PrivaSphere™

PrivaSphere
Secure Messaging

Quorum
the smart way to even more confidentiality

PrivaSphere Secure Messaging

Quorum Verschlüsselung

for more information and contact:

https://www.privasphere.com

PrivaSphere AG, Jupiterstrasse 49, 8032 Zürich — Supportline: +41 43 500-MAIL (6245)
https://www.privasphere.com/info@privasphere.com

Quorum[1] - *the smart way to even more confidentiality*

Um erhöhten Sicherheitsbedürfnissen von Kundendaten Rechnung zu tragen, hat die PrivaSphere AG eine **zusätzliche Verschlüsselung der Kundendaten** im PrivaSphere Secure Messaging Service entwickelt, die ohne asymmetrischen Endbenutzerschlüssel auskommt[2]. Diese kann durch den Sender optional zugeschaltet werden - zurzeit im Beta-Test.

Dabei werden die Nutzdaten mit einem vom System generierten symmetrischen Schlüssel auf dem System zusätzlich verschlüsselt. Dieser Schlüssel wird dem Empfänger mit der Abholeinladung im Link versandt. Zusätzlich werden sie auch noch mit einem auf dem Server liegenden und automatisch generiertem Schlüsselmaterial verschlüsselt.

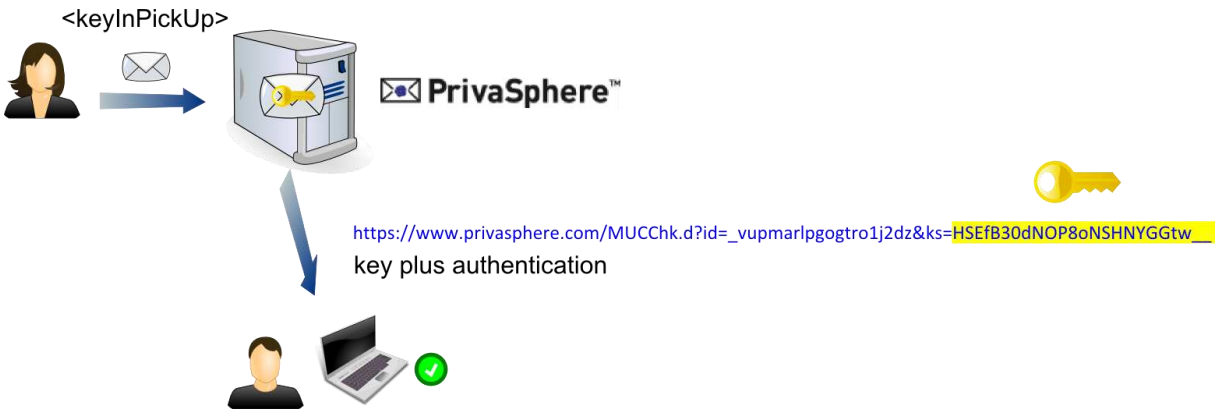

Abbildung: Quorum Verschlüsselung auf PrivaSphere Secure Messaging

Beim Empfang der sicheren Mail werden demnach benötigt:

1. Link mit dem Schlüssel (Beziehungsvertraulichkeit gewahrt!)
2. Authentisierung des Benutzers (mit MUC und/oder Passwort oder Zertifikat)
3. Individuelles Server Schlüsselmaterial (nicht sichtbar für den Benutzer)

Vorteile:

- Erhöhte Vertraulichkeit (das Plattform Passwort alleine gibt noch keinen Zugriff auf Inhalt)
- Verschiedene, neue Anwendungs-Szenarien, wie z.B. 4- bzw. X-Augenprinzip des Zugriffs möglich[3]
- Speicherung nach Rechtssprechungsräumen möglich[4]
- Verkürzen der Exposure (mögliche Einsehbarkeit) des Plattformbetreibers auf den Versand- und Abholzeitpunkt beschränkt.
- Keine Empfänger-seitige Grössenprobleme und mehrfach-Speicherung/3-fach-Übertragung im Vergleich zu Verfahren mit denselben Sicherheitsambitionen.

[1] Zum Patent angemeldet
[2] z.B. PGP Schlüssel oder S/Mime Encryption Zertifikat
[3] Verfügbar in Version 1.1
[4] Verfügbar mit Quorum Appliance