

FlexiTrust 3.0 ReCryption Agent for MS Outlook®

Bei der kryptografischen Absicherung von E-Mail müssen alte Schlüssel und Zertifikate normalerweise aufwändig archiviert werden.

Der FlexiTrust ReCryption Agent for MS Outlook® löst dieses Problem durch Umschlüsseln, so dass immer nur ein Schlüssel pro Benutzer verwaltet werden muss. Dies erhöht die Ausfallsicherheit und vereinfacht zudem den Einsatz von Chipkarten.

Absicherung von E-Mail

Zunehmend werden in Unternehmen E-Mails digital signiert oder verschlüsselt, denn dieses Kommunikationsmedium ist an sich nicht sehr sicher: E-Mails können vergleichsweise einfach mitgelesen oder auch nur versehentlich fehlgeleitet werden. Zum Schutz sensibler Daten sollen diese daher unbedingt verschlüsselt verschickt und auch verschlüsselt gespeichert werden.

Zertifikate und private Schlüssel

Um verschlüsselte und signierte E-Mails senden und empfangen zu können, benötigt ein Benutzer lediglich ein so genanntes Zertifikat und den zugehörigen kryptografischen privaten Schlüssel. Nur wer diesen privaten Schlüssel besitzt, kann die verschlüsselten Nachrichten lesen. Über Zertifikate wird eine Verbindung zwischen Schlüssel und dem Inhaber vergleichbar einem Ausweis hergestellt. Zertifikate werden daher oft auch als digitale IDs bezeichnet, denn sie enthalten den Namen der Person, der der Schlüssel gehört, deren E-Mail-Adresse, sowie den Firmennamen. Aus Sicherheitsgründen wird ein Zertifikat – genau wie auch ein Ausweis – nur für eine begrenzte Zeit ausgestellt, danach muss es erneuert werden.

Zertifikats- und Schlüsselerneuerung

Mit einem neuen Zertifikat wird aus Sicherheitsgründen üblicherweise auch gleichzeitig der private Schlüssel des Inhabers gewechselt. Neben der turnusmäßigen Erneuerung kann dieser Fall z.B. auch auftreten, wenn ein Unternehmen auf eine leistungsfähigere Public Key Infrastruktur (PKI) zur Bereitstellung der Zertifikate migriert oder sich für die Einführung von Chipkarten entscheidet.

Mit einem neuen privaten Schlüssel sind die mit dem bisherigen Schlüssel verschlüsselten Nachrichten nicht mehr lesbar. Die Archivierung aller vorhergehenden privaten Schlüssel (sowie ggf. auch der jeweiligen Chipkarten) ist jedoch eine komplexe und zudem sicherheitskritische

Aufgabe: Geht ein privater Schlüssel verloren oder wird die Chipkarte, auf der er gespeichert ist, beschädigt, so kann dies einen teuren Datenverlust zur Folge haben, da auf der Festplatte verschlüsselt gespeicherte E-Mails unwiederbringlich verloren sind.

Der FlexiTrust 3.0 ReCryption Agent for MS Outlook® löst dieses Problem, indem es die E-Mails für den neuen Schlüssel lesbar macht. Dieses „Umschlüsseln“ hat den großen Vorteil, dass immer nur ein privater Schlüssel pro Benutzer verwaltet werden muss. Zudem lassen sich die E-Mails so umschlüsseln, dass sie für mehrere Personen lesbar sind; dies mindert die Gefahr des Datenverlusts erheblich.

Funktionsweise

FlexiTrust ReCryption Agent verarbeitet alle E-Mails in einem Outlook® - Ordner, die für ein bestimmtes Zertifikat verschlüsselt werden. Alle verschlüsselten Nachrichten werden inklusive möglicher Dateianhänge zunächst mit dem alten privaten Schlüssel entschlüsselt und dann für ein oder mehrere Zertifikate neu verschlüsselt, die sich vom Benutzer frei wählen lassen. Das Werkzeug ist dabei sehr einfach und sicher zu bedienen.

FlexiTrust ReCryption Agent unterstützt Outlook® sowohl als eigenständige Applikation wie auch in Verbindung mit einem Microsoft Exchange Server® und ist damit perfekt für den Unternehmens Einsatz geeignet. Es lässt sich problemlos mit dem FlexiTrust 3.0 Out-of-the-Box ID-Management System kombinieren, um eine Migration oder auch nur den täglichen Betrieb zu vereinfachen. Auch Chipkarten, die nur sehr wenige private Schlüssel speichern können, lassen sich somit zur Absicherung von E-Mail verwenden.

Über FlexSecure

"Die FlexSecure GmbH ist einer der führenden Anbieter von innovativen Sicherheitslösungen in der Informationstechnologie. In enger Kooperation mit namhaften Forschungsinstituten entwickelt FlexSecure eSecurity-Anwendungen zur Autorisierung, Authentifizierung, Integritätsprüfung und Verschlüsselung auf der Basis von digitalen Signaturen.

Seit dem Gründungsjahr 2000 hat sich FlexSecure zu einem international anerkannter Vorreiter für sichere Informationen und sichere Identität in der digitalen Welt entwickelt.

Lösungen von FlexSecure sorgen dafür, dass elektronische Geschäftsprozesse sicherer, einfacher und wirtschaftlicher werden. So liefert Flexsecure z.B. die Zertifizierungstechnologie für den neuen Reisepass. Kunden sind u.a. das Bundesamt für Sicherheit in der Informationstechnologie (BSI), die Bundesnetzagentur, führende Versicherungs- und Telekommunikationsunternehmen, das Zweite Deutsche Fernsehen und das Deutsche Gesundheitsnetz."