

Inhalt

IntelliSecure: Sichere E-Mail Kommunikation durch Verschlüsselung.....	3
Enhanced Secure WebMail	3
Vollautomatische Domänen-Verschlüsselung zwischen allen IntelliSecure Anwendern sowie allen SEPPmail-Appliances	4
S/MIME User Verschlüsselung	4
OpenPGP User Verschlüsselung	4
TLS/SSL Transport-Verschlüsselung.....	4
Digitale E-Mail Signaturen	4
Digitale E-Mail Signatur mit Benutzerzertifikat.....	4
Digitale E-Mail Signatur mit Firmenzertifikat	5
Zentraler Firmen E-Mail Disclaimer.....	5
E-Mail Contentprüfung mit AntiVirus.....	5
Kompatibilität zu anderen Secure E-Mail Systemen	5
IntelliSecure Produktlinien	6
IntelliSecure Standard	6
IntelliSecure Professional	6
IntelliSecure Enterprise	6
Ergänzende Produktlinien	Fehler! Textmarke nicht definiert.
IntelliArchive.....	Fehler! Textmarke nicht definiert.
IntelliPrevent.....	Fehler! Textmarke nicht definiert.
Support.....	Fehler! Textmarke nicht definiert.
Verwendung von IntelliSecure	7
So versenden Sie ein sicheres E-Mail mit IntelliSecure:.....	7
E-Mailversand mit MS-Outlook:	7
E-Mailversand mit anderen E-Mail-Programmen:	7
Ergänzende Produktlinien	7
IntelliArchive.....	7
IntelliPrevent	7
Vertrieb.....	7



IntelliSecure: Sichere E-Mail Kommunikation durch Verschlüsselung

IntelliSecure setzt auf verschiedene standardisierte Verschlüsselungsverfahren und bietet dadurch höchste Sicherheit für unterschiedliche Kommunikationspartner. In diesem Abschnitt werden die Verfahren erläutert, die dabei zum Einsatz kommen.

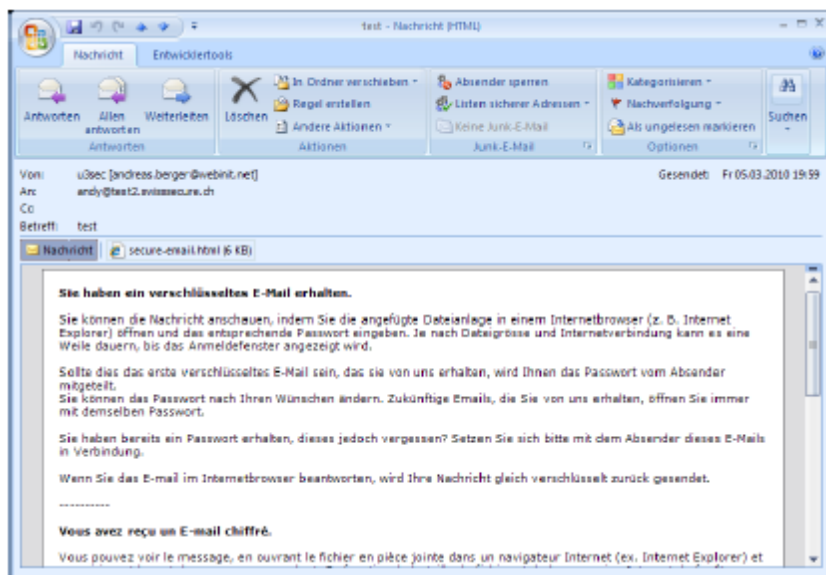
Das Secure-E-Mail-Gateway IntelliSecure entschlüsselt eingehende E-Mails automatisch. Der Vorgang ist für den E-Mail-Empfänger komplett transparent. Er erhält seine E-Mails unverschlüsselt in seiner Mailbox und liest diese wie bisher, ohne Zusatzaufwand.

Eingehende E-Mails können mit einer digitalen Signatur versehen sein. Bestandteil dieser Signatur ist das öffentliche S/MIME Zertifikat des Absenders. Um den Verwaltungsaufwand zu minimieren, speichert IntelliSecure diese S/MIME Zertifikate automatisch und nutzt sie zur S/MIME E-Mail-Verschlüsselung für die entsprechenden Kommunikationspartner.

Für den sicheren E-Mail Versand wählt IntelliSecure aus folgenden **5 Methoden** die für den Empfänger bestmögliche aus:

Enhanced Secure WebMail

Bei der Enhanced Secure WebMail Verschlüsselungstechnologie handelt es sich um ein patentiertes Verfahren der Schweizerische Post[®]. Dabei werden E-Mails nicht bis zur Abholung zwischengespeichert, wie es bei anderen Webmailverfahren üblich ist, sondern vollständig verschlüsselt an den Empfänger ausgeliefert. Dort werden sie in seiner Mailbox (z.B. im Outlook) gelagert. Mails sind bei diesem Verfahren vor Phishing-Attacken geschützt, denn neben dem Passwort ist für den erfolgreichen Zugriff auch die verschlüsselte E-Mail aus der Mailbox notwendig. Eine Enhanced Secure WebMail enthält die Nachricht in verschlüsselter Form als Anhang. Der Empfänger ruft die Nachricht ab, indem er die verschlüsselte Dateianlage öffnet. Diese wird dadurch über eine sichere SSL-Verbindung an IntelliSecure übertragen und dort nach Eingabe eines Passworts entschlüsselt und angezeigt. Durch die Passworteingabe wird die Identität des Empfängers bei jedem Abruf geprüft. Im Gegensatz zum herkömmlichen E-Mail-Versand können EMail-Zustellungen aufgrund der korrekten Authentifizierung nachgewiesen werden. Die nachfolgende Abbildung zeigt ein Beispiel einer Enhance Secure WebMail:



Vollautomatische Domänen-Verschlüsselung zwischen allen IntelliSecure Anwendern sowie allen SEPPmail-Appliances

IntelliSecure bietet Ihnen die Möglichkeit, den E-Mail-Verkehr permanent zwischen mehreren Domänen zu verschlüsseln. Einzige Bedingung dabei ist, dass die Kommunikationsstellen ebenfalls IntelliSecure einsetzen oder über eine SEPPmail-Appliance verfügen. Zwischen den Geräten werden alle Nachrichten automatisch ver- und entschlüsselt. Bei diesem Verfahren kommen sogenannte Domain-Keys zum Einsatz.

S/MIME User Verschlüsselung

Das Verfahren der Verschlüsselung mittels S/MIME basiert auf öffentlichen und privaten Schlüsseln. Mit öffentlichen Schlüsseln werden die E-Mails verschlüsselt und können anschließend nur mit den zugehörigen privaten Schlüsseln entschlüsselt werden. Dank der zentralen Verarbeitung läuft dieser Vorgang automatisch ab, wenn entsprechende S/MIME Benutzerzertifikate innerhalb IntelliSecure existieren. Diese können auf IntelliSecure selbst signiert oder durch einen öffentlichen Zertifikatsanbieter wie SwissSign ausgestellt werden. In beiden Fällen lassen sich die Zertifikate automatisch erstellen. IntelliSecure unterstützt zu diesem Zweck verschiedene Schnittstellen.

OpenPGP User Verschlüsselung

OpenPGP funktioniert nach dem gleichen Grundprinzip wie S/MIME. Auch die OpenPGP-Schlüssel werden von IntelliSecure verwaltet und E-Mails entsprechend automatisch verschlüsselt, wenn das Schlüsselmaterial vorhanden ist. Im Gegensatz zu S/MIME werden die Schlüssel immer selbst erzeugt und nicht von Zertifizierungsstellen ausgestellt.

TLS/SSL Transport-Verschlüsselung

TLS/SSL bietet eine zusätzliche Sicherheit und ergänzt die bisher beschriebenen Verschlüsselungsmethoden. Die Kommunikation zwischen IntelliSecure und anderen Mailservern wird per Standardkonfiguration immer über einen TLS/SSL gesicherten Kanal aufgebaut, sofern die Gegenstelle dies unterstützt. Ebenfalls kommt TLS/SSL bei der bereits beschriebenen Domänen-Verschlüsselung zur Anwendung.

Digitale E-Mail Signaturen

Beim Einsatz digitaler E-Mail Signaturen wird die verbindliche E-Mail-Kommunikation gewährleistet, indem die Authentizität einer Nachricht verifiziert werden kann. Es wird somit sichergestellt, dass eine Nachricht unverändert beim Empfänger eintrifft und der angezeigte Absender dem tatsächlichen Absender entspricht.

IntelliSecure kann E-Mails entweder mit Benutzer- oder mit Firmen-Zertifikaten signieren. Die beiden Verfahren werden im Folgenden kurz erläutert:

Digitale E-Mail Signatur mit Benutzerzertifikat

Die Signierung der E-Mails mit einem S/MIME Benutzerzertifikat erlaubt dem Empfänger die Authentizität des E-Mails mit seinem Mailclient zu prüfen. Damit wird sichergestellt, dass der Absender authentisch ist und das E-Mail während und nach dem Versand nicht verändert wurde. Bei dieser Methode wird für jede E-Mail Senderadresse ein entsprechendes S/MIME Zertifikat benötigt.

Wir empfehlen die Verwendung von Zertifikaten, die durch einen öffentliche Zertifikatsanbieter ausgestellt wurden. Sie können diesen Vorgang automatisieren, indem Sie dafür die IntelliSecure-Integration der offiziellen Zertifizierungsstelle SwissSign oder einer anderen Zertifizierungsstelle

verwenden. Die Verbindung von IntelliSecure zu den Zertifikats-Providern ermöglicht Ihnen eine vollautomatisierte Ausstellung der Zertifikate, ohne Betreuungsaufwand.

Alternativ können die E-Mails auch im E-Mailclient des jeweiligen Absenders signiert werden. IntelliSecure wird diese E-Mails dann nur noch verschlüsseln.

Viele S/MIME Zertifikate eignen sich sowohl zum Signieren als auch zum Verschlüsseln. Es kann deshalb sinnvoll sein, die Zertifikate zusätzlich auf IntelliSecure zu installieren. Dadurch können Mails mit den entsprechenden Zertifikaten automatisch entschlüsselt werden.

Digitale E-Mail Signatur mit Firmenzertifikat

Die Signierung von E-Mails mit einem S/MIME Firmenzertifikat erfüllt denselben Zweck wie die Signierung mit einem S/MIME Benutzerzertifikat. Bei dieser Variante wird jedoch nur ein Zertifikat benötigt.

Da S/MIME Zertifikate grundsätzlich nur für eine E-Mail Senderadresse gültig sind, erhalten alle ausgehenden Mails den gleichen (technischen) Absender. E-Mails erscheinen beim Empfänger mit der jeweils identischen E-Mail Adresse, aber korrektem Namen. Die automatische Erfassung von Kontakten und zugehörigen E-Mail Adressen funktioniert dadurch beim Empfänger nicht mehr wie erwartet. Ebenso sind an anderen Stellen Schwierigkeiten zu erwarten. So besteht z.B. die Gefahr, dass alle Ihre Firmen-E-Mails abgewiesen werden, wenn diese eine Absenderadresse beim Empfänger fälschlich als Spam-Absender eingestuft wird.

Zentraler Firmen E-Mail Disclaimer

Der Secure E-Mail Gateway Dienst IntelliSecure kann Ihre E-Mails mit einem Firmen E-Mail Disclaimer ergänzen. Es werden Disclaimer im Text- oder HTML-Format unterstützt.

Nutzen Sie den zentralen Firmendisclaimer, um einen einheitlichen Text oder die handelsrechtlich geforderten Angaben an alle E-Mails anzubringen.

E-Mail Contentprüfung mit AntiVirus

IntelliSecure AntiVirus ist als Option erhältlich und schützt Sie vor virenverseuchten E-Mails.

Die Antivirus Komponente aktualisiert stündlich ihre Virendefinitionen und führt automatisch Virenprüfungen Ihrer E-Mails durch.

Wollen Sie diese Funktion auf AntiSpam- und weitere AntiViren-Filterfunktionen ausweiten, steht Ihnen mit IntelliPrevent ein entsprechender Service der Ubiqum Technologies zur Verfügung.

Kompatibilität zu anderen Secure E-Mail Systemen

Aufgrund der zentralen Mailverarbeitung und Schlüsselmanagement lässt sich IntelliSecure transparent in Ihre E-Mail-Infrastruktur integrieren. Alle anerkannten und sicheren Standard-Verschlüsselungstechniken sind implementiert. Die Kompatibilität zu den gängigen Secure E-Mail Systemen ist damit sichergestellt und die Installation zusätzlicher Client-Software entfällt. Für Empfänger, die keine S/MIME- oder OpenPGP-Schlüssel besitzen, kann Enhanced Secure WebMail zur sicheren E-Mail-Übertragung genutzt werden.

IntelliSecure Produktlinien

IntelliSecure Standard

IntelliSecure Standard bezeichnet einen einzelnen Mailaccount.

Die Mail-Domäne dieses Einzelaccounts lautet *@intellisecure.de.

Die Landingpage, die der Empfänger bei Abruf einer Enhanced Secure WebMail erhält, lautet <https://getmail.intellisecure.de>.

Der Inhaber eines Standardaccounts kann seine E-Mails über den Webmailer (<https://webmail.intellisecure.de>) oder einen mit Pop3, SMTP, IMAP, angebundenen Mailclient schreiben und abrufen.

Bei Einsatz eines eigenen Mailservers muss dieser eingehende E-Mails via Pop3 abholen und für das entsprechende IntelliSecure E-Mail-Konto E-Mails über den IntelliSecure Smarthost versenden können.

IntelliSecure Professional

IntelliSecure Professional bezeichnet einen Firmenaccount, der beliebig viele Mailkonten beinhalten kann.

Die Mail-Domäne dieses Einzelaccounts entspricht der Maildomäne der bisherigen Maildomäne des Kunden *@kundendomaene.de.

Die Landingpage, die der Empfänger bei Abruf einer Enhanced Secure WebMail erhält, lautet <https://getmail.kundendomaene.de>.

Das Erscheinungsbild kann an den Endkunden angepasst werden. Es werden Userzertifikate und ein SSL-Zertifikat, ausgestellt auf die Domäne des Kunden, benötigt. Diese Zertifikate kann das Unternehmen wahlweise selbst stellen oder, als SwissSign-Zertifikate, über Ubique Technologies beziehen.

Das Unternehmen kann seine E-Mails wahlweise über den Webmailer (<https://webmail.intellisecure.de>), über mit Pop3, SMTP, IMAP, angebundene Mailclients oder einen angebundenen Mailserver schreiben und abrufen. Zusätzlich muss der MX-Eintrag der Maildomäne auf die IP-Adresse von IntelliSecure zeigen und bei Verwendung eines eigenen Mailservers muss dieser über eine feste IP-Verfügen.

IntelliSecure Enterprise

IntelliSecure Enterprise unterscheidet sich zu IntelliSecure Professional durch die Anbindung an die CA der SwissSign, wodurch Userzertifikate automatisiert ausgestellt und den einzelnen Mailkonten zugeordnet werden. Die Verwendung eigener Zertifikate ist dabei weiterhin möglich.

Der Einsatz eines eigenen Mailservers ist Voraussetzung. Dabei muss der MX-Eintrag der Maildomäne auf die IP-Adresse von IntelliSecure zeigen, der Mailservers des Unternehmens muss über eine feste IP-Adresse verfügen und ausgehende E-Mails über IntelliSecure als Smarthost versenden.

Verwendung von IntelliSecure

So versenden Sie ein sicheres E-Mail mit IntelliSecure:

E-Mailversand mit MS-Outlook:

Nachdem Sie Ihren Mailserver an IntelliSecure angebunden haben setzen Sie, vor dem Versand der Nachricht, unter „Kategorien“ die Vertraulichkeit der E-Mail auf „Vertraulich“.

Unser System versendet diese E-Mail automatisch verschlüsselt und sendet dem internen Absender das Kennwort für dieses E-Mail, welche dem Kommunikationspartner mitzuteilen ist (wir empfehlen hier eine SMS oder eine telefonische Mitteilung).

E-Mailversand mit anderen E-Mail-Programmen:

Setzen sie folgenden Begriff - inkl. der eckigen Klammern in den Betreff der E-Mail:

- [vertraulich]

Unser System versendet diese E-Mail automatisch verschlüsselt und sendet Ihnen das Kennwort für dieses E-Mail mit, welches Sie bitte Ihrem Kommunikationspartner mitteilen (wir empfehlen hier eine SMS oder eine telefonische Mitteilung).

Ergänzende Produktlinien

IntelliArchive

IntelliArchive ist die Online E-Mail-Archivierung von Ubique Technologies.

Weiterführende Informationen finden Sie unter <http://www.ubique-technologies.de/intelliarchive>

IntelliPrevent

IntelliPrevent ist die online AntiViren- und AntiSpam-Lösung von Ubique Technologies.

Weiterführende Informationen finden Sie unter <http://www.ubique-technologies.de/intelliprevent>

Vertrieb

Sollten Sie weitere Fragen zu IntelliSecure oder anderen Lösungen der Ubique Technologies haben, wenden Sie sich gerne an unseren Vertrieb:

Vertrieb Süd:

Carlos Pinilla– +49 (0)6093 – 369 999-93 - carlos.pinilla@ubique-technologies.de

Vertrieb Nord:

Clemens Sökefeld– +49 (0)6093 – 369 999-94 – clemens.soekefeld@ubique-technologies.de