BÖLLHOFF

E-Mail-Verschlüsselung

In der Böllhoff Gruppe

Informationen für unsere Geschäftspartner

BÖLLHOFF

Inhaltsverzeichnis

1 E-Mail-Verschlüsselung generell

Die Wahrung von Vertraulichkeit, Sicherheit und Integrität für Dokumente, die wir mit unseren Geschäftspartnern austauschen, ist uns sehr wichtig.

Aus diesem Grunde besteht für Sie die Möglichkeit, mit uns Daten auf verschlüsseltem Wege auszutauschen.

Dabei können folgende Verfahren genutzt werden:

1. Secure WebMail-Box
   (für Nutzer, die kein eigenes E-Mail-Verschlüsselungsverfahren einsetzen)
2. PGP
3. S/MIME

Böllhoff stellt zur sicheren Kommunikation ein Emailgateway zur Verfügung, welches mit S/MIME und PGP Schlüsselmaterial umgehen kann.

Sofern Sie nicht über ein PGP- oder S/MIME-Zertifikat verfügen, können Sie mit uns über eine SSL-geschützte Webmail-Box Dokumente sicher austauschen.

Sobald Ihnen ein Böllhoff-Mitarbeiter erstmalig eine verschlüsselte Nachricht sendet, wird Ihnen in diesem Fall eine E-Mail zur Einrichtung Ihrer Webmail-Box gesendet.

Die genaue Vorgehensweise finden Sie nachfolgend beschrieben.

1.1 S/MIME

S/MIME (Secure/Multipurpose Internet Mail Extensions) oder auch X.509 ist eine weitgehend akzeptierte Methode, genauer gesagt ein Protokoll, zum Senden digital signierter und verschlüsselter Nachrichten. S/MIME ermöglicht Ihnen das Verschlüsseln und digitale Signieren von E-Mails.

Wenn Sie S/MIME mit einer E-Mail verwenden, können die Empfänger sicher sein, dass sie genau die Nachricht im Postfach haben, die der Absender abgeschickt hat. Zudem können Empfänger von Nachrichten sicher sein, dass die Nachricht von dem spezifischen Absender stammt und nicht von jemanden, der vorgibt, der Absender zu sein. Dafür bietet S/MIME kryptografische Sicherheitsdienste, wie Authentifizierung, Nachrichtenintegrität und Ursprungszulassung (anhand von digitalen Signaturen). Es sorgt auch für mehr Datenschutz und -sicherheit (anhand von Verschlüsselung) für die elektronische Nachrichtenübermittlung.

(Quelle: Microsoft Technet Okt. 2015)

1.2 PGP

Pretty Good Privacy (PGP, deutsch sinngemäß „Ziemlich gute Privatsphäre“) ist ein von Phil Zimmermann entwickeltes Programm zur Verschlüsselung und zum Unterschreiben von Daten.

PGP benutzt ein sogenanntes Public-Key-Verfahren, in dem es ein eindeutig zugeordnetes Schlüsselpaar gibt:

Genutzt werden ein öffentlicher Schlüssel, mit dem jeder Daten für den Empfänger verschlüsseln und dessen Signaturen prüfen kann, und ein privater geheimer Schlüssel, den nur der Empfänger besitzt und der normalerweise durch ein Passwort geschützt ist. Nachrichten an einen Empfänger werden mit dessen öffentlichem Schlüssel verschlüsselt und können dann ausschließlich mittels seines privaten Schlüssels entschlüsselt werden. Diese Verfahren werden auch asymmetrische Verfahren genannt, da Sender und Empfänger zwei unterschiedliche Schlüssel verwenden.

(Quelle: Wikipedia Okt. 2015)

2 Korrespondenz mit Böllhoff

Der sichere Datenaustausch mit Kommunikationspartnern innerhalb der Böllhoff Unternehmensgruppe kann mittels den Verfahren S/MIME oder PGP erfolgen, alternativ via Secure WebMail-Box oder kennwortgeschütztem PDF-Dokument.

Die Richtlinien im Verschlüsselungssystem bei Böllhoff sehen die Nutzung von Verschlüsselung und Signatur vor.

Unter Verschlüsselung versteht man die Unkenntlichmachung eines Nachrichteninhaltes für dritte, nicht in die Kommunikation eingebundene Personen. Hierbei wird mittels der bereits beschriebenen Verfahren die Nachricht nur für die legitimen Empfänger lesbar gemacht.

Die digitale Signatur ist ähnlich wie ein mittelalterliches Siegel eine Bestätigung der Echtheit der zu übertragenden Nachricht. Durch die Kennzeichnung einer E-Mail mit dem privaten Schlüssel des Versenders, wird eine Art von Prüfsumme erstellt welche sich mit dem öffentlichen Schlüsselteil des Versenders auf Echtheit verifizieren lässt.

2.1 PGP

Der Austausch von PGP-Schlüsselmaterial erfolgt häufig auch direkt mittels E-Mail. Bei Böllhoff wird ein Emailgateway eingesetzt welches mit geringer Benutzerbelastung E-Mails verschlüsseln und entschlüsseln kann.

Emailgateway= Server welcher die E-Mails vom Mailserver entgegennimmt und anhand von spezifischen Regeln verschlüsselt und weitersendet

Falls Sie bereits einen PGP-Schlüssel besitzen, können sie den öffentlichen Teil dem Kommunikationspartner bei Böllhoff zur Verfügung stellen.

Öffentliche Schlüssel der Kommunikationspartner bei Böllhoff finden Sie auf den Schlüsselservern:

ldap://keys.boellhoff.com bzw. *ldaps://keys.boellhoff.com*

2.2 S/MIME

Der Austausch von S/MIME-Schlüsselmaterial erfolgt häufig auch direkt mittels E-Mail. Bei Böllhoff wird ein Emailgateway eingesetzt welches mit geringer Benutzerbelastung E-Mails verschlüsseln und entschlüsseln kann.

Emailgateway= Server welcher die E-Mails vom Mailserver entgegennimmt und anhand von spezifischen Regeln verschlüsselt und weitersendet

Falls Sie bereits einen S/MIME-Schlüssel besitzen, können sie den öffentlichen Teil dem Kommunikationspartner bei Böllhoff zur Verfügung stellen.

Das öffentliche S/MIME-Organisationszertifikat von Böllhoff finden Sie auf unseren Webseiten:

http://www.boellhoff.com/securemail/certificate

2.3 Webmailbox

Wenn Sie kein Verschlüsselungsverfahren wie PGP oder S/MIME einsetzen, ermöglichen wir Ihnen eine sichere Kommunikation mit uns über den Böllhoff Secure-WebMail-Server.

Bitte verwenden Sie diese Plattform, um vertrauliche Informationen mit Böllhoff auzutauschen. Die Dokumente in diesem Bereich werden für 60 Tage verfügbar gehalten, maximal stehen 200 MB Platz zur Verfügung.

Wenn auf unserem Security-System kein Schlüssel des Empfängers bekannt ist, kann ein Verfahren genutzt werden, bei dem die eigentliche E-Mail nicht direkt zum Empfänger gesendet wird sondern auf unserem Secure WebMail-Server verbleibt. Diese wird geschützt in einem sicheren Postfach abgelegt auf das nur der Empfänger mit einer eigens definierten Passphrase (Passwort) Zugriff bekommt.

Diese URL kann der Benutzer jederzeit aufrufen um auf seine Webmailbox zuzugreifen

http://www.boellhoff.com/securemail/webmail

Über die Webmailbox kann ebenso Schlüsselmaterial (S/MIME, PGP) von Ihnen bereitgestellt werden.

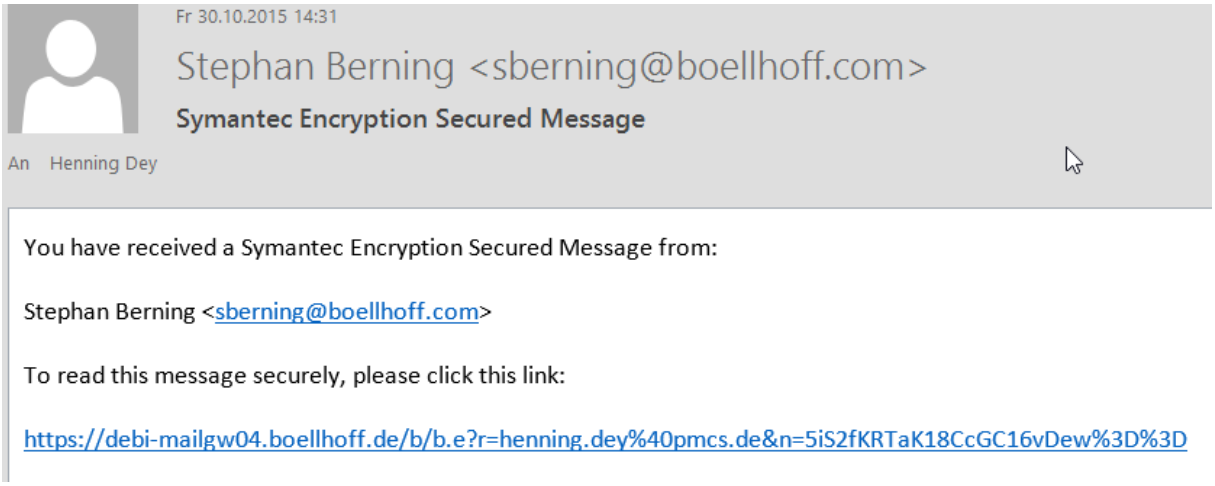
2.4 PDF-Verschlüsselung

Wenn auf unserem Security-System kein Schlüssel des Empfängers bekannt ist, kann ein Verfahren genutzt werden bei dem die eigentliche E-Mail in ein verschlüsseltes PDF gespeichert wird. Dieses wird mit einer zuvor durch den Empfänger definierten Passphrase (Passwort) gesichert. Das PDF wird anschließend direkt an den Empfänger gesendet und kann mit dessen Passphrase gelesen werden.

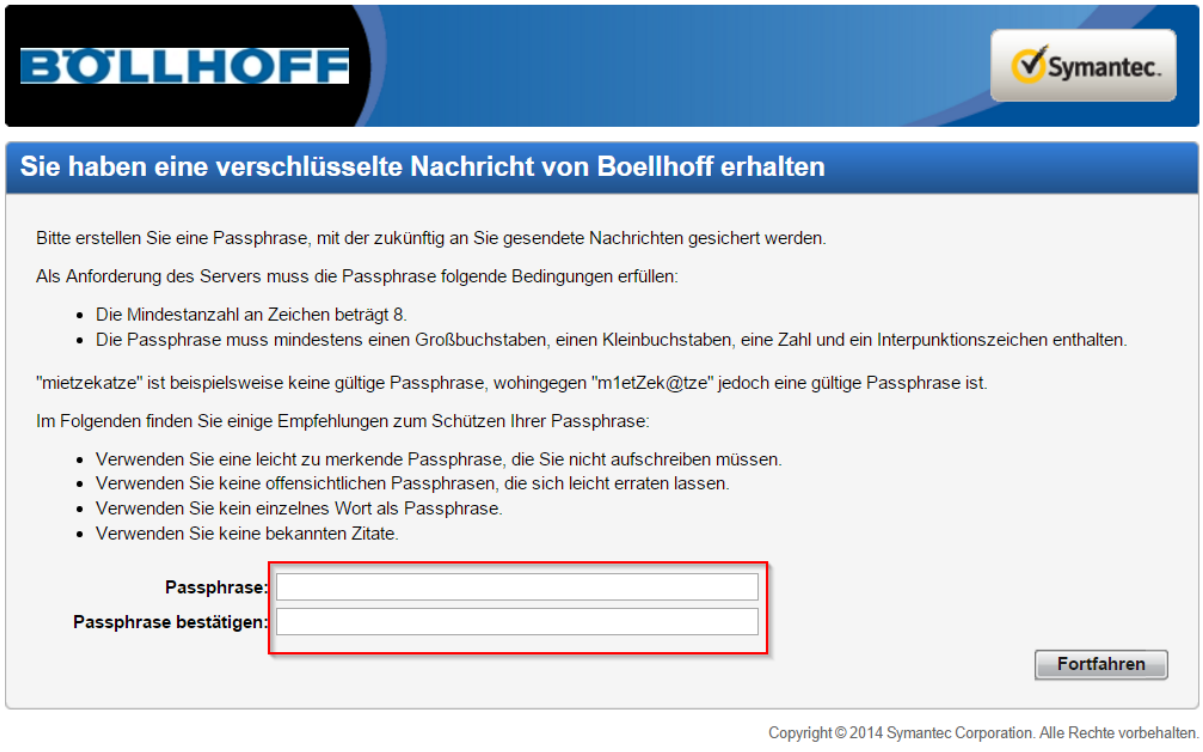
Die Verwendung von verschlüsselten PDF Dokumenten ist optional durch den Empfänger in der Webmailbox einstellbar.

3 Webmailbox Workflow

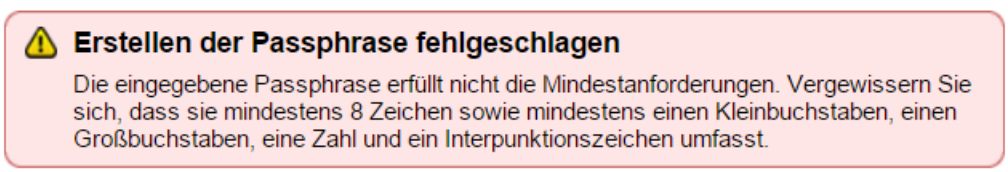
Wenn Sie mit einer verschlüsselten Nachricht angeschrieben werden, erhalten Sie eine E-Mail mit folgendem Inhalt:



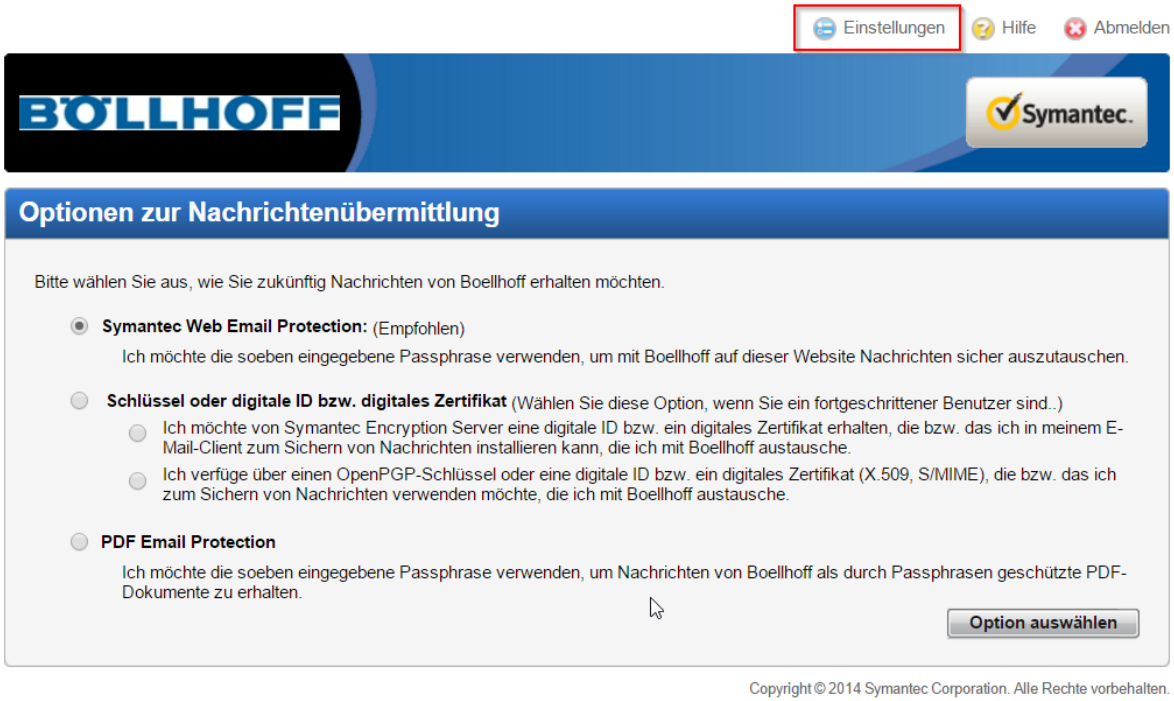
Wenn Sie die Website aus der E-Mail aufrufen muss eine Passphrase definiert werden:



Falls die Passphrase nicht den festgelegten Standards entspricht, wird eine Fehlermeldung ausgegeben:



Nach erfolgreichem Login an das Webportal wird eine Auswahlseite angezeigt. Hier können Sie die Einstellung für den künftigen E-Mailversand setzen.



Symantec Web Email Protection

Nutzung der Web-Mailbox mit Antwortfunktion und lokaler Speicherung der Nachrichten auf dem PGP-Mailgateway.

Schlüssel oder digitale ID bzw. digitales Zertifikat

Hier kann Schlüsselmaterial bereitgestellt werden. Dies kann sowohl ein S/MIME Zertifikat, als auch ein PGP-Schlüssel sein.

PDF Email Protection

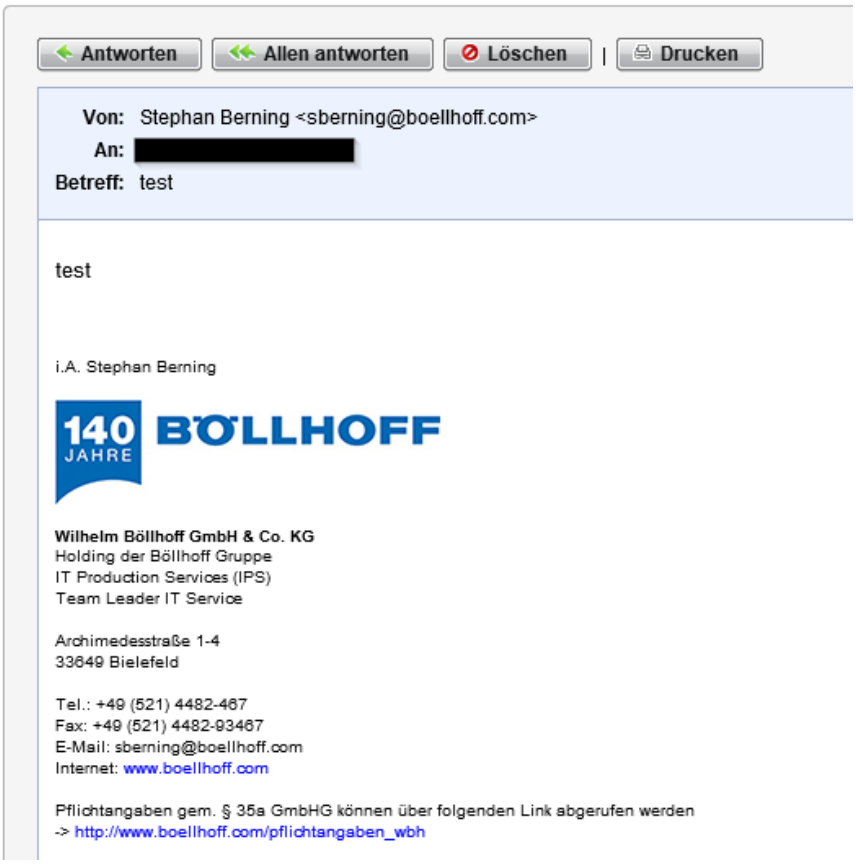
Mit dieser Einstellung werden verschlüsselte E-Mails versendet, welche mit der Passphrase der Webmailbox verschlüsselt werden.

Den Einstellungsdialog kann man über das Menü Einstellungen (im Bildschirmausschnitt rot markiert) auch nachträglich verändern.

Diese URL kann jederzeit aufrufen werden um auf die eigene Webmailbox zuzugreifen

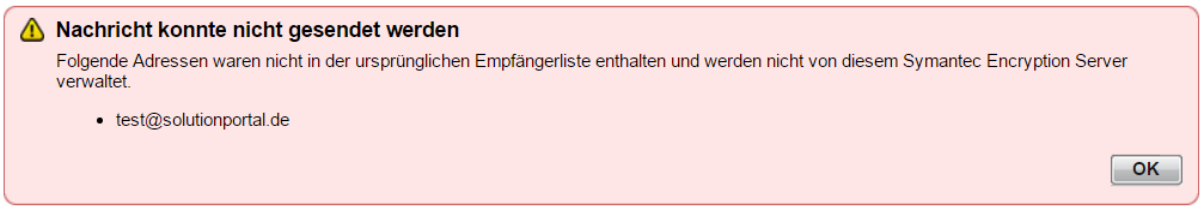
http://www.boellhoff.com/securemail/webmail

Die gesendete E-Mail ist jetzt über den Posteingang der Webmailbox einsehbar:



Hier können die üblichen Funktionen verwendet werden. Ebenso steht über die Schaltfläche „Verfassen“ die Möglichkeit zur Kommunikationsaufnahme mit Böllhoff Mitarbeitern zur Verfügung.

Hierbei ist zu beachten, dass nur interne Benutzer angeschrieben werden können. Die Warnung hierzu wie folgt:



4 Links zum Thema

Information für Geschäftspartner:	***http://www.boellhoff.com/de/securemail***
	http://www.boellhoff.com/en/securemail
Öffentlicher Teil S/MIME-Zertifikat Böllhoff:	***http://www.boellhoff.com/securemail/certificate***
Aufruf Secure WebMail-Box für Geschäftspartner:	***http://www.boellhoff.com/securemail/webmail***