

Totemo TrustDEX

Secure Managed File Transfer

Securing Your Data in Motion

INHALT

| | |
|---|----|
| _ Totemo TrustDEX | 3 |
| :: Software für den kontrollierten und sicheren Austausch von sensiblen Daten | 3 |
| :: Kundennutzen | 3 |
| :: Sicherheit | 3 |
| :: Optimale Compliance | 4 |
| :: Umfassendes Logging / Monitoring | 4 |
| :: Hochverfügbarkeit | 4 |
| :: Kontrolle | 4 |
| :: Automatismen / Workflows | 4 |
| :: Offene Architektur | 4 |
| :: Benachrichtigung | 4 |
| _ Datenaustausch treibt Geschäftsprozesse an | 5 |
| _ Unkontrollierter und schwer handhabbarer Datenaustausch | 6 |
| :: Beispiel Internet Protocol (IP) | 6 |
| :: Beispiel File Transfer Protocol (FTP) | 6 |
| _ Fazit: Hohe Anforderung an einen sicheren und kontrollierten Datenaustausch | 7 |
| _ Firmen operieren im unkontrollierten Umfeld | 8 |
| :: Zunehmender Datenaustausch | 8 |
| :: Vielfältige Anforderungen an eine Datenaustausch-Lösung | 8 |
| _ Totemo TrustDEX: eine „kontrollierte Umgebung“ mit offener, flexibler Architektur | 10 |
| Architektur | 10 |
| _ Funktionen und Module | 12 |
| :: Workflow | 12 |
| :: Modul Attachment Service | 13 |
| :: Modul Site-To-Site Synchronisation | 13 |
| :: Modul File Exchange Proxy | 14 |
| _ Nutzen für Unternehmen durch kontrollierte Datenaustausch-Umgebung | 15 |
| :: E-Mail-Integration | 15 |
| :: Compliance | 15 |
| :: Kommunikationsabläufe | 15 |
| :: Health Care, Industrie, Financial Services etc. | 15 |
| _ Einfache Implementierung und Konfiguration | 16 |
| _ Hoher Investitionsschutz mit Totemo Security Platform | 17 |
| :: Totemo AG | 18 |
| :: Haben Sie noch Fragen? | 18 |

TOTEMO TRUSTDEX – TRUSTED DATA EXCHANGE

SOFTWARE FÜR DEN KONTROLLIERTEN UND SICHEREN AUSTAUSCH VON SENSIBLEN DATEN

Die wichtigsten Merkmale auf einen Blick:

- Kontrollierte Umgebung für sichere Datentransfers mit integrierter Workflow Engine
- Plattformunabhängige Java-Lösung (z.B. für Windows, Sun Solaris, Linux)
- Appliance für einfachen und schnellen Anschluss ans Firmennetz
- Geeignet für alle Firmen

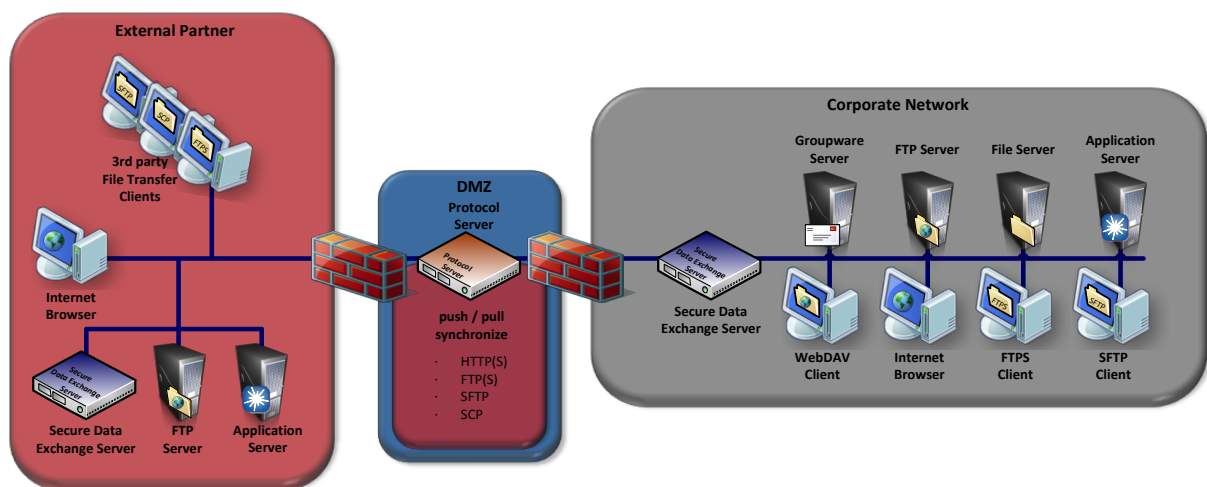


Abbildung 1 – Die Totemo TrustDEX Architektur in der Übersicht: zentrale Kontrollinstanz

KUNDENNUTZEN

SICHERHEIT

- Verschlüsselung für die Übertragungsprotokolle
- Verschlüsselung der Daten, die auf dem Gateway gespeichert sind
- Automatisierte Ver- und Entschlüsselung einzelner Dateien
- Unterstützung unterschiedlicher Authentication Mechanismen wie LDAP, Digitale Signaturen, Shared Secrets, SmartCards, RSA SecurID und Hardware Tokens
- Verwaltung von digitalen Zertifikaten und Schlüsseln sowie dazu gehörende automatisierte Austauschmechanismen
- Zentrale digitale Signaturen (z.B. PDF- oder .doc-Dateien)
- Durch «push» keine Zugriffe von der DMZ in das interne Netzwerk
- Schutz vor Viren und Trojanern durch Integration von 3rd Party Produkten
- Schutz vor Datenverlust durch Anbindung von Data Loss Prevention / Data Leakage Protection Lösungen

OPTIMALE COMPLIANCE

- Datenbewegungen über das Internet werden effektiv und nachvollziehbar an zentraler Stelle gesteuert, gesichert und umfassend protokolliert.
- Überwachung von Regulatorien und Compliance Richtlinien durch Anbindung von Security Information Event Management Lösungen (SIEM)
- Überwachung von Dateiinhalten mittels Content-Scanning (PCI, GLBA, SOX etc.)

UMFASSENDES LOGGING / MONITORING

- Protokollierung der Serveradministrations- und Benutzeraktivitäten für Überwachung und Auditing
- fortlaufende Aufzeichnungen über die Serverbenutzung (alle Aktionen und Ereignisse, die mit Speicherung und/oder Übertragung von Dateien zu tun haben)

HOCHVERFÜGBARKEIT

- Clustering und Load Balancing
- Redundanz und Failover

KONTROLLE

- Sichere Verwaltung des Dateizugriffs mit granularen Zugriffsrechten pro Ordner, Nutzer oder Nutzergruppe

AUTOMATISMEN / WORKFLOWS

- Integrierte Workflow Engine, mit der Abläufe automatisiert werden. Die ereignis- oder zeitgesteuerte Ausführung von Jobs integriert Anwendungen auf einfache Art und Weise in den Kommunikationsprozess.
- Transparente Nutzung für alle Beteiligten

OFFENE ARCHITEKTUR

- Unterstützung unterschiedlicher Schnittstellen, um verschiedene Plattformen und Drittprodukte anbinden zu können
- Unterstützung verschiedener Plattformen (Plattformunabhängigkeit)
- Unterstützung mehrerer Protokolle (FTP, FTPS, HTTP, HTTPS, SSH/SCP, SFTP)
- Übertragung grosser Datenmengen (mehrere GB)

BENACHRICHTIGUNG

- Alerts / Notifications per E-Mail oder SNMP

Totemo TrustDEX basiert ebenfalls auf der Totemo Security Platform (TSP) und harmoniert bestens mit dem Totemo TrustMail® Secure Messaging Gateway. Die Lösung ist als Software und Hardware Appliance verfügbar.

DATENAUSTAUSCH TREIBT GESCHÄFTSPROZESSE AN

Die geschäftliche Kommunikation zeigt sich enorm fragmentiert. Je einfacher Mitarbeitende und Partner zu erreichen sind, desto komplexer wird das technische Umfeld gestaltet, in dem Kommunikation stattfindet. Der gemeinsame Nenner der geschäftlichen Kommunikation ist das IP-Protokoll. Das ist aber auch schon alles; viele verschiedene Kommunikationswege eröffnen sich den Anwendern. Aber betrachten wir die Problematik etwas genauer:

Zwar sichert die IP-Kommunikation die Zustellung von Sprache, Video und anderen Daten automatisch und auf dem gerade möglichen und gewünschten Weg.

Eine wesentliche Frage rückt nun aber zunehmend in den Vordergrund: Wer garantiert Herkunft, Originalität, Vertraulichkeit und Integrität der Daten? Datenströme sind Datenströme: In klassischen IP-Architekturen fehlt eine Kontrollinstanz, die den sicheren Datenfluss gewährleistet. Anders ausgedrückt: Weil diese in der Netzwerkschicht nicht enthalten ist, muss sie auf Anwendungsebene realisiert werden. Dass dies bisher kaum gemacht wurde, hängt mit der Komplexität möglicher Lösungen zusammen. Nichtsdestotrotz steigt das Bedürfnis nach kontrollierten Datentransfers, denn diese sind in vielen Unternehmen und Branchen von geschäftskritischer Bedeutung.

Letztlich sind Daten ein wesentliches logistisches Gut und genauso zu behandeln wie die Lieferflüsse in der Industrie, die heute bis zum Ursprung der kleinsten Komponente dokumentiert sein müssen. Daten sind ein mindestens ebenso wertvolles Gut. Sie treiben Geschäftsprozesse an; sie sind das Blut in den Adern fast jedes Unternehmens. Wer den Datenfluss kontrolliert, schützt seine Geschäftsprozesse.

UNKONTROLLIERTER UND SCHWER HANDHABBARER DATENAUSTAUSCH

Jeder Transfer birgt das Risiko, dass sensible Daten in falsche Hände geraten, eine Übertragung fehlschlägt, Sicherheitsrichtlinien sowie rechtliche, organisatorische oder regulatorische Bestimmungen verletzt werden. Damit ist jede Beeinflussung oder Störung des Datentransfers eine potenzielle Gefahr für das Business. Das Problem äussert sich auf zwei Ebenen. Administratoren sehen sich mit einer Vielzahl von Datenflüssen verschiedenster Protokolle konfrontiert, die sich mit gängigen Mitteln und Methoden kaum kontrollieren lassen. Auf der technischen Ebene liegt ein wichtiger Grund in verschiedenen Unzulänglichkeiten der Datenaustausch-Protokolle.

BEISPIEL INTERNET PROTOCOL (IP)

Das IP-Protokoll kennt keine wirksamen Sicherheitsmechanismen, welche die Datenpakete fälschungssicher mit einem bestimmten Absender verbinden. Es garantiert bloss, dass die Pakete auch tatsächlich ankommen, gesendet von wem auch immer, auf welchem Weg auch immer. So ist denn auch das Internet grundsätzlich eine «offene» Architektur, in der Daten und Metainformationen beliebig mitgeschnitten oder gar manipuliert werden können. Der Empfänger ist so nie sicher, ob das, was er soeben erhalten hat, tatsächlich vom genannten Absender stammt. Umgekehrt erhalten Sender keine sichere Bestätigung über den Empfang der Daten und dass diese auch tatsächlich vom gewünschten Empfänger genutzt werden können. Kurz: Das IP-Protokoll ohne zusätzliche Massnahmen führt zu einem unzuverlässigen Dienst.

BEISPIEL FILE TRANSFER PROTOCOL (FTP)

FTP ist ein beliebtes Protokoll zum Austauschen von grossen Dateien. Es ist aber technisch veraltet und gilt als sehr unsicher. So werden etwa nicht einmal die Passwörter verschlüsselt übertragen. Seine Beliebtheit gründet in seiner Einfachheit: Ein FTP-Server ist rasch aufgesetzt und lässt sich mit praktisch jedem Browser aufsuchen. Doch er öffnet Sicherheitslücken und garantiert die Auslieferung einer Datei nicht. Die Daten liegen meist über einen längeren Zeitraum hinweg in einem Netzwerkbereich, der über das Internet zugänglich ist. Somit könnte die Konkurrenz problemlos auf die Informationen zugreifen – FTP öffnet Industriespionens Tür und Tor. Sicherheit muss mit Software von Drittherstellern hergestellt werden – was nebst höheren Kosten im Bereich von Lizenzierung und Wartung auch Sicherheitslücken schaffen kann. VPN als Alternative ist aufwändig, für die User zu umständlich und letztlich ein Leistungshemmer.

FAZIT: HOHE ANFORDERUNG AN EINEN SICHEREN UND KONTROLLIERTEN DATENAUSTAUSCH

Die Problempunkte beim Senden und Empfangen von Daten lassen sich wie folgt zusammenfassen:

- Fehlende Sende- und Empfangsbestätigung auf Seiten Empfänger und Sender
- Integrität der Daten wird nicht gewährleistet
- Fehlende Identifikation von Sender und Empfänger
- Nachverfolgbarkeit nur einseitig und lokal möglich – nicht im Netz selbst

Eine Lösung, mit der diese Hürden aus dem Weg geräumt werden, muss demnach folgende Eigenschaften aufweisen:

- Garantierte Zustellung der Daten
- Einfache und transparente Administration
- Einfache Integration in die bestehende Netzwerk- und Messaging-Infrastruktur
- Einfache Anwendungsintegration durch ereignis- und zeitbasierte Abläufe (Workflows)

Es leuchtet ein, dass die unzuverlässige und offene Art der Kommunikation im geschäftlichen Umfeld nicht der Weisheit letzter Schluss sein kann. Es muss eine kontrollierte Umgebung geschaffen werden, in welcher der Austausch von Daten sicher und nachvollziehbar stattfinden kann. Es geht darum sicherzustellen, dass die richtigen Daten des richtigen Senders zur gewünschten Zeit beim gewünschten Empfänger auch tatsächlich ankommen und dieser Vorgang transparent ist. Und dass sich jederzeit überprüfen lässt, ob ein Datentransfer erfolgreich war und ob richtig kommuniziert werden konnte. Darüber hinaus muss ein Kontrollinstrument geschaffen werden, das sicherstellt, dass vorhandene Sicherheits- und Compliance-Richtlinien eingehalten werden.

Verschiedene technische Lösungen und andere Protokolle sollen für mehr Sicherheit sorgen. In der Realität sind diese entweder nach wie vor sehr unzuverlässig oder dann so komplex, dass sie nur mit grossem Aufwand zu implementieren und zu nutzen sind. In den meisten Unternehmen stehen unsichere, unkontrollierte Datentransfers immer noch im Vordergrund. Oder es haben sich sichere, oft proprietäre Insellösungen etabliert, die wiederum das Problem aufwerfen, nur einen Bruchteil der Kommunikation zu sichern und nachvollziehbar zu halten. Und das Bemühen der Unternehmen um mehr Sicherheit und Kontrolle mittels eines teuren Projektes führt oft zu einer Lösung, die von den Mitarbeitenden nur schwer zu nutzen ist, ohne in Unproduktivität zu verfallen.

FIRMEN OPERIEREN IM UNKONTROLLIERTEN UMFELD

Die Globalisierung des Business macht vor keiner Firmengrösse Halt. Auch KMU müssen sich denselben Herausforderungen stellen wie grosse Unternehmen. Sie sind ebenso – wenn nicht sogar stärker – innovationsgetrieben, weisen aber eine höhere Fragilität ihres Business auf. Umso wichtiger ist der Schutz ihres Datenaustauschs, etwa um sich vor Industriespionage zu schützen. Gleichzeitig weichen die neuen konvergenten Kommunikationsformen die etablierten Firmenstrukturen auf. Die Wertschöpfungskette wird immer stärker fragmentiert, indem um die Kernprozesse herum das eigentliche Produkt erst in Zusammenarbeit mit Partnern entsteht. Ad-hoc-Teams bilden sich, die sich fallweise aus den Besten ihres Fachs zusammensetzen. Unabhängig von der Firma, bei der sie auf der Gehaltsliste stehen. Kommunikationsabläufe rollen entsprechend nicht länger innerhalb einer scharf definierten Firmengrenze ab, sondern erstrecken sich über mehrere Netze, Firmen und Zeitzonen. Dies birgt neue Angriffspunkte, da Menschen miteinander arbeiten, die sich unter Umständen gar nie persönlich begegnet sind. Datentransfers sind die Stütze einer solchen standort- und firmenübergreifenden kollaborativen Kommunikation.

Mit dem Schutz der Daten ist der Nachweis verbunden, wer welchen Datentransfer zu welcher Zeit durchgeführt hat. Dies einwandfrei zu belegen, garantiert die Integrität der Sendung und die Identität des Datenstroms. Dies verhindert übliche Attacks, bei denen sich der Angreifer mit einer gefälschten Identität der Daten bemächtigt.

Weiter nimmt die Regulierungsdichte für Unternehmen jeder Grösse massiv zu. Angesprochen sind etwa SOX, HIPAA, PCI, GLBA und lokale gesetzliche Bestimmungen, was die Aufbewahrungsfrist von E-Mails und ihren Anhängen angeht. Diese Aufgabe ist in einer unkontrollierten Umgebung kaum zu bewältigen und für die Mitarbeiter nicht mehr nachvollziehbar.

ZUNEHMENDER DATENAUSTAUSCH

Auf der Datenebene ist ein anderer Aspekt ebenso wichtig: Innerhalb des Unternehmens werden Daten über verschiedene Systeme hinweg ausgetauscht, zum Beispiel von einer CD auf die Festplatte, von einer Software in die andere, von einer Datenbank in ein Dateisystem oder Netzwerk etc. Dies erfolgt meist über unsichere Verbindungen, die keine Rückschlüsse zulassen, wer wann und was erfolgreich oder nicht erfolgreich übermittelt hat. Zudem steigt im Unternehmen der Aufwand massiv, «gute» von den «schlechten» Datentransfers zu unterscheiden. In einer kontrollierten Umgebung reduziert sich die Komplexität dieser Aufgabe. Ein weiteres Problem ist die massive Zunahme der per E-Mail verschickten Daten. Die Anhänge werden immer grösser oder aufgrund der Gefahr von Schädlingen blockiert. Schätzungen zufolge erhalten Mitarbeitende in Unternehmen bis 2011 täglich 30 MB an Daten auf dem langsamen, teilweise unsicheren Weg per E-Mail-Server.

VIelfÄLTIGE ANFORDERUNGEN AN EINE DATENAUSTAUSCH-LÖSUNG

Zusammenfassend müssen Unternehmen Datenflüsse in folgenden Situationen sichern, identifizieren und nachvollziehbar gestalten:

- Kommunikation mit externen Personen, Organisationen und Behörden
- Kommunikation zwischen Systemen innerhalb des Unternehmens
- Kommunikationsabläufe in Teams für kollaborative Zwecke
- Kommunikation in Business-Netzwerken
- Kommunikation in Geschäftsprozessen (system- und personenübergreifend)

In allen Situationen muss eine kontrollierte Umgebung folgende Fragen beantworten:

- Wie kann sichergestellt werden, dass die Daten auch tatsächlich gesendet/empfangen wurden?
- Wie kann eine solche Lösung schnell und einfach in die bestehende Infrastruktur eingebunden werden?
- Wie können Audits durchgeführt werden, die von Regulatorien wie SOX, HIPAA, PCI, GLBA und anderen gefordert werden?
- Wie kann man sicherstellen, dass die Daten an den Endpunkten der Übertragung geschützt sind?
- Wie kann der File- und Datentransfer zentralisiert und in bestehende Monitoringsysteme eingebunden werden?
- Wie können Datei-Anhänge in E-Mails mit den geringsten Störungen und Unterbrüchen überprüft werden?
- Wie wird beim Blockieren bestimmter Dateitypen aufgrund von Grösse oder Sicherheit sichergestellt, dass der Empfänger diese Daten trotzdem nutzen kann?
- Wie können B2B- und EDI-Transaktionen sicher und zuverlässig auf der Grundlage standardisierter Internetprotokolle durchgeführt werden?

TOTEMO TRUSTDEX: EINE „KONTROLLIERTE UMGEBUNG“ MIT OFFENER, FLEXIBLER ARCHITEKTUR

TrustDEX ist eine branchenneutrale Lösung, die mit einer Vielzahl von Schnittstellen ausgerüstet ist. Sie lässt sich schnell und einfach in die bestehende Infrastruktur integrieren. Sie setzt sich aus zwei Komponenten zusammen: dem Secure Data Exchange Server und dem Protocol Server. Beide lassen sich bei Bedarf auch auf einem physikalischen Host betreiben. Eine höhere Sicherheit bieten aber zwei physisch getrennte Maschinen.

Die technische Lösung ist das eine. Ein Secure File Transfer Gateway enthält bereits integrierte Sicherheitsfunktionen, welche durch den Einsatz komplementärer Technologien wie Data Loss Prevention (DLP) mittels Inhaltsanalyse (Block/Quarantine/Encrypt/Delete) erweitert werden können.

Manager müssen aber zuvor eine klare Vorstellung davon haben, welche Daten über welche Geschäftsprozesse ausgetauscht werden und welche Bestimmungen in puncto Vertraulichkeit und Datenschutz einzuhalten sind.

ARCHITEKTUR

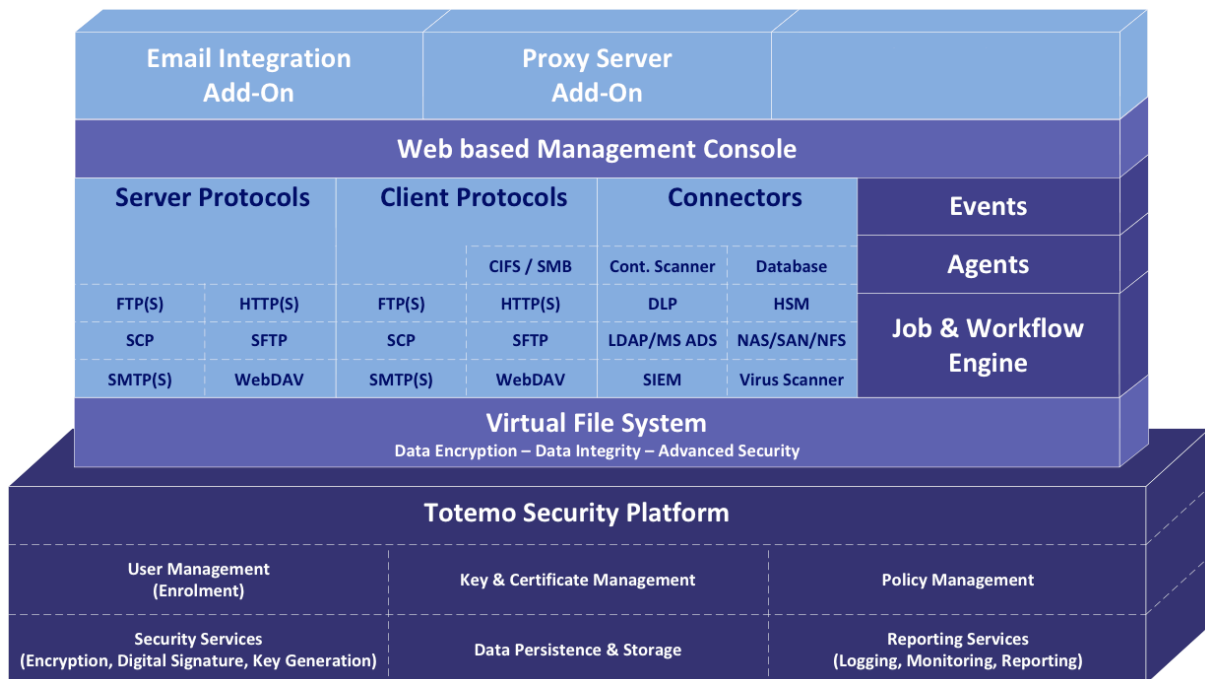


Abbildung 2 – Die Bestandteile der Totemo TrustDEX-Lösung auf einen Blick

Totemo TrustDEX besteht aus zwei Services. Der erste Service ist der Secure Data Exchange Server, der das komplette Management übernimmt. Dieses beinhaltet neben der Datenspeicherung auch die Userverwaltung, Verwaltung der Workflows, Reporting und Auditing Funktionalitäten. Des Weiteren bietet er alle Schnittstellen für die Speicherung von Daten im internen Netzwerk.

Der zweite Service ist der Protocol Server, der als Perimeter in der DMZ des Unternehmens installiert wird. Er erhöht die Sicherheit der gesamten Umgebung. Der Protocol Server ist für die Authentifizierung und Autorisation der externen Partner zuständig und sorgt dafür, dass diese die Daten auf dem gewünschten Weg bekommen. Er speichert selbst jedoch keine Daten, sondern bezieht diese vom Secure Data Exchange Server. Dieser arbeitet auch ohne Protocol Server.

Die Kommunikation zwischen dem Secure Data Exchange Server und dem Protocol Server erfolgt via Java Message Service (JMS). Dabei erfolgt kein Zugriff vom Protocol Server auf den Management Server. Der Management Server «pusht» die benötigten Daten auf den Protocol Proxy Server. Dieser verfügt nur für den Zeitraum der Übertragung über die Daten. Dieses Verhalten erhöht die Sicherheit der Gesamtlösung und ermöglicht eine einfache und schnelle Integration in die bestehende Netzwerkarchitektur, da keine Änderungen an der Firewall durchgeführt werden müssen.

TrustDEX unterstützt alle gängigen Datenaustausch-Protokolle und integriert somit eine Vielzahl unterschiedlicher Anwendungen.

- **WebDAV (Web-based Distributed Authoring and Versioning)** ist ein offener Standard zur Bereitstellung von Dateien im Internet. Dabei können Benutzer auf ihre Daten wie auf eine Online-Festplatte zugreifen.
- **HTTPS (HyperText Transfer Protocol Secure)** ist ein URI-Schema, das eine zusätzliche Schicht zwischen HTTP und TCP definiert. Es basiert auf der Transport Layer Security (TLS).
- **FTPS (Secure File Transfer Protocol)** ist ein Netzwerkprotokoll zur Übertragung von Dateien über TCP/IP-Netzwerke. Die Besonderheit hierbei ist, dass eine ansonsten ungesicherte File-Transfer-Protocol-Verbindung (FTP) über Transport Layer Security (TLS) abgesichert wird.
- **SFTP (SSH File Transfer Protocol)** ist eine Weiterentwicklung von SCP und erlaubt sichere Datenübertragung und Dateizugriffe auf entfernte Systeme.
- **SCP (Secure Copy)** ist ein Protokoll sowie ein Programm zur verschlüsselten Übertragung von Daten zwischen zwei Computern über ein Netzwerk.
- **SMTP (Simple Mail Transfer Protocol)** ist ein Protokoll der Internetprotokollfamilie, das zum Austausch von E-Mails in Computernetzen dient. Es wird dabei vorrangig zum Einspeisen und zum Weiterleiten von E-Mails verwendet. Dabei erfolgt idealerweise der Schutz der Daten über ein Secure Messaging Gateway wie z.B. Totemo TrustMail®.

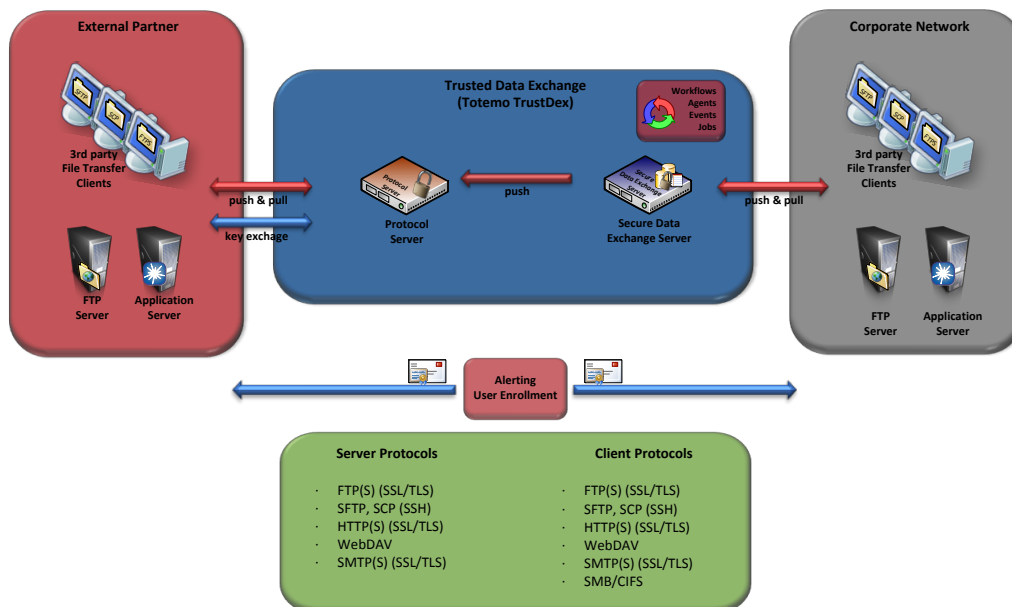


Abbildung 3 – Das Herzstück von Totemo TrustDEX: die Zusammenarbeit von Secure Data Exchange und Protocol Server

FUNKTIONEN UND MODULE

TrustDEX bildet eine kontrollierte Umgebung für den sicheren Datenaustausch über mehrere Personen, Netzwerke und Systeme hinweg, sogar über Unternehmensgrenzen hinaus. Im Zentrum steht eine Workflow-Engine, mit der IT-Administratoren auf einfache Art und Weise Berechtigungen für Datenflüsse erstellen können. Die Lösung verschlüsselt die Übertragungsprotokolle und prüft die Integrität der Daten. Sie unterstützt alle möglichen Arten von Authentifizierungsmechanismen (z.B. Smart Cards oder Hardware Tokens) und verwaltet digitale Zertifikate. Datenbewegungen über das Internet werden im Sinne der Compliance effektiv und nachvollziehbar gesteuert, gesichert und protokolliert. Hierzu bedient sich die Lösung mehrerer Verfahren. Sie zeichnet etwa fortlaufend alle Benutzeraktivitäten hinsichtlich von Dateitransfers auf. Sie bietet einen sicheren Zugriff auf die Daten mit fein definierbaren Zugriffsrechten. Mit einem Regelwerk lassen sich die Abläufe automatisieren. Die Architektur ist offen gestaltet, so dass jede Art von System leicht eingebunden werden kann. Dies betrifft etwa CRM- oder ERP-Systeme unterschiedlichster Hersteller.

Der Kundennutzen im Überblick:

- Flexible und sichere Kommunikation mit Partnern
- Sicheres «pushen» der relevanten Daten in die DMZ
- Einfache und sichere Integration in die bestehende Infrastruktur
- Verschlüsselung des virtuellen Dateisystems (Schutz vor unbefugten Zugriffen)
- Garantierte Datenverschlüsselung
- Einfache und flexible Integration in verschiedene Anwendungen
- Granulare Rechteverwaltung

WORKFLOW

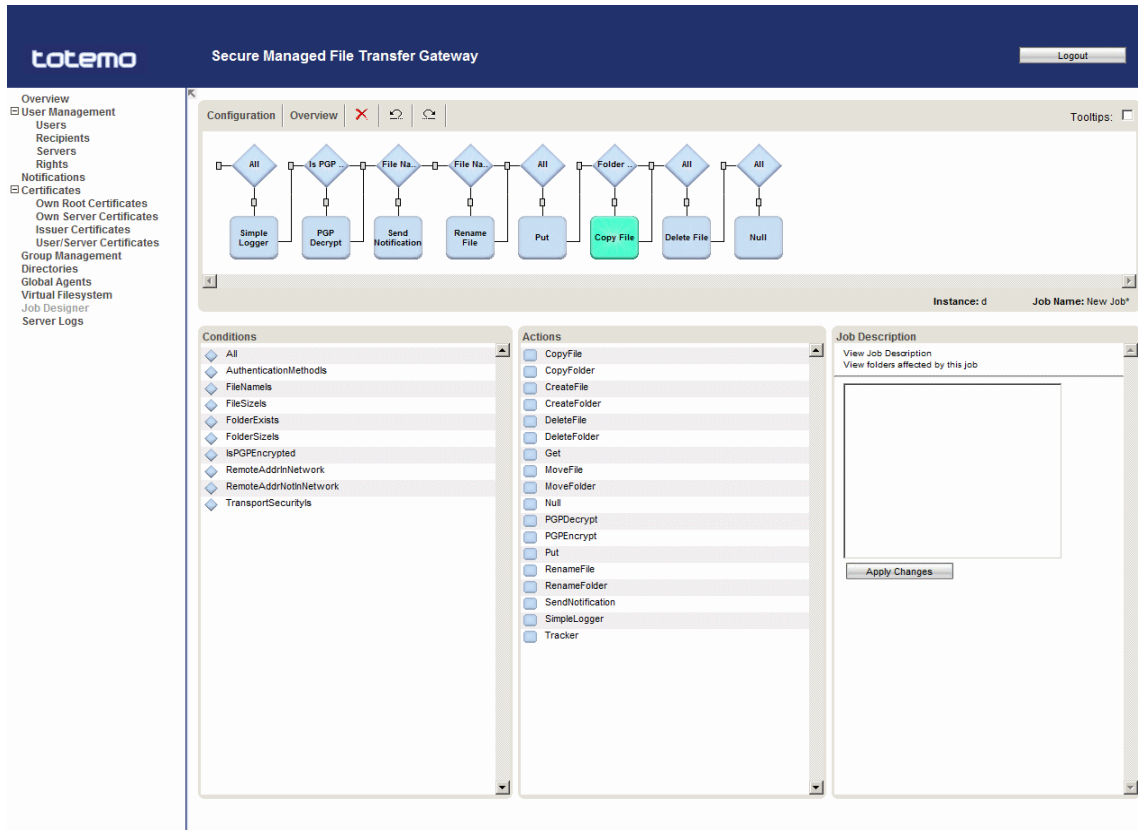


Abbildung 4 – Workflow-Oberfläche, die das konkrete Szenario unten zeigt

Die Workflow Engine von TrustDEX ermöglicht die gesicherte Datenübertragung im gesamten Unternehmen und den Einsatz in nahezu jedem Szenario. Das einfache Management über eine zentrale webbasierte Administrationskonsole und die enge Kopplung mit LDAP und Active Directory erlauben die effiziente Steuerung von Zugriffsrechten und Privilegien. Endbenutzer und IT-Admins behalten stets die volle Kontrolle über den Datenfluss. So kann etwa die Workflow Engine dazu verwendet werden, Daten nach Eintritt eines zuvor definierten Events zu verschlüsseln, sie zu verschieben und – falls eine bestimmte Grösse erreicht wurde – sie im Anschluss auf ein weiteres System zu übertragen. Dies kann etwa ein Windows Network Share oder ein FTP-Server sein. Durch den Alerting Mechanismus können Benutzer und Administrationen zu jeder Zeit über bestimmte Vorgänge informiert werden. Der Alarm kann etwa via SMS oder E-Mail erfolgen. Der grafische Workflow Designer erlaubt die Anpassung an die eigenen Bedürfnisse, ohne eine zusätzliche Programmiersprache zu erlernen oder Scripts zu definieren. Unternehmen können so neue Anwendungen rasch, ohne Kosten- und Programmieraufwand integrieren und in TrustDEX abbilden.

Wie einfach die Workflow Engine von TrustDEX arbeitet, lässt sich anhand des folgenden Szenarios (siehe Abbildung 4) feststellen, das in wenigen Minuten abgebildet wird:

Alle Benutzer, die zu einer definierten Active Directory Gruppe gehören, haben zusätzlich zu ihrem eigenen auch einen «Shared»-Bereich. Wenn nun ein Benutzer eine neue Datei mit Hilfe eines sicheren Protokolls wie SCP oder FTPS in den «Shared»-Bereich kopiert, wird diese – falls verschlüsselt – automatisch entschlüsselt. Falls die Datei ein Word-Dokument ist, wird via E-Mail eine Benachrichtigung an die Zugriffsberechtigten gesendet und das File anschliessend umbenannt. Danach wird die Datei über FTPS auf einen Drittserver und in ein anderes Verzeichnis kopiert. Eine Stunde nach Abschluss des Kopiervorgangs wird die Datei automatisch gelöscht.

MODUL ATTACHMENT SERVICE

Die Aufgabe des Attachment Service besteht in der Bereitstellung von sehr grossen E-Mail-Anhängen. Es ist oft entweder nicht möglich oder etwa bei mobiler Nutzung des Postfachs kaum sinnvoll, die Anhänge zu übertragen. Hier greift der Service ein. Er stellt sicher, dass Anhänge mit einer zuvor definierten Grösse herausgelöst und dem Empfänger auf einem alternativen Weg (z.B. Download-Link) angeboten werden. Dieses Modul ist ausserdem ideal für eine Koppelung mit Totemo TrustMail® geeignet.

MODUL SITE-TO-SITE SYNCHRONISATION

Viele Unternehmen müssen über mehrere Standorte hinweg kommunizieren – dies schliesst oft auch Niederlassungen im Ausland und in anderen Zeitzonen mit ein. Die Teams müssen trotzdem Informationen, Daten und Dateien austauschen. Diese in speziell für den Austausch bestimmten Ordnern liegenden Informationen können über das Synchronisationsmodul in einer sicheren Art und Weise mit anderen Gateways für Secure Managed File Transfer synchronisiert und verfügbar gemacht werden.

MODUL FILE EXCHANGE PROXY

Die Lösung kann auch als Proxy zwischen einem beliebigen internen Benutzer und einer Download-Seite im Internet fungieren. Dabei wird die Seite nicht gespiegelt. Der Vorteil ist eine zentrale Stelle, von der aus man sämtliche Datentransfers überwachen kann. Dies erlaubt:

- Datenflusskontrolle (Viren, Spam etc.)
- Zentrales Logging/Monitoring

Die oben aufgeführten Funktionen sind selbst für verschlüsselte Verbindungen möglich, da das jeweilige Transportprotokoll an zentraler Stelle aufgebrochen – und fall notwendig – in ein anderes Transportprotokoll transformiert wird.

NUTZEN FÜR UNTERNEHMEN DURCH KONTROLLIERTE DATENAUSTAUSCH-UMGEBUNG

TrustDEX löst verschiedene Probleme mit einem Schlag. Die Lösung sichert und protokolliert jede Art von Datentransfer über verschiedene Netze und Systeme hinweg.

E-MAIL-INTEGRATION

Ein Mitarbeitender sendet eine E-Mail-Nachricht an einen Geschäftspartner, die einen grossen Anhang enthält. Das System entscheidet nun – bevor das E-Mail das Firmennetz verlässt – aufgrund vordefinierter Regeln, wie mit dem Anhang zu verfahren ist und lagert ihn entsprechend aus. Der Empfänger erhält die Nachricht ohne den Anhang, erfährt aber gleichzeitig, auf welchem Wege er ihn beziehen kann, zum Beispiel mit einem bequemen Klick auf einen Download-Link.

In Kombination mit Totemo TrustMail® kann sichergestellt werden, dass die Zugangsdaten auf sehr komfortable Art und Weise (via E-Mail) verschlüsselt übertragen werden.

COMPLIANCE

Mit TrustDEX lassen sich die diversen Compliance-Vorschriften in Unternehmen leichter befolgen:

- Einhaltung von Datenschutzgesetzen und internen Richtlinien
- Rechtliche Vorschriften wie HIPAA, Basel II, SOX, PCI, GLBA etc.
- Vorschriften zum Schutz des geistigen Eigentums (Intellectual Property wie beispielsweise Patente, Source Code etc.)
- Vorschriften im Bereich Corporate Governance

KOMMUNIKATIONSABLÄUFE

Projekte geraten nicht länger ins Stocken, weil zum entscheidenden Zeitpunkt ein Teammitglied nicht in den Besitz eines wichtigen Dokumentes gelangt. Tritt beim Dateitransfer ein Fehler auf, erhält der Absender in jedem Fall eine Quittung.

HEALTH CARE, INDUSTRIE, FINANCIAL SERVICES, ETC.

E-Health ist ein weltweiter Trend, der nicht mehr aufzuhalten ist. Auch die Schweiz macht mit. Derzeit befindet sich die Vernetzung aller Akteure im Gesundheitswesen im vollen Gang. Zum sicheren Datenaustausch sind teure, proprietäre Lösungen überflüssig. Auch kleinere Arztpraxen können sich mit TrustDEX sicher vernetzen.

TrustDEX, die Lösung für den Aufbau einer kontrollierten Datentransfer-Umgebung, erfüllt in vielen anderen Bereichen die Bedürfnisse von Kommunikationspartnern. Einige Beispiele:

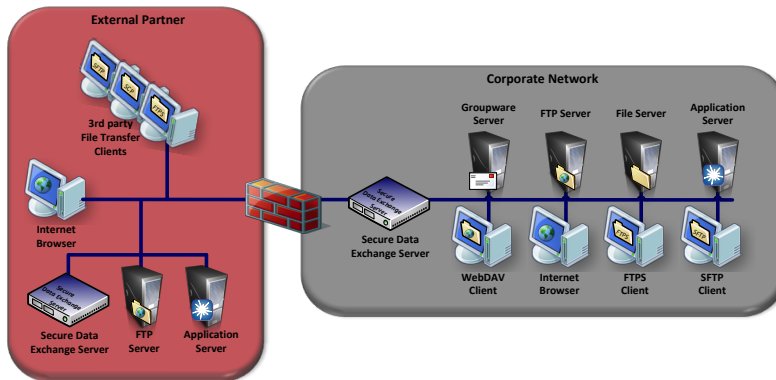
- Transaktionen bei Finanzdienstleistern
- Behörden: Austausch vertraulicher Daten zwischen Departements
- Industrie: Austausch von Bestell- & Rechnungsdaten zwischen Herstellern und Lieferanten
- Genehmigungsprozesse in der Pharmaindustrie (z.B. FDA)
- Austausch von Konstruktionsplänen und –informationen zwischen Herstellern und Lieferanten (z.B. Automobilindustrie)

EINFACHE IMPLEMENTIERUNG UND KONFIGURATION

Die Implementierung der Software ist eine Sache von wenigen Stunden. Die grafische Oberfläche der Workflow Engine lässt sich von IT-Administratoren ohne Programmierkenntnisse bedienen – der Einschulungsaufwand ist minimal. Ein eigentliches Projekt ist nicht notwendig. Die IT-Abteilung jedes Unternehmens kann die Software leicht selbst auf bestehender Server-Hardware installieren und in Betrieb nehmen. Alternativ steht eine Appliance zur Verfügung. Diese wird wie jedes andere Netzwerkgerät in Betrieb genommen. Anschliessend wird die Workflow-Engine eingerichtet.

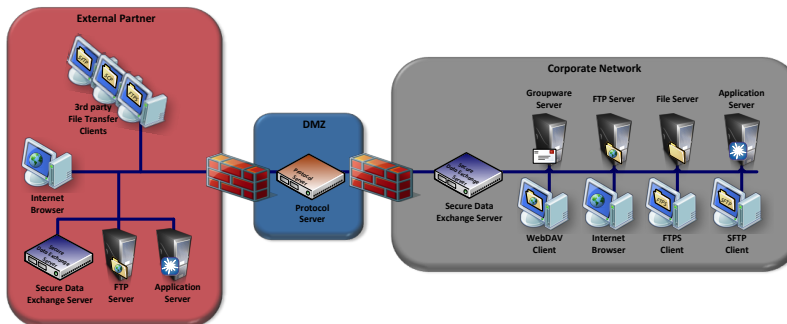
Totemo TrustDEX ist sehr flexibel und bietet verschiedene Deployment Optionen, um sich ideal an die unterschiedlichsten Bedürfnisse und Infrastrukturen anzupassen.

DEPLOYMENT OPTION 1 – FÜR KLEINE INSTALLATIONEN OHNE PROTOCOL SERVER



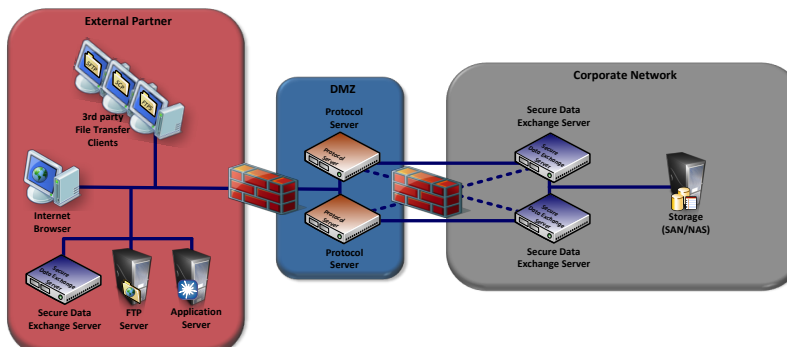
Deployment Option 1: Für kleinere Installationen ohne Protocol Server

DEPLOYMENT OPTION 2 – HOHE SICHERHEIT



Deployment Option 2: Mit Protocol Server für höhere Sicherheit, da keine Daten in der DMZ gespeichert werden

DEPLOYMENT OPTION 3 – HOCHVERFÜGBARKEIT



Deployment Option 3: High Availability Option

HOHER INVESTITIONSSCHUTZ MIT TOTEMO SECURITY PLATFORM

Die Totemo Security Platform ist eine dynamische, erweiterbare Sicherheitsarchitektur, welche auf interoperablen Standards basiert und alle « Data in Motion » (Daten in Bewegung) schützt. Sicherheitsmerkmale wie Verschlüsselung, Authentifizierung und Autorisierung, Zertifikats- und Schlüssel-Management, zentralisierte Verwaltung und mehr sind vollständig integriert und bereits mehrfach am Markt erprobt. Die Totemo Security Platform ist plattformunabhängig, hoch skalierbar, ganz einfach zu installieren und zu verwalten, transparent für den Endbenutzer und ausgerichtet auf zukünftige Entwicklungen.

Totemo TrustDEX ist ein Bestandteil der Totemo Security Platform. Die Lösung ergänzt auf ideale Weise Totemo TrustMail®, ein System zur regelbasierten Ver- und Entschlüsselung von E-Mails. Dieses arbeitet mit jeder gängigen E-Mail-Anwendung und jedem Mail-Server zusammen. Empfänger müssen keine Zusatzsoftware installieren, sondern arbeiten wie gewohnt mit ihrer E-Mail-Software.

Totemo TrustMail® stellt sicher, dass

- sämtliche E-Mails mittels S/MIME, PGP oder SSL sicher übermittelt werden (Secure Transmission).
- der jeweilige Absender identifiziert wird (Sender Identification).
- die Übermittlung bestätigt wird (Delivery Confirmation).
- die Nicht-Widerrufbarkeit der Nachricht gewährleistet ist (Non-repudiation).
- der Nachrichteninhalt unverändert bleibt (Content Integrity).
- Mehr über Totemo TrustMail® lesen Sie hier: www.totemo.ch/trustmail

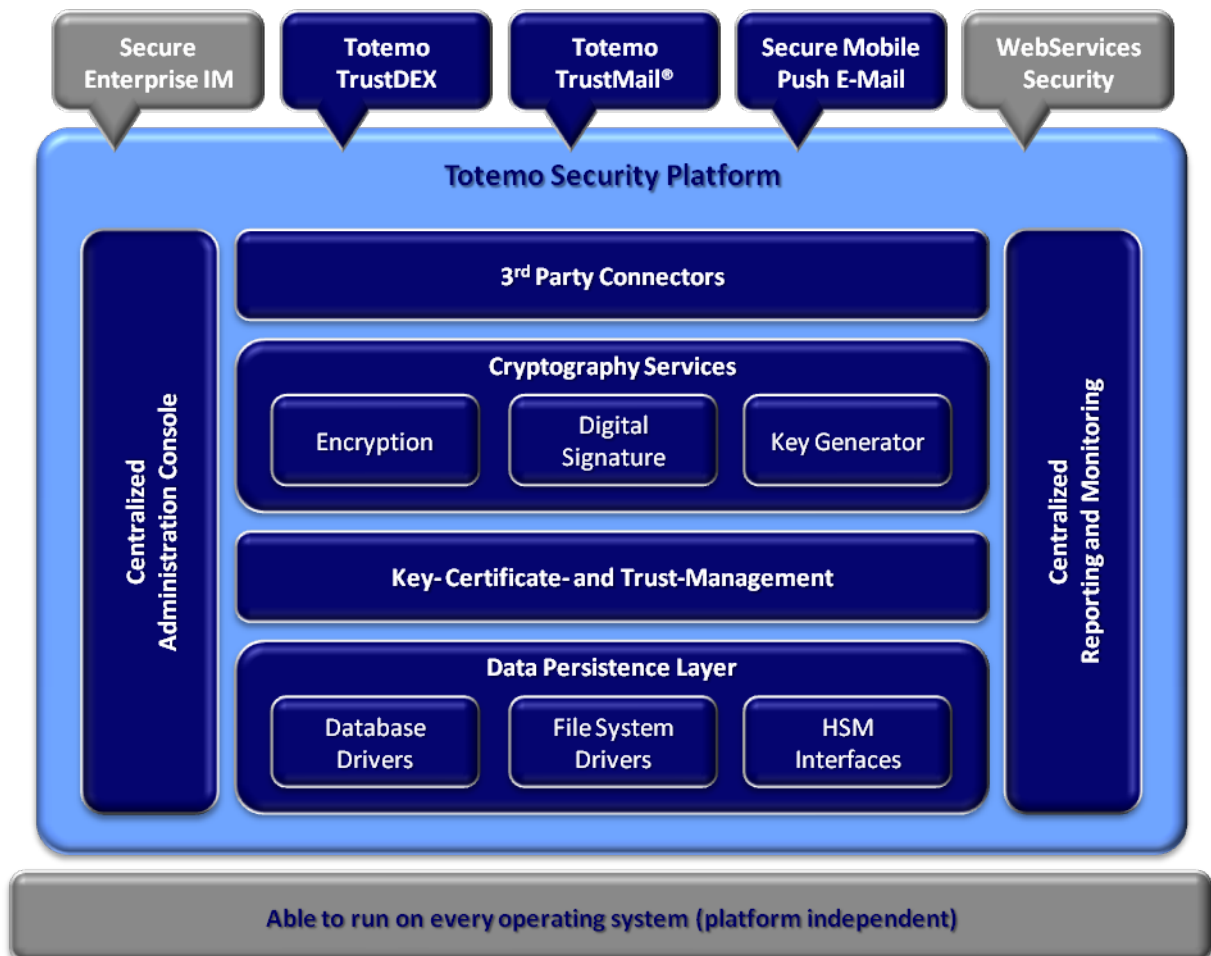


Abbildung 5 – Schutz über alle Systeme, Medien und Protokolle hinweg: Die Totemo Security Platform (TSP)

TOTEMO AG

Die Totemo AG ist ein Schweizer Softwareunternehmen, welches Secure Messaging, Secure Managed File Transfer und Secure Mobile Messaging Lösungen für Unternehmen und Behörden entwickelt und vertreibt, die sensible Daten sicher und über verschiedene Kanäle austauschen möchten. Mit dem ganzheitlichen Ansatz zur Sicherung der unternehmensweiten Online-Kommunikation bleibt sichergestellt, dass sämtliche E-Mails, File Transfers, Web-Interaktionen und Transaktionen jederzeit vertraulich, zuverlässig und effizient bleiben.

Totemo's zum Patent angemeldete Sicherheitsarchitektur trennt die Authentifizierung von der Verschlüsselung, ist interoperabel mit oder ohne Schlüssel sowie Zertifikate und ermöglicht den Anwendern die Beibehaltung der vollständigen Kontrolle über ihre Daten, auch nachdem diese versendet worden sind.

Zu den Kunden von Totemo zählen namhafte Organisationen und Unternehmen aus den Branchen Financial Services, Government, Managed Services und Outsourcing Provider, Versicherungen, Industrie, Technologie und Professional Services.

Das Unternehmen wurde im September 2001 gegründet und ist in Küsnacht (ZH) domiziliert.

HABEN SIE NOCH FRAGEN?

Zögern Sie nicht, uns zu kontaktieren:

Totemo AG
Freihofstrasse 22
CH-8700 Küsnacht

phone: +41 (0) 44 914 9900
fax: +41 (0) 44 914 9999
e-mail: info@totemo.ch
website: www.totemo.ch

© Totemo AG