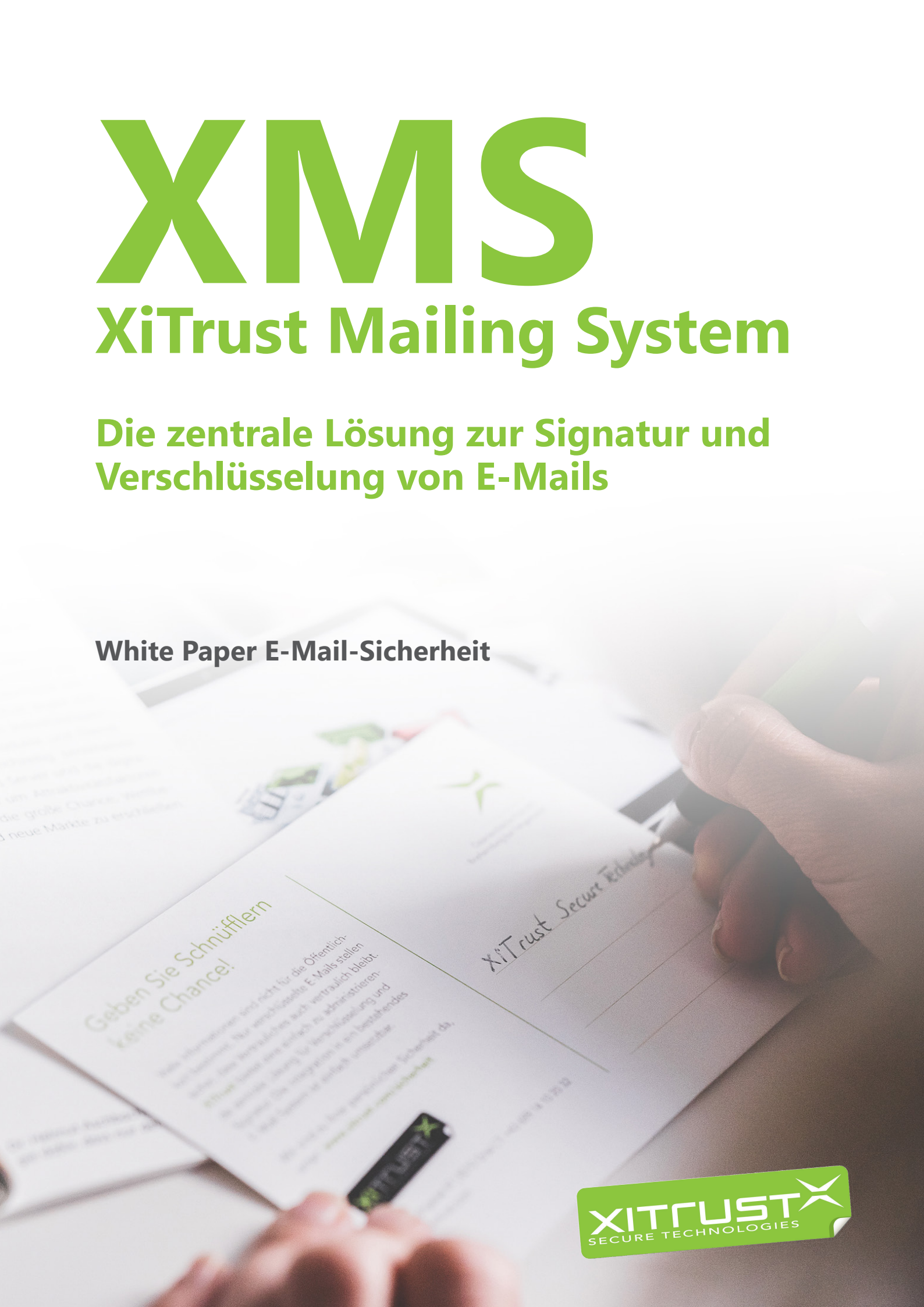
XMS

XiTrust Mailing System

Die zentrale Lösung zur Signatur und Verschlüsselung von E-Mails

White Paper E-Mail-Sicherheit



1 EINLEITUNG

Immer mehr Unternehmen entscheiden sich beim Austausch sensibler Daten per E Mail für den sicheren Weg: Mitarbeiterdaten, Kennzahlen und andere Geschäftsdokumente werden nur noch signiert und verschlüsselt versendet. **XiTrust Secure Technologies** unterstützt diese Entwicklung seit vielen Jahren mit innovativen Lösungen für alle Branchen.

Mit dem **XiTrust Mailing System (XMS)** bietet XiTrust seinen Kunden eine **zentrale Signatur- und Verschlüsselungslösung**, die alle Absender eines Unternehmens **automatisch mit personenbezogenen S/MIME Zertifikaten** ausstattet.

XMS ist einfach und ohne zusätzliche Installation von Software am E-Mail-Client in bestehende E-Mail-Infrastruktur zu integrieren. **XMS** wird wie eine Firewall dem E-Mail-System vorgeschaltet. Durch Erweiterung eines E-Mail-Systems um elektronische Signatur und Verschlüsselung führen Anwender mit **XMS Briefkuvert, Siegel und Unterschrift** auf elektronischer Ebene ein. Kundenspezifisch können die entsprechenden E-Mail-Wege an die Anforderungen der Gesamtlösung angepasst werden.

XMS bietet optional die Möglichkeit auch solchen Empfängern vertrauliche E-Mails zu schicken, die noch keine Verschlüsselungs-Infrastruktur implementiert haben. Dieses White Paper beschreibt die **Rundum-Lösung** von **XiTrust Secure Technologies** für garantierte E-Mail-Sicherheit. Maximaler Komfort in der Betriebsführung/ausgelegt für große Unternehmen.

2 MOTIVATION

Im digitalen Zeitalter erlebt die Sicherung des Briefgeheimnisses eine Renaissance. Das liegt daran, dass der wichtigste Kommunikationskanal für persönliche Nachrichten mit sensiblen Inhalten, nämlich die gewöhnliche E-Mail, im Prinzip genauso leicht zu auszuhebeln ist, wie man einen Brief öffnet. **Standardmäßig versendete E-Mails sind nicht einmal sicherer als Postkarten.** Ihr Inhalt kann ohne großen Aufwand mitgelesen oder verändert werden. Die Sicherheit, dass der Absender auch wirklich der Absender ist, existiert bei herkömmlichen E-Mails ebenfalls nicht. **Mit gewöhnlichen E-Mails ist die Wahrung des Briefgeheimnisses ausgeschlossen.**

So wie in früheren Zeiten durch die „analoge" Verletzung des Briefgeheimnisses finanzielle Schäden entstehen konnten, gilt dies heute für unzureichend verschlüsselte E-Mails umso mehr. Die Schäden für Unternehmen sind in Einzelfällen bereits in die Millionen Euro gegangen. Es ist deshalb auch naheliegend, dass die zuverlässige Sicherung von E-Mails in der IT-Welt den Terminus **„Enveloping"** kennt. Nur mit dem Unterschied, dass der digital verschlossene Briefumschlag mit der passenden **E-Mail-Sicherheits-Lösung** nicht aufgerissen werden kann.

XiTrust Secure Technologies hat mit dem **XiTrust Mailing System (XMS)** einen überzeugenden Weg gefunden, das Briefgeheimnis per E-Mail zu gewährleisten und versetzt Unternehmen in die Lage, jederzeit die Kontrolle über den eigenen Nachrichtenfluss zu behaupten. **Die heute zuverlässigste Methode zur Wahrung des Briefgeheimnisses bei E-Mails liegt allein in der Prävention durch ausgereifte Sicherheits-Systeme wie XMS.**

KOMPAKT

- Standard-E-Mails sind nicht sicherer als Postkarten
- Datenintegrität und -authentizität sind bei Standard-E-Mails nie gewährleistet
- Manipulierte Mailinhalte und gefälschte Absenderdaten können Schäden in Millionenhöhe verursachen
- Prävention ist die zentrale Strategie, um E-Mail-Missbrauch zu verhindern

2.1. Exkurs: Briefgeheimnis

Das Briefgeheimnis gehört zu den wichtigsten Errungenschaften freiheitlicher Gesellschaften. Es wurde als wichtiges Element zum Schutz der Privatsphäre und zur freien Entfaltung der Persönlichkeit etwa ab Mitte des 19. Jahrhunderts in Europa gesetzlich festgeschrieben. Der gesetzliche Schutz des Briefgeheimnisses in Österreich jährt sich in diesem Jahr übrigens zum 150sten Mal: Es trat mit der Dezemberverfassung von 1867 in Kraft.

Die Strafen für Verletzung des Briefgeheimnisses waren in den einzelnen Staaten zum Teil drakonisch – ein Hinweis auf die Bedeutung, die seiner Unverletzlichkeit beigemessen wurde. Dabei ging es um mehr als die Wahrung der Privatsphäre. Es ging dabei auch um die Unverletzlichkeit geistigen Eigentums und Autorschaft. **Die Gesellschaften hatten erkannt, welchen Wert Informationen darstellen und welche Verluste Informationen in den falschen Händen nach sich ziehen.**

3 WAS UNTERSCHEIDET XMS VON ANDEREN E-MAIL-SICHERHEITS-LÖSUNGEN?

3.1 Das Gateway-Zertifikat

Es gibt heute verschiedene hochwertige Methoden, Mailinhalte per Verschlüsselung und Signatur zu schützen. Zu den gängigsten zählt das **Gateway-Zertifikat.** An zentraler Stelle werden dabei E-Mails mit einem Zertifikat versehen, das zur Signatur und Verschlüsselung von Mailinhalten unabdingbar ist. Der Empfänger kann sich der Integrität des Inhalts und der Authentizität des Absenders sicher sein. Absender ist bei Gateway-Zertifikaten nie eine Einzelperson, sondern immer das aussendende Unternehmen. **Der Absender arbeitet hier mit einem einzigen Zertifikat für alle.**

Diese Methode sorgt so lange für zufriedenstellende Ergebnisse, wie die Anzahl der E-Mails und damit ihrer Empfänger überschaubar bleibt. Für kleinere Unternehmen kann die Sicherheit eines Gateway-Zertifikats deshalb als ausreichend angesehen werden.

3.2 Viele E-Mails: höhere Sicherheitsanforderungen

Komplexer wird die Thematik E-Mail-Sicherheit, sobald eine Vielzahl an E-Mails pro Tag zu versenden ist. Bei größeren Unternehmen können das leicht mehrere tausend sein. Hier steigt die Wahrscheinlichkeit, dass es zu so genannten „Mismatchings" kommt. Viele Client-Server auf Empfängerseite durchforsten nämlich zunächst noch das Zertifikat auf den Namen des Absenders. Der steht aber im Gateway-Zertifikat nicht drin, dort findet sich bei dieser Lösung nur der

3 WAS UNTERSCHEIDET XMS VON ANDEREN E-MAIL-SICHERHEITS-LÖSUNGEN?

Firmenname des Absenders. Die Folge: Der zumeist veraltete Server verweigert aufgrund dieses fehlenden Übereinstimmungsmerkmals die Annahme der E-Mail, obwohl sie verschlüsselt und signiert ist. Es kommt zu Verzögerungen bis zur Klärung des Sachverhalts – mögliche Wettbewerbsnachteile inklusive.

An dieser Stelle setzt **XMS** an. Wie ein Gateway-Zertifikat auch, arbeitet **XMS** mit Verschlüsselung und Signatur. Der Unterschied besteht zuerst in der Beschaffenheit des Zertifikats. Denn das ist bei **XMS** immer ein **personenbezogenes Einzelzertifikat.** Jeder Absender kann der E-Mail persönlich zugeordnet werden, Mismatches werden damit ausgeschlossen.

3.3 Unternehmensweites Roll-Out von Zertifikaten durch XMS

Bleibt die Frage, auf welchem Weg Unternehmen ihre Mitarbeiter mit Zertifikaten ausstatten. Selbstverständlich können sie das Roll-Out von Einzelzertifikaten selbst in die Hand nehmen. Dies erfordert bei größeren Unternehmen mit einer Vielzahl von Absendern allerdings einen erheblichen administrativen Aufwand. Die E-Mail-Clients müssen jeder für sich einzeln mit einem Zertifikat ausgestattet werden. Dies ist in der Praxis mit einem zusätzlichen Schulungsaufwand für die Mitarbeiter verbunden, die erforderliche Akzeptanz des Verfahrens durch die Mitarbeiter noch nicht berücksichtigt.

XMS erledigt die gesamte Arbeit selbst und nimmt der Administration den Aufwand der Verwaltung ab. Personenbezogene Einzelzertifikate werden durch XMS automatisch ausgestellt und zentral verwaltet. Bei jeder ausgehenden, als vertraulich gekennzeichneten E-Mail prüft XMS: Hat der Absender bereits ein persönliches Zertifikat? Ist dieses noch nicht hinterlegt, wird es von einem **eIDAS-konformen**, zertifizierten Trust-Center, in diesem Fall **XiTrust-Partner-Unternehmen A-Trust, automatisch ausgestellt.** So erhalten alle Mitarbeiter, die vertrauliche E-Mails aussenden, ihr persönliches Einzelzertifikat ohne jeden zusätzlichen Aufwand. Versehen mit persönlichem Zertifikat geht die E-Mail signiert und verschlüsselt an den Empfänger, der sich sicher sein kann, von welcher Person die Nachricht stammt und dass der Inhalt unangetastet geblieben ist.

Damit übernimmt **XMS** in Automation das **unternehmensweite Roll-Out mit S/MIME Einzelzertifikaten** in beliebiger Anzahl.

KOMPAKT

- XMS stellt die Echtheit der Inhalte und die Authentizität des Absenders individuell sicher.
- XMS bietet denselben Komfort wie ein einzelnes Gateway-Zertifikat, versehen mit allen Vorteilen des personenbezogenen Einzelzertifikats.
- XMS ermöglicht es, dass der Absender einer Mail immer persönlich zuzuordnen ist.
- XMS erstellt personenbezogene Einzelzertifikate vollautomatisch und zentral.
- XMS übernimmt das unternehmensweite Roll-Out von Einzelzertifikaten in Vollautomation.

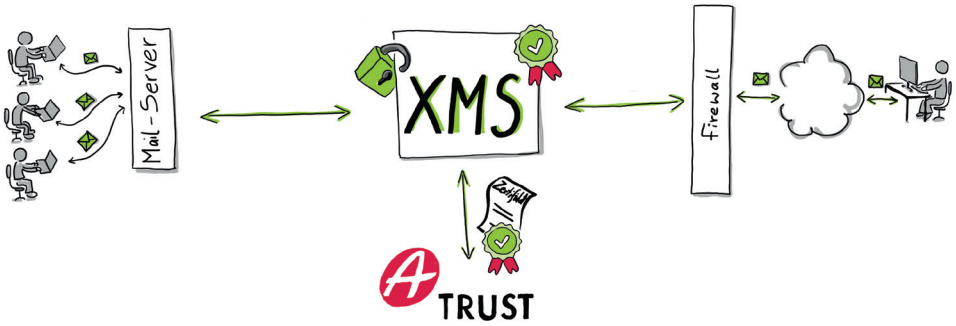
4 GRUNDLAGEN: XMS – DIE ZENTRALE SIGNATUR UND VERSCHLÜSSELUNGSLÖSUNG

Um **XMS** in den Unternehmens-Workflow zu integrieren, ist keine zusätzliche Software notwendig. **XMS** wird an zentraler Stelle in die bestehende E-Mail-Infrastruktur eingebunden, ohne dass diese angepasst werden müsste. **XMS** ist einfach zu administrieren und mit **keinerlei Schulungsaufwand** für Mitarbeiter verbunden.
Mit dem **zentralen Ansatz** lassen sich unternehmensweite **Sicherheits-Policies einfach durchsetzen.** So lässt sich einfach steuern,

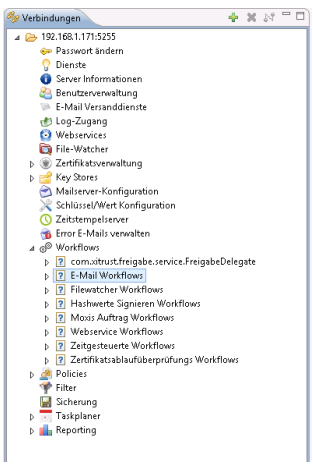
- dass die Kommunikation mit ausgewählten Kunden ausschließlich verschlüsselt erfolgen soll.
- dass E-Mails von einem Kommunikationspartner nur dann akzeptiert werden, wenn sie von ihm elektronisch signiert und damit eindeutig ihm zuzuordnen sind.

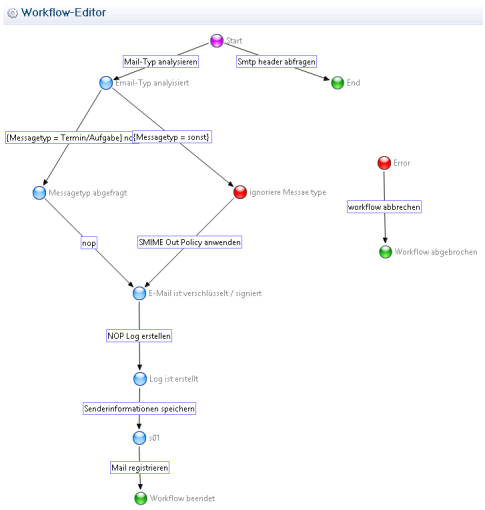
Die E-Mail-Lösung von XiTrust unterstützt **international anerkannte Standards** für elektronische Signatur und Verschlüsselung, wie etwa **S/MIME, PGP**[1]**, oder X.509.** Dadurch wird sichergestellt, dass der E-Mail-Verkehr über **XMS** mit dem **Empfänger problemlos zusammenarbeitet.**

ABLAUF



PRODUKT





[1] Bei PGP wird aus Effizienzgründen nur die PGP Mime Version unterstützt

5 DIE SIGNATUR- UND VERSCHLÜSSELUNGS-LÖSUNG XMS IM DETAIL

5.1 Module

Das **XMS-Paket** E-Mail-Sicherheit besteht aus den folgenden Modulen:

- **Einzelzertifikate**
  XMS kann on Demand oder zeitgesteuert Zertifikate für User bei der A-Trust beantragen. Das ist sowohl für die initiale Beantragung als auch für eine Verlängerung des Zertifikats möglich. Die Zertifikate können für S/MIME Signatur und Verschlüsselung benutzt werden.

- **Signaturerzeugung**
  Erzeugung digitaler Signaturen für E-Mails nach den offenen Standards S/MIME und X.509; gewährleistet höchste Zuverlässigkeit und Kompatibilität.

- **Signaturprüfung**
  Prüfen digitaler Signaturen auf eingehenden E-Mails nach den offenen Standards S/MIME und X.509 inklusive aller für eine Komplettprüfung notwendigen Verzeichnisabfragen; Möglichkeit der Generierung eines endbenutzerfreundlichen Signaturprüfberichts.

- **Verschlüsselung und Entschlüsselung**
  E-Mails werden nach den etablierten Sicherheitsstandards S/MIME und PGP chiffriert und dechiffriert.

5.2 Sichere E-Mails für alle: PDF-E-Mail-Verschlüsselung mit XMS

Um auch mit Geschäftspartnern vertraulich kommunizieren zu können, die keine Verschlüsselungs-Infrastruktur implementiert haben, verfügt XMS optional über die Möglichkeit, einen passwortgeschützten PDF-Container zu übermitteln und das Passwort per SMS oder telefonisch zu erhalten. Der Vorteil dieser Art der Verschlüsselung liegt darin, dass der **Empfänger keinerlei Vorbereitungen treffen muss, um verschlüsselte Dokumente erhalten zu können.**

5.2.1 So funktioniert's: Der Ablauf im Detail

1. Der E-Mail-Versender stellt die E-Mail mit den sensiblen Inhalten zusammen und sendet sie an den Empfänger.
2. XMS wandelt die ursprüngliche E-Mail in ein verschlüsseltes PDF-Dokument um, wobei alle Beilagen der E-Mail ins PDF-Dokument übernommen werden.
3. XMS sendet diese E-Mail jetzt an den Empfänger mit dem verschlüsselten PDF-Dokument als Beilage, dazu den Hinweis, dass das verschlüsselte PDF-Dokument nur mit Hilfe eines Passworts geöffnet, also entschlüsselt, werden kann.
4. XMS sendet dann eine E-Mail mit dem für die Verschlüsselung des PDF-Dokuments verwendeten Passwort an den E-Mail Absender.
5. Schließlich erfragt der Empfänger das Passwort für das verschlüsselte PDF-Dokument beim E-Mail-Absender, und kann damit das PDF-Dokument nach Eingabe des Passworts in seinem Adobe Reader lesen.

6 DIE LÖSUNG VON XITRUST SECURE TECHNOLOGIES

6.1 Direkte SSL-Verbindung mit dem empfangenden E-Mail-Server

6.1.1 Funktionsprinzip

E-Mail-Server kommunizieren untereinander über das SMTP-Protokoll. Dieses ist als unverschlüsseltes Protokoll konzipiert. Es wurde jedoch um die Möglichkeit erweitert, dass der Server **eine Verschlüsselungsoption anbieten kann.** Dieses Verfahren des Anbietens wird als STARTTLS bezeichnet und ist im RFC3207[2] geregelt. Dabei wird auf Transportebene ein verschlüsselter Kanal etabliert und die E-Mail verschlüsselt übertragen. Die E-Mail selbst wird nicht via S/MIME oder PGP verschlüsselt. Man kann damit also den Weg der E-Mail zwischen zwei SMTP-Servern absichern.

6.1.2 Die STARTTLS-Funktion bei XMS

Die E-Mail-Komponenten bei **XMS** unterstützen STARTTLS als Option, wenn **XMS** als eingehender E-Mail-Server benutzt wird. Hier kann in der Grundkonfiguration des SMTP-Dienstes ein Zertifikat ausgewählt werden, mit dem die verschlüsselte Verbindung auf Transportebene hergestellt wird.

Wird **XMS** als ausgehender E-Mail-Server eingesetzt, können verschiedene Transports angelegt werden. Ein Transport definiert, mit welchen Workflow eine E-Mail verarbeitet werden soll und wie die E-Mail zugestellt wird. Welcher Transport für eine E-Mail zuständig ist, wird durch Regeln festgelegt, die z.B. E-Mail-Adresse des Absenders oder des Empfängers enthalten. Für jeden Transport kann bei den Zustelloptionen festgelegt werden, ob eine E-Mail an den SMTP-Server verschlüsselt übertragen werden soll oder nicht.

Dadurch ist es z.B. möglich zu erzwingen, dass eine E-Mail an einen Kunden/Partner nur dann verschickt werden darf, wenn auf Transportebene verschlüsselt werden kann, der annehmende SMTP-Server also die STARTTLS-Option unterstützt. Dies ist nur dann möglich, wenn XMS die E-Mail direkt versendet und die Zustellung nicht an ein internes Gateway weitergibt.

[2] Siehe dazu http://tools.ietf.org/html/rfc3207