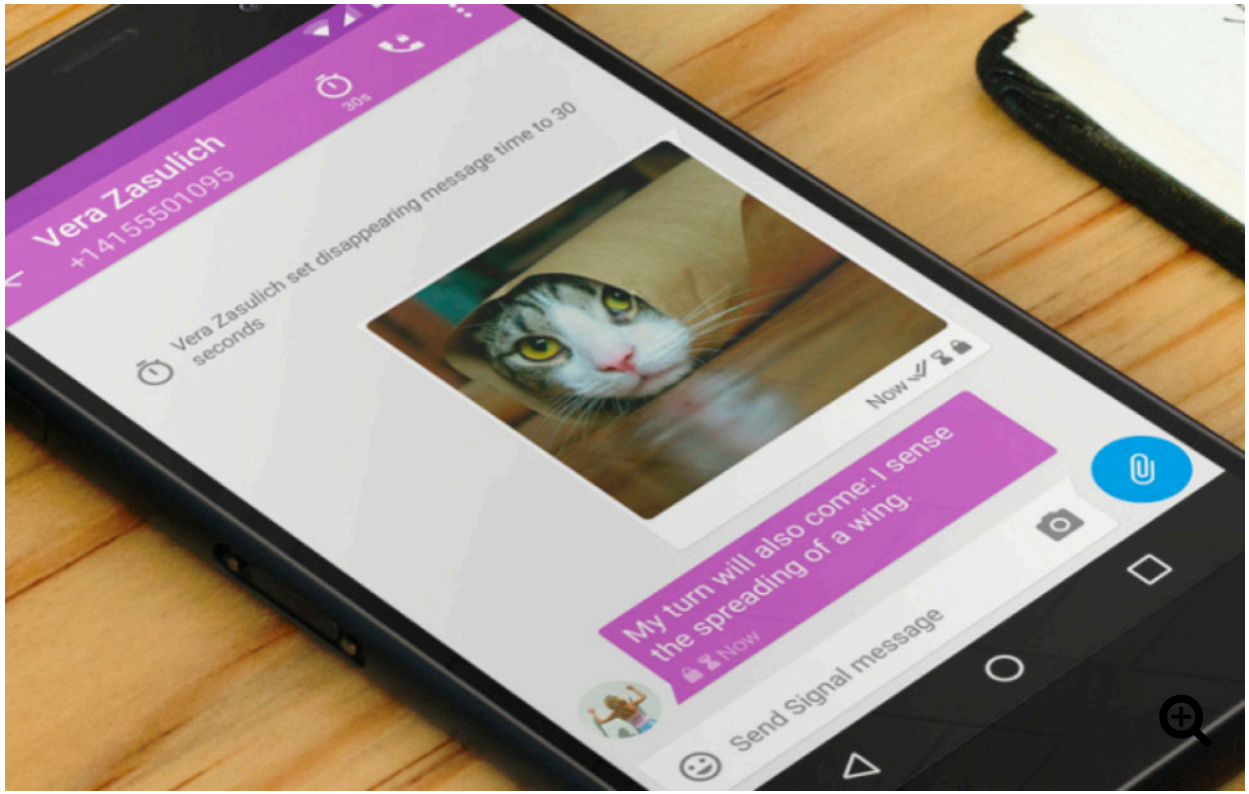
Sealed Sender *30.10.2018, 15:42 Uhr*

Signal arbeitet an anonymisierten Absendern

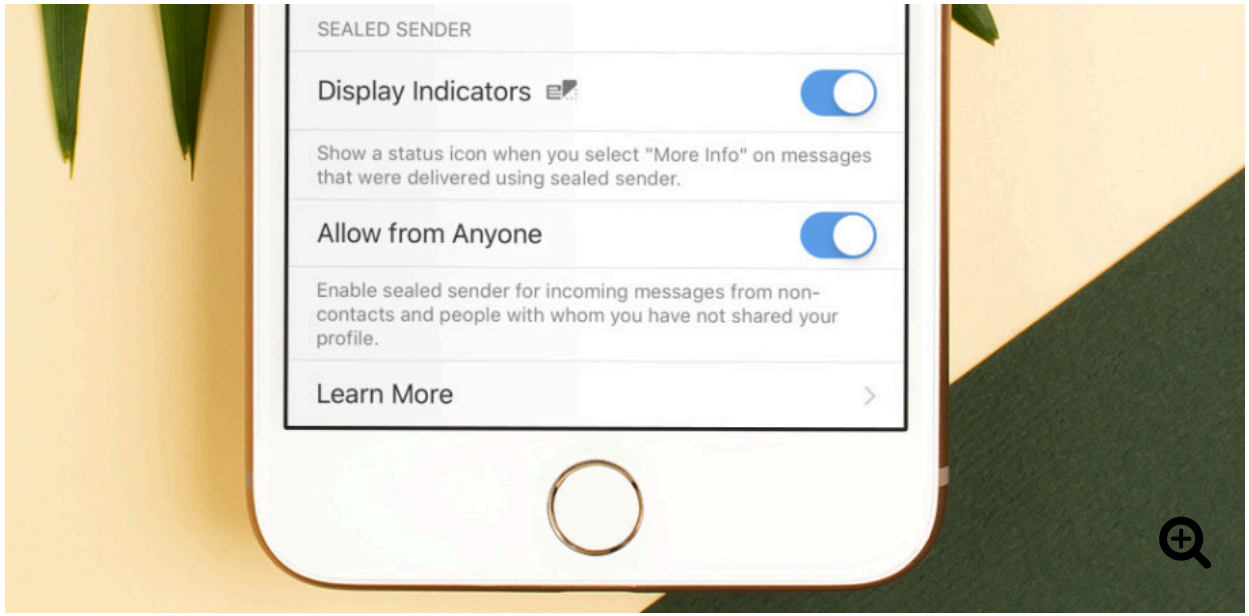
Der verschlüsselte Messenger-Dienst Signal will künftig auch die beim Versandprozess anfallenden Metadaten absichern und damit den Absender anonymisieren.



(Quelle: Signal)

Der Messenger-Dienst Signal arbeitet derzeit an einer neuen Datenschutz-Funktion zur Anonymisierung des Absender. Wie die Sicherheitsspezialisten auf ihrem Blog mitteilen, wolle man hierzu die beim Versand anfallenden Metadaten auf den Servern verschlüsseln. Die Grundüberlegung beruht dabei darauf, dass die Signal-Server zwar wissen müssen, an wen eine Nachricht gerichtet ist. Wohingegen der Absender für die Grundfunktionalität keine Rolle spielen sollte.

Bislang sendet ein Signal-Client eine Nachricht, indem er sich über TLS mit dem Dienst verbindet, authentifiziert und die verschlüsselten Nachrichteninhalte zusammen mit einem Ziel übergibt. Die Authentifizierung kommt zum Einsatz, um Spoofing zu verhindern und dem Empfänger Gewissheit über die Identität des Absender zu verschaffen. Ausserdem könne die Identität des Absender dazu verwendet werden, um Missbrauch vorzubeugen.



Die neue Sealed-Sender-Funktion steht in der Beta-Version von Signal bereits zur Verfügung.
Quelle: Signal

Bei der neuen Sealed-Sender-Funktion in Signal nutzen die Entwickler für die Authentifizierung hingegen eine Kombination aus kurzlebigen Absenderzertifikaten und Delivery-Token. Die Zertifikate beinhalten die Telefonnummer des Clients, den öffentlichen Identifikationsschlüssel sowie einen Ablaufzeitstempel. Beim Versand der Nachrichten können diese Zertifikate vom Client mit aufgenommen werden, während der Empfänger-Client die Gültigkeit der Zertifikate prüfen kann. Da die Zertifikate für die Übertragung genau wie die übrigen Nachrichteninhalte verschlüsselt werden, fallen auf den Signal-Servern keine nutzbaren Metadaten an, die Rückschlüsse auf den Absender zulassen.

Daneben werden ebenfalls verschlüsselte Delivery-Tokens übertragen, die sich aus dem Profil des Empfängers herleiten. Weil diese Profile allerdings nur für berechtigte Kontakte einsehbar sind, kann Missbrauch hier prinzipiell ausgeschlossen werden. Damit ist die neue Versandoption «Sealed Sender» aber auch nur beim Austausch mit persönlichen Kontakten einsetzbar.

In der Beta-Version des Signal-Messengers kann die neue Funktion bereits getestet werden.

Signal beliefert Messenger-Dienste mit Kryptografie

Die für Signal entwickelte Ende-zu-Ende-Verschlüsselung kommt mittlerweile auch in zahlreichen Messenger-Diensten zum Einsatz. Neben WhatsApp und Facebook setzt auch Microsofts Skype auf die freie kryptografische Lösung. Bleibt abzuwarten, ob auch weitere Datenschutz-Features, wie Sealed Sender, ihren Weg in die kommerziellen Lösungen der grossen Anbieter finden.

Autor(in)
Stefan Bordel

Folgen auf