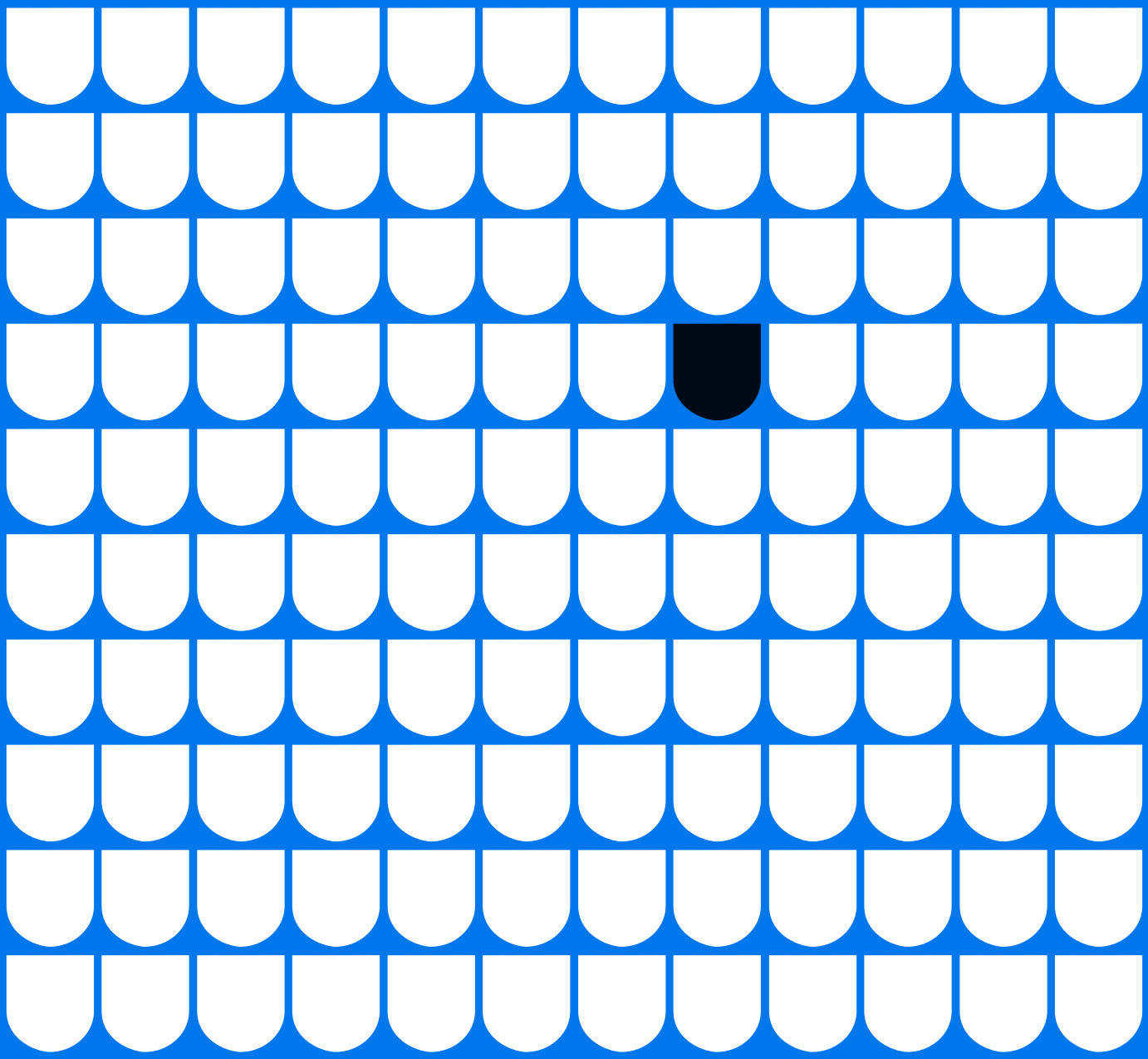


Ende-zu-Ende Verschlüsselung

compentum.de

Ein Leitfaden zur sicheren Kommunikation
und Verschlüsselung von sensiblen Daten.

Stand: 20.02.2023 v.1.0.0

compentum™

Inhaltsverzeichnis

compentum™

Einleitung

Im digitalen Zeitalter, in dem Datenschutz und Datensicherheit zu den wichtigsten Anliegen geworden sind, spielen Hinweisgebersysteme eine immer wichtigere Rolle. Diese Systeme ermöglichen es Whistleblowern, vertrauliche Informationen sicher an Organisationen zu melden, ohne Angst vor unfreiwilliger Identifizierung haben zu müssen.

Eine Hinweisgeber-Software mit clientseitiger Ende-zu-Ende-Verschlüsselung stellt hierbei eine wichtige und sichere Lösung dar. Durch die Verwendung von Ende-zu-Ende-Verschlüsselung werden die Daten so verschlüsselt, dass nur der Empfänger sie entschlüsseln und lesen kann. Dies bietet einen zusätzlichen Schutz gegen Datenmissbrauch und garantiert, dass die Meldungen vertraulich bleiben.

In diesem Whitepaper werden sowohl die technischen als auch die geschäftlichen Aspekte einer Hinweisgeber-Software mit Ende-zu-Ende-Verschlüsselung untersucht. Wir werden die Vorteile besprechen, die diese Art von Software für Organisationen bietet, wie sie den Datenschutz und die Datensicherheit verbessern und wie sie in der Praxis angewendet werden kann.

Zusammenfassend soll dieses Whitepaper eine umfassende Übersicht über die Vorteile und Möglichkeiten einer Hinweisgeber-Software mit Ende-zu-Ende-Verschlüsselung bieten und dabei sowohl die technischen als auch die geschäftlichen Aspekte betrachten. Durch die Verwendung einer solchen Software können Organisationen ihre Verantwortung gegenüber den Whistleblowern wahrnehmen und gleichzeitig sicherstellen, dass die Meldungen vertraulich bleiben.

compentum™

Anforderungen

Die Ende-zu-Ende Verschlüsselung muss folgende technische und geschäftliche Anforderungen erfüllen.

Sicherheitseigenschaften

Die folgenden Sicherheitseigenschaften müssen erfüllt sein:

- Zugriff auf den Ciphertext darf keinen Rückschluss auf die Nachricht oder den Whistleblower geben
- Die öffentlichen Schlüssel der Benutzer müssen auditierbar sein
- Wenn ein Benutzer aus einem verschlüsselten Portal entfernt wurde, sollte er kein relevantes Schlüsselmaterial mehr besitzen, um Meldungen, die in der Zukunft aktualisiert oder erstellt werden, zu verschlüsseln.

Bibliotheken

Verwendung weitverbreitetetr und getesteter Bibliotheken für Kryptoprimitive:

- Die verwendete Bibliothek für Kryptoprimitive muss weit verbreitet eingesetzt werden.
- Die verwendete Bibliothek für Kryptoprimitive muss erfolgreich auf Sicherheit überprüft worden sein.

Zentrale Datenwiederherstellung

Das grundlegende Konzept von Ende-zu-Ende Verschlüsselung ist Daten und Kommunikation vor unberechtigten Dritten zu schützen. In der Realität passiert es jedoch, dass Benutzer ihre Schlüssel oder Passwörter vergessen oder verlieren.

Im Enterprise Bereich ist es daher keine Option den Zugriff auf die Daten zu verlieren. Deswegen bietet compentum eine zentrale Datenwiederherstellung an, die folgende Möglichkeiten bietet:

- Für jedes Unternehmen wird ein Schlüsselpaar generiert
- Jede Meldung wird zusätzlich mit dem Unternehmensschlüssel verschlüsselt
- Der private Schlüssel kann verschlüsselt auf der Instanz gespeichert oder exportiert werden und z.B. physikalisch gespeichert werden.

Akzeptierter Funktionsverlust

Durch die Ende-zu-Ende Verschlüsselung hat der Server keinen Zugriff auf die relevanten Meldungsdaten. Daher ist der Verlust bestimmter Funktionen akzeptabel:

- Volltextsuche der Meldungen
- Suche / Filterung nach Kontaktinformationen des Hinweisgebers
- Durchsuchbare Dateianhänge

Technische Implementierung

Die Verschlüsselung basiert auf einer Mischung aus Asymmetrischer- und Symmetrischer Verschlüsselung um das höchste Maß an Datensicherheit und Komfort in einem Mehrbenutzersystem zu gewährleisten.

Darüber hinaus wird ausschließlich clientseitige Ende-zu-Ende Verschlüsselung verwendet.

Clientseitige Ende-zu-Ende-Verschlüsselung ist ein Verfahren, bei dem die Daten vor der Übertragung von dem Absender verschlüsselt und erst am Empfänger wieder entschlüsselt werden. Hierbei bleiben die Daten jederzeit geschützt, da sie nur auf den Geräten des Absenders und des Empfängers lesbar sind und nicht von Dritten eingesehen werden können.

Diese Methode ist am besten, da sie ein hohes Maß an Datensicherheit bietet und gleichzeitig die Privatsphäre des Benutzers schützt. Weil die Daten auf keinem Server gespeichert werden, kann auch kein Dritter Zugang zu den Daten erlangen, wodurch ein hoher Schutz gegen Datenmissbrauch und Hackerangriffe gewährleistet wird.

Somit werden die Daten nur im Browser der Ombudsperson oder des Hinweisgebers entschlüsselt.

Algorithmen

RSA-OAEP

Für jeden Benutzer (Inhaber, Ombudsperson) wird ein 4096 bit langer öffentlicher und privater RSA-OAEP Schlüssel generiert.

AES-GCM

Für jede Meldung wird ein einzigartiger 256 bit langer AES GCM Schlüssel generiert.
Für die Verschlüsselung der privaten Schlüssel die im System gespeichert werden wird auch AES-GCM verwendet.

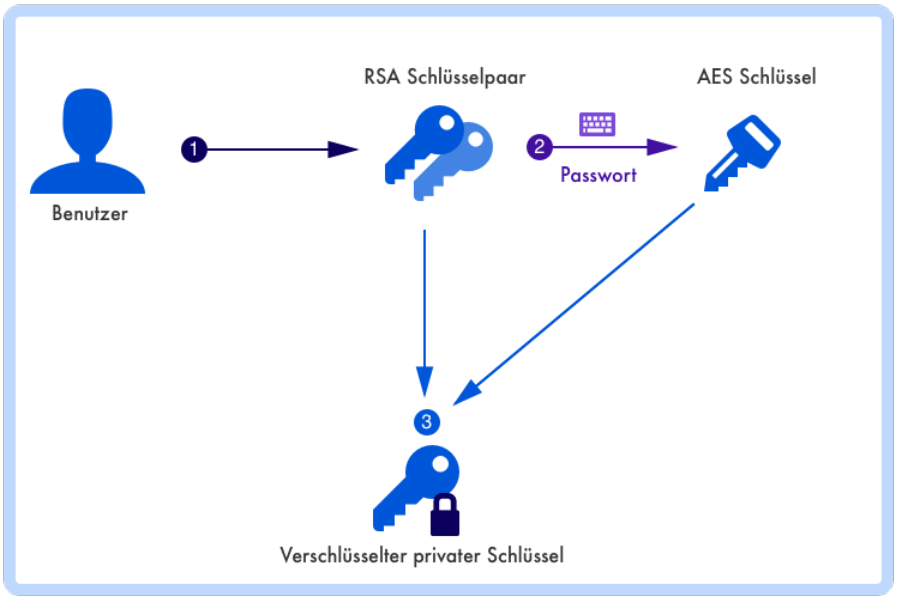
PBKDF2

Wird verwendet um kryptografisch sichere Schlüssel aus Passwörtern zu generieren um die privaten Schlüssel verschlüsselt zu speichern.

Konto erstellen

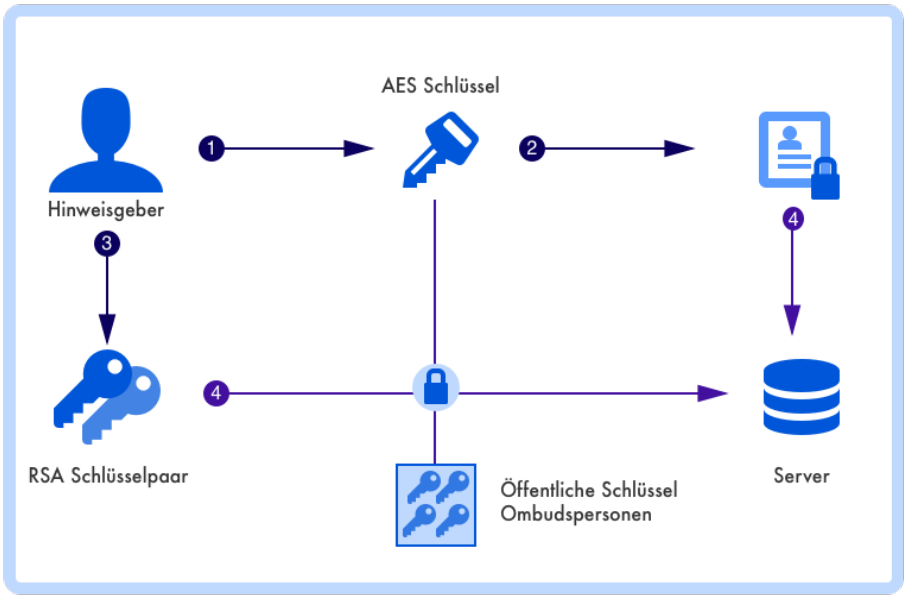
1. Für jeden Benutzer wird ein RSA Schlüsselpaar bestehend aus öffentlichem und privaten Schlüssel generiert.
2. Mittels PBKDF2 wird aus dem Benutzerpasswort ein kryptografischer Schlüssel erzeugt.
3. Der private Schlüssel wird mit dem vorher erstellten Schlüssel mittels AES-GCM verschlüsselt

Das gleiche Verfahren wird verwendet, wenn ein Unternehmen erstellt wird. Siehe „Zentrale Datenwiederherstellung“.



Meldung einreichen

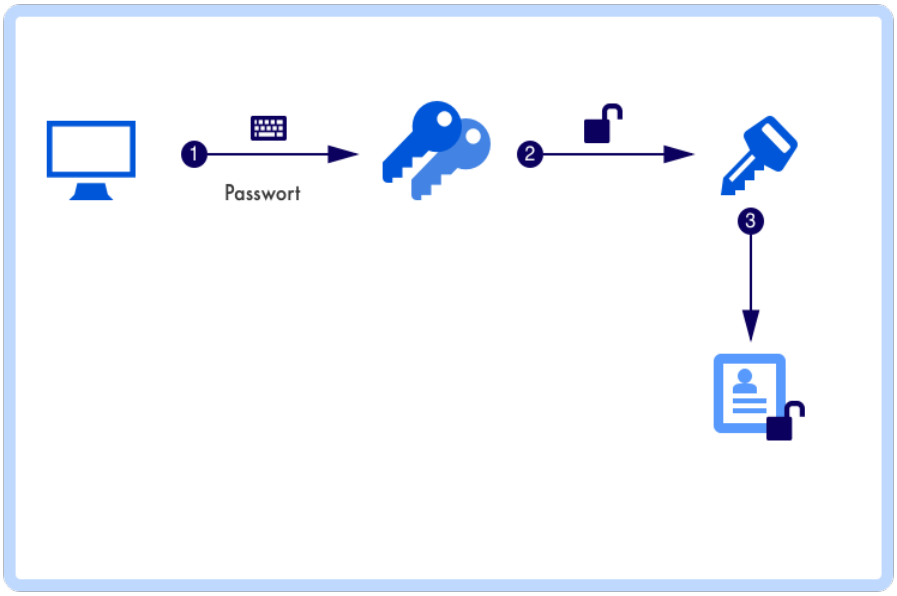
1. Für jede Meldung wird ein einzigartiger 256 bit AES Schlüssel erzeugt. Im folgenden „Meldungsschlüssel“ genannt.
2. Die relevanten Meldungsdaten werden mit dem Meldungsschlüssel verschlüsselt.
3. Für den Hinweisgeber wird ein RSA Schlüsselpaar erzeugt (öffentlicher- und privater Schlüssel).
4. Der Meldungsschlüssel wird jeweils mit dem öffentlichen Schlüssel aller Zugangsberechtigten verschlüsselt und gespeichert.



Zugriff auf eine Meldung

Beim Zugriff auf eine Meldung wird prinzipiell das gleiche Verfahren verwendet, ungeachtet ob es sich um einen Hinweisgeber oder Ombudsperson handelt.

1. Der private Schlüssel wird mit dem Benutzerpasswort oder Meldungspasswort entschlüsselt.
2. Der Meldungsschlüssel wird mit dem privaten Schlüssel entschlüsselt.
3. Die Meldungsdaten werden mit dem Meldungsschlüssel entschlüsselt.



Zugriffsberechtige ändern

Da eine clientseitige Ende-zu-Ende Verschlüsselung verwendet wird, passiert das Ver- und Entschlüsseln direkt im Browser. Daher muss beim Hinzufügen eines Benutzers zu einem Meldeportal, der Meldungsschlüssel mit dem öffentlichen Schlüssel dieses Benutzers verschlüsselt werden. Beim entfernen eines Benutzer, muss diese Prozedur wiederholt werden, allerdings ohne den betroffenen Schlüssel des entfernten Benutzers.

1. Inhaber fügt einen Benutzer, einem Meldeportal hinzu. (Oder entfernt diesen)
2. Der private Schlüssel des Inhabers wird entschlüsselt
3. Der Meldungsschlüssel jeder Meldung wird entschlüsselt und mit den öffentlichen Schlüsseln der Zugangsberechtigten verschlüsselt