E-MAIL-VERSCHLÜSSELUNG IN DS-WIN

Version: 1.1

Pionier der Zahnarzt-Software.
Seit 1986.

DAMPSOFT
Die Zahnarzt-Software

Inhaltsverzeichnis

1 Allgemeines zur E-Mail-Verschlüsselung

1.1 E-Mail Verschlüsselung innerhalb der Telematikinfrastruktur im Gesundheitswesen über den KIM-Client

Alle Teilnehmer im Gesundheitswesen sind an der Telematikinfrastruktur angeschlossen. Die E-Mailverschlüsselung wird in diesem Netzwerk über den KIM-Client gewährleistet. Ist dieser installiert und eingerichtet sind keine weiteren Konfigurationsschritte für einen verschlüsselten E-Mail-Versand notwendig. Zur Installation des KIM-Clients nutzen Sie auch gerne unsere Anleitungen unter www.dampsoft.de unter Service – Infos für Systembetreuer – 7. e-health- und KIM-Installation.

In der vorliegenden Anleitung geht es ausschließlich um die E-Mailverschlüsselung im allgemeinen öffentlichen E-Mailsystem und den Dampsoft E-Mail-Client, jedoch nicht um KIM-Mail der Telematikinfrastruktur.

1.2 E-Mail Verschlüssung außerhalb der Telematikinfrastruktur im Gesundheitswesen

Insbesondere nach der endgültigen Einführung der europäischen Datenschutzgrundverordnung (DSGVO) herrscht bei vielen Anwendern eine große Unsicherheit im Zusammenhang mit diesem Thema. Mit diesem Dokument möchte Dampsoft Ihnen einen Überblick über den Themenbereich der E-Mail-Verschlüsselung geben, um Sie so bei der Umsetzung Ihrer individuellen Datenschutzlösung zu unterstützen. Die fachgerechte Verschlüsselung von E-Mails, die vertrauliche Patientendaten enthalten können, ist dabei nur ein kleiner Baustein.

Falls Sie nicht über ein umfassendes Konzept zum Datenschutz in Ihrer Praxis verfügen, wenden Sie sich bitte an Ihren Systemadministrator, Ihren Datenschutzbeauftragten oder ggf. Ihren Rechtsbeistand um die nächsten Schritte auf dem Weg zu einer DSGVO-konformen Praxis abzuklären. Obwohl Dampsoft aufgrund der Vielfalt verschiedener Programme und Schnittstellen dabei nur sehr eingeschränkt helfen kann, hoffen wir, mit diesem Dokument einen Beitrag dazu leisten zu können.

Bei der Verschlüsselung von E-Mails werden oft zwei verschiedene Möglichkeiten miteinander verwechselt: Die Transportwegeverschlüsselung und die Verschlüsselung des Inhalts der einzelnen E-Mail. Der Vollständigkeit halber gehen wir im Folgenden auf beide Arten ein.

Dieses Dokument richtet sich an technisch versierte Anwender und Systemadministratoren. Wir bitten um Ihr Verständnis dafür, dass der Dampsoft-Support weitergehenden Fragen zur Verschlüsselung, die über den Inhalt dieses Dokuments hinausgehen, nicht bearbeiten kann. Falls Sie Fragen zu den einzelnen Unterpunkten haben, wenden Sie sich bitte an den Systemadministrator Ihrer Praxis oder an ein Systemhaus, das Dienstleistungen zur E-Mail-Verschlüsselung anbietet.

2 Transportwegeverschlüsselung

Bereits seit einigen Jahren ist die Verschlüsselung des Transportweges allgemeiner Standard. Nur noch wenige Anbieter lassen Zugriffe über unverschlüsselte Verbindungen zu. Die verbreitetsten Lösungen sind hier SMTP über SSL (SMTPS) und STARTTLS.

Wie der Name bereits sagt, wird hierbei nur der Übertragungsweg verschlüsselt. Die E-Mail selbst wird innerhalb dieses „Tunnels“ in Klartext übermittelt. Wenn eine E-Mail versehentlich an einen falschen Empfänger verschickt wird, kann dieser den Inhalt völlig frei einsehen. Gleiches gilt, wenn unberechtigte Dritte Zugriff auf eins der beteiligten E-Mailkonten oder auf die Mailserver der Anbieter erlangen.

Die Transportwegeverschlüsselung sollte trotz dieser Einschränkung immer verwendet werden, da sie einen einfach einzusetzenden Basisschutz darstellt.

2.1 Technische Umsetzung

Die Transportwegeverschlüsselung schützt ausschließlich die Übertragung von Ihrem E-Mail-Client (z.B. DS-Win, Outlook oder Thunderbird) bis zu Ihrem E-Mail-Anbieter.

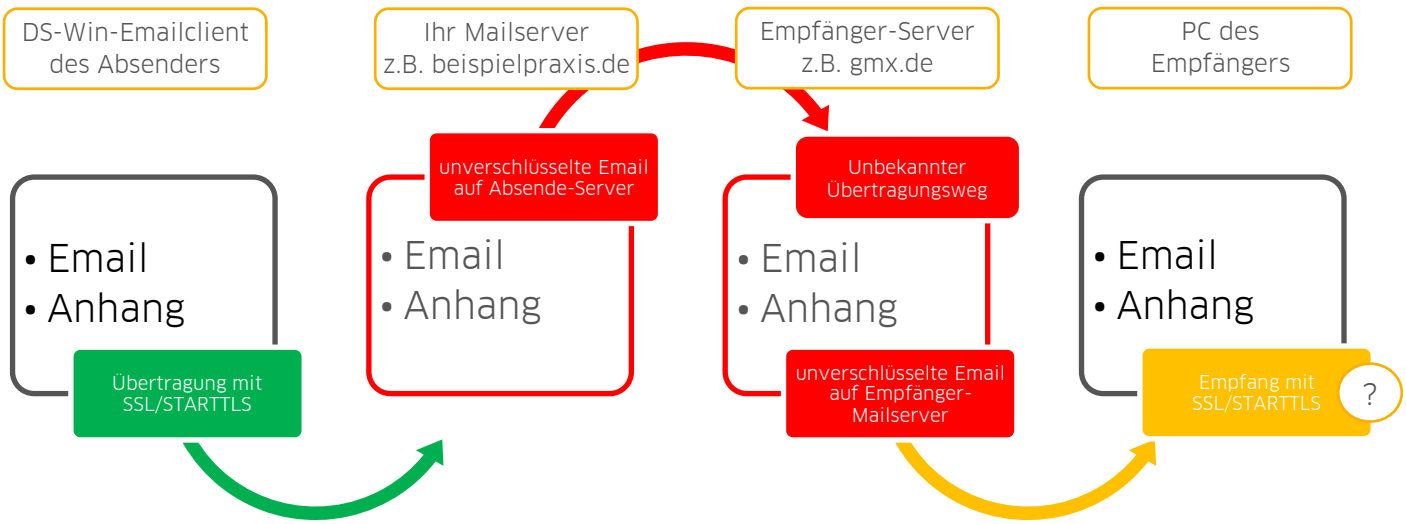

Abbildung 1

Nachdem die Übertragung von Ihrem E-Mail-Client zu Ihrem E-Mail-Provider (hier beispielpraxis.de) verschlüsselt erfolgt, ist der Inhalt im weiteren Verlauf der Übertragung theoretisch ungeschützt.

Der gesamte mittlere Bereich (rot hervorgehoben) spielt sich zwischen den E-Mail-Providern ab. Insbesondere die Übertragungstechnik zwischen den Mailservern ist den Benutzern völlig unbekannt. Man darf zwar davon ausgehen, dass die E-Mail-Anbieter sich um starke Schutzmechanismen bemühen, aber spätestens seit den Enthüllungen um Edward Snowden muss jedem Internetnutzer bewusst sein, dass diese Bemühungen erfolgreich umgangen werden (siehe Abschnitt Sicherheitshinweise).

Da auf der Seite des Empfängers unklar ist, ob dort ebenfalls eine Transportwegeverschlüsselung zum Einsatz kommt, muss davon ausgegangen werden, dass auch dieser Teil der Übertragung nicht vertrauenswürdig ist.

2.2 Transportwegeverschlüsselung in DS-Win aktivieren

Sobald in DS-Win die Zugangsdaten zu Ihrem E-Mailserver mit den entsprechenden Optionen (SSL oder STARTTLS) und den ggf. abweichenden Ports eingestellt sind, ist die Transportwegeverschlüsselung automatisch aktiviert. Beim Versand der E-Mails sind keine weiteren Schritte mehr notwendig.

Weitere Informationen zu den Einstellungen für Ihren E-Mail-Provider, erhalten Sie von Ihrem System-administrator oder Ihrem E-Mail-Anbieter.

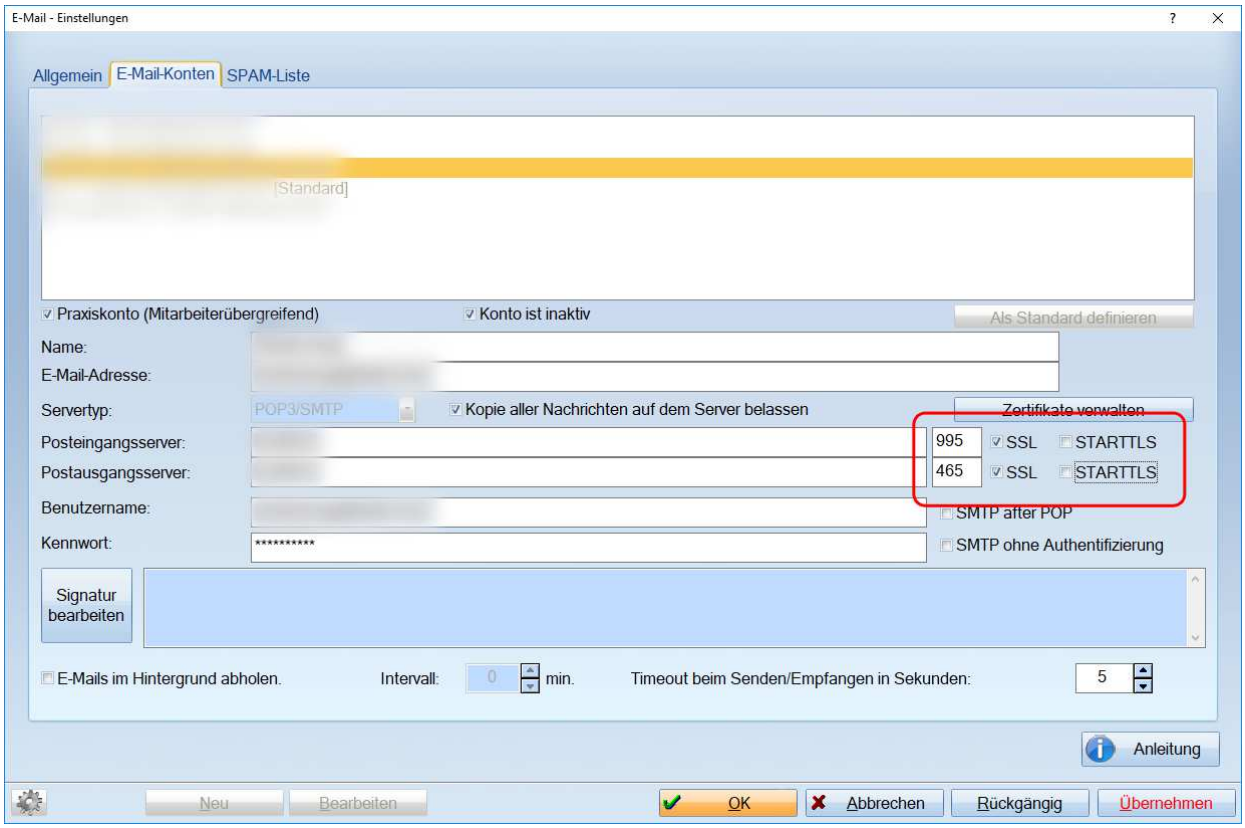

Abbildung 2

3 Inhaltsverschlüsselung (Ende-zu-Ende)

Bei der Verschlüsselung der E-Mail wird der komplette Inhalt der E-Mail, also Text und Anhang, verschlüsselt. Lesbar bleiben nur die sogenannten Meta-Daten: Sender, Empfänger, Betreff und der Versandzeitpunkt. Hier bietet die o.g. Transportwegeverschlüsselung noch weiteren Schutz. Die vom Absender verschlüsselten Daten kann nur der Empfänger selbst wieder in lesbare Daten umwandeln. Es gibt hierbei zwei international eingesetzte Varianten: S/MIME und PGP. Prinzipiell funktionieren beide nach dem gleichen Prinzip. Im DS-Win wird nur die Verschlüsselung über S/MIME unterstützt.

3.1 Technische Umsetzung der Ende-zu-Ende-Verschlüsselung

Zur Verschlüsselung werden zwei Zertifikate, auch „Schlüssel“ oder „Schlüsselpaar“ genannt, benötigt. Dabei handelt es sich um Dateien, die im Betriebssystem oder E-Mail-Client in den sog. Zertifikatspeicher installiert werden. Sie werden von verschiedenen Zertifizierungsstellen im Internet angeboten (teils kostenlos*) oder können auch selbst erzeugt werden. Ihr Systemadministrator wird Sie dazu eingehend beraten können. Der Aufwand für selbsterstellte Zertifikate ist bei fachgerechter, sicherer Ausführung sehr groß und unwirtschaftlich, weshalb wir diese Lösung für Produktivsysteme nicht empfehlen und im Folgenden nicht darauf eingehen werden.

** bitte beachten Sie die jeweiligen Lizenz- und Vertragsbedingungen der Anbieter und die u.U. kurzen Laufzeiten der Zertifikate*

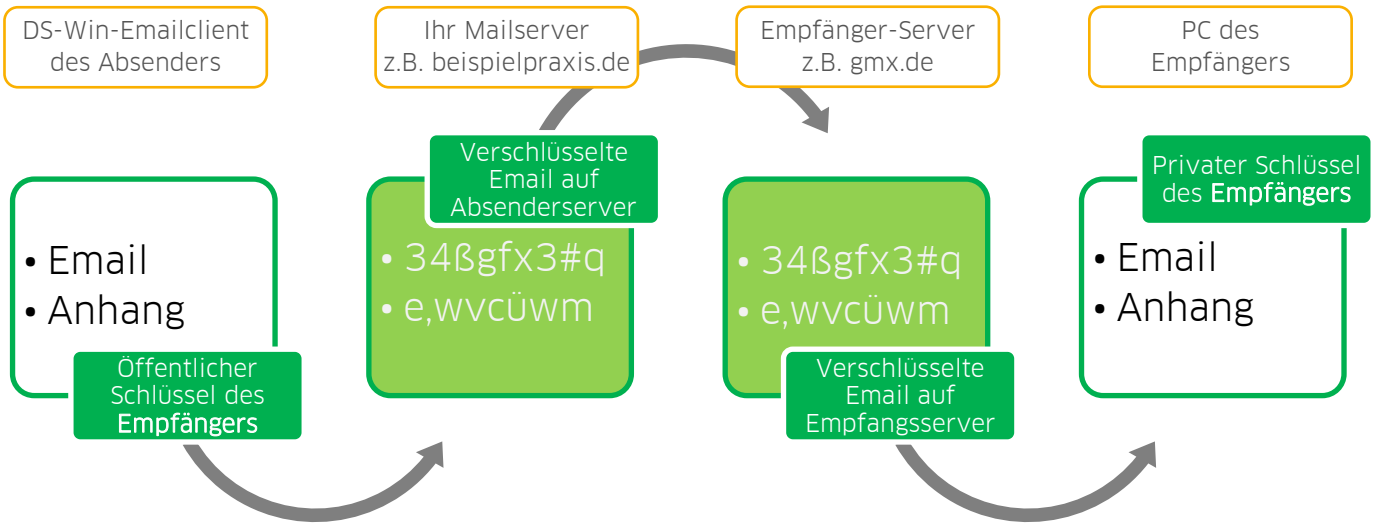

Abbildung 3

Im Schaubild sind die Übertragungswege grau markiert. Sie spielen für die bereits verschlüsselten E-Mails keine Rolle mehr. Trotzdem sollte die Transportwegeverschlüsselung natürlich auch hier benutzt werden. Die konkreten E-Mailinhalte sind im Internet zu keiner Zeit einsehbar. Sie werden direkt beim Absenden – vor der Übertragung auf den Mailserver – verschlüsselt und später erst durch die Anwendung des privaten Schlüssels wieder lesbar. Nur wer den privaten Schlüssel besitzt, kann die E-Mails lesen.

Bitte beachten Sie: Dampsoft bietet keine Zertifikate an. Bei Fragen zu Erstellung, Einrichtung und Benutzung von Zertifikaten wenden Sie sich bitte an Ihren Systembetreuer bzw. -administrator oder ein Systemhaus, das diese Dienstleistung anbietet.

3.2 Die Zertifikate

Es wird grundsätzlich zwischen vier verschiedenen Arten von Zertifikaten unterschieden:

3.2.1 Root-CA (Stammzertifizierungsstelle)

Diese Zertifikate werden in der Regel vom Betriebssystem oder dem Browseranbieter mitgeliefert und durch Updates aktuell gehalten. Die Stammzertifizierungsstelle bildet in der Zertifizierungskette das oberste Glied. Alle anderen Zertifikate beziehen sich (teils indirekt) auf sie.

Teil der Root-CA ist auch die sogenannte Revoke-Liste. Sie gibt an, welche ihrer abgeleiteten Zertifikate ungültig und daher nicht mehr vertrauenswürdig sind. Ohne diese Revoke-Liste ist eine Stammzertifizierungsstelle grundsätzlich nicht vertrauenswürdig, da veraltete Zertifikate einen Unsicherheitsfaktor darstellen. Die Revoke-Liste muss öffentlich über das Internet erreichbar sein, damit sie bei jedem Vorgang direkt abgefragt werden kann.

3.2.2 Zwischenzertifizierungsstellen

Sie werden vom Anbieter der Root-CA mit ausgeliefert und vom Betriebssystem oder Browser bei Bedarf selbsttätig heruntergeladen. Falls das nicht möglich ist, müssen sie manuell auf jedem beteiligten PC nachinstalliert werden.

3.2.3 Öffentliches Clientzertifikat

Das öffentliche Zertifikat wird, wie auch das anschließend erläuterte Private Zertifikat, aus der Stamm- oder Zwischenzertifizierungsstelle abgeleitet. Ohne die übergeordnete Instanz sind beide nicht vertrauenswürdig.

Mit dem öffentlichen Zertifikat eines Empfängers wird es dem Absender einer E-Mail ermöglicht, ihm verschlüsselte E-Mails zu senden sowie die Echtheit einer digital signierten E-Mail zu prüfen. Bevor eine verschlüsselte Übertragung von E-Mails möglich ist, müssen beide Partner ihre öffentlichen Schlüssel miteinander ausgetauscht haben.

3.2.4 Privates Clientzertifikat

Das private Clientzertifikat ist der geheime Schlüssel, mit dem die Verschlüsselung aufgelöst werden kann. Es muss stets sicher unter Verschluss gehalten werden. Wenn es auf einem PC in der Praxis installiert wird, darf es dort nicht exportierbar sein, da unberechtigte Benutzer es anderenfalls entwenden könnten. Die Verschlüsselung wird in diesem Fall sofort wertlos und die Zertifikate müssen von Ihnen beim Anbieter gesperrt und durch neue ersetzt werden (siehe o.g. Revoke-Liste).

Clientzertifikate sind immer nur für eine spezifische E-Mailadresse gültig. Es gibt es keine sog. Wildcards, die für eine ganze Domain – z.B. @dampsoft.de oder @<Ihre-Praxis>.de – gültig sind.

Bitte beachten Sie: Dampsoft-Mitarbeiter werden Sie niemals um die Herausgabe des privaten Zertifikats bitten. Es ist nicht Teil der DS-Win-Datensicherung, da es Bestandteil der Windows-Umgebung der Arbeitsstation ist. Bitte bewahren Sie es an einem sicheren Ort auf!

3.3 Ende-zu-Ende-Verschlüsselung in DS-Win aktivieren

DS-Win verwendet völlig automatisch und ohne weitere Konfiguration den zentralen Windows-Zertifikatspeicher. Je nach Einrichtung Ihres Netzwerks können die Zertifikate zentral über den Server oder über jeden einzelnen Client verwaltet werden. Für Details zur Einrichtung und Installation von Clientzertifikaten wenden Sie sich bitte an Ihren Systemadministrator. Hierbei darf und wird der Dampsoft-Support nicht helfen, da es sich um tiefgreifend sicherheitsrelevante Eingriffe in Ihre individuelle Praxis-IT und Datenschutz-Gesamtlösung handelt.

3.4 Optionen beim Versand von E-Mails in DS-Win

3.4.1 digital signierte E-Mails in DS-Win

Wenn für Ihre verwendete Absenderadresse ein privates Zertifikat installiert ist, wird der Haken „signiert“ freigegeben. Ohne privaten Schlüssel des Absenders ist die digitale Signatur nicht möglich und die Option bleibt daher inaktiv. Durch das Versenden einer digital signierten E-Mail wird der eigene öffentliche Schlüssel an den Empfänger übertragen, sodass er ihn installieren kann und verschlüsselt auf Ihre erste E-Mail antworten kann.

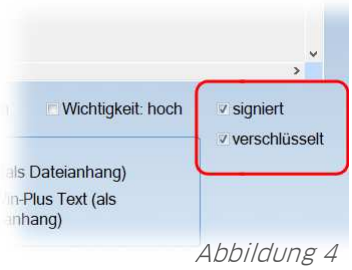

Abbildung 4

3.4.2 verschlüsselte E-Mails in DS-Win

Wenn DS-Win bei der Eingabe der E-Mailadresse im Empfänger-Feld feststellt, dass dafür ein öffentlicher Schlüssel installiert ist, wird der Haken „verschlüsselt“ zur Aktivierung freigegeben. Ohne öffentliches Zertifikat des Empfängers ist keine Verschlüsselung möglich und der Haken bleibt inaktiv.

Es ist nicht möglich, mehrere Emfänger mit einer einzelnen verschlüsselten E-Mail zu erreichen. Wenn Sie eine E-Mail an mehrere Empfänger senden und für einen davon kein öffentlicher Schlüssel installiert ist, wird die E-Mail an alle Empfänger unverschlüsselt versandt.

Ungültige oder abgelaufene Clientzertifikate werden von DS-Win nicht akzeptiert. Falls die Optionen „verschlüsselt“ und/oder „signiert“ nicht aktiv sind, obwohl Sie die passenden Zertifikate installiert haben, wenden Sie sich bitte an den Systemadministrator um die Gültigkeit zu überprüfen.

4 Sicherheitshinweise

4.1 Sicherheit von S/MIME und PGP

Anfang 2018 kursierten unter dem Oberbegriff „Efail“ Nachrichten darüber, dass die Verschlüsselung über S/MIME (und auch PGP) „geknackt“ sei. Diese Nachrichten waren oberflächlich recherchiert und vorschnell veröffentlicht worden. Die Verschlüsselung selbst gilt nach aktuellem Kenntnisstand weiterhin als sicher.

Tatsächlich ging es dabei um die Umsetzung dieser Verschlüsselungen in einigen E-Mail-Clients – also in den Programmen, die die Ver- und Entschlüsselung automatisch übernehmen sollen. Der mögliche Angriff erfolgte durch Fehler in der Verarbeitung von HTML-E-Mails.

Zum Schutz vor diesen und anderen Angriffen werden E-Mails in DS-Win in der Standard-Einstellung als einfacher Text (Option „Nur Text“) und damit ohne potenziell gefährliche HTML- oder JavaScript-Inhalte versandt.

Abbildung 5

4.2 Auswahl Ihres E-Mail-Anbieters

Nach unserer Erfahrung verwenden immernoch viele Praxen kommerzielle E-Mail-Provider mit sogenannten Free-Mail-Angeboten. Die prominentesten Beispiele sind hier GMX.DE, WEB.DE oder auch Google (GMAIL.COM). Diese kostenlosen Angebote werden fast ausschließlich über Werbung finanziert. Einige E-Mail-Anbieter scannen die Inhalte der E-Mails ihrer Kunden automatisiert und erstellen so genaue Benutzerprofile für personen- bzw. interessenbezogene Werbung. Neben der computergestützten Auswertung erhalten in bestimmten Fällen auch Menschen komplette Einsicht in Ihre elektronische Post.

Bei der Auswahl Ihres E-Mail-Providers sollten Sie Anbieter mit derartigen Praktiken grundsätzlich vermeiden. Das gilt insbesondere für die Übertragung von personenbezogenen Patientendaten.

Die Verschlüsselung über S/MIME kann E-Mail-Anbieter wirkungsvoll davon abhalten, Ihre E-Mails zu lesen.

DAMPSOFT GmbH
Vogelsang 1 / 24351 Damp

T 04352 9171-16 / F 04352 9171-90
info@dampsoft.de / www.dampsoft.de