Landschaftsverband Westfalen-Lippe

Elektronische Kommunikation

Leitfaden für eine sichere elektronische Kommunikation mit dem LWL

Stand: 11.04.2017
Version: 1.0

Für die Menschen.
Für Westfalen-Lippe.

Landschaftsverband Westfalen-Lippe

Autoren:	Herr Dieter Lehmkuhl Herr Dietmar Schönborner Frau Annette Freuer
E-Mail:	dieter.lehmkuhl@lwl.org dietmar.schoenborner@lwl.org annette.freuer@lwl.org

1 Ausgangslage

Der LWL kommuniziert täglich mit einer Vielzahl an Einrichtungen, Behörden und Partner per E-Mail.
Die E-Mail Kommunikation ist schnell und zuverlässig. Sie kann zeitnah Informationen bereitstellen, die für die weitere Bearbeitung von Prozessen zur Leistungserbringung erforderlich sind.

Die einfache E-Mail hat nur einen entscheidenden Nachteil: Die Informationen sind auf dem Übertragungsweg durch das Internet ungeschützt. In der Regel werden E-Mail Nachrichten und ihre Anhänge unverschlüsselt verschickt. Dabei besteht das potentielle Risiko, dass sensible Daten dieser E-Mail abgefangen und missbräuchlich verwendet werden könnten. Trotzdem bleibt die E-Mail das Transportmedium Nummer Eins für Informationen im täglichen Geschäftsverkehr. Die Nutzung der Papierpost ist eine denkbare, aber im Zuge der digitalen Transformation der Verwaltung eine unwirtschaftliche Variante der Kommunikationsbeziehungen.

Der LWL hat durch die Implementierung eines serverbasierten Systems die Möglichkeit geschaffen, verschlüsselt per E-Mail zu kommunizieren. Dadurch kann seitens des LWL eine sichere Übertragung sensibler Daten, vor allem personenbezogener, gewährleistet werden. Dazu ist es aber erforderlich, dass dem LWL der öffentliche Schlüssel des Kommunikationspartners vorliegt.

Alternativ kann mittels sogenannter Komprimierungsprogramme (z.B. 7-Zip) ein passwortverschlüsseltes Archiv erstellt werden. In diesem Archiv können Dokumente mit sensiblen Inhalten sicher abgelegt und anschließend per Mail verschickt werden.

Der LWL hat großes Interesse daran, die sichere Mail Kommunikation mit sensiblen und personenbezogenen Inhalten mit seinen Kommunikationspartner weiter auszubauen.

Dieser Leitfaden soll dabei helfen, die möglichen Verschlüsselungsalternativen des LWL aufzuzeigen und transparent zu machen. Es soll deutlich gemacht werden, dass durch die Nutzung von Verschlüsslungstechniken zum einen ein wirtschaftlicher Nutzen erzeugt wird, zum anderen aber auch rechtliche Sicherheit gewährleistet werden kann. Denn sensible Daten wie zum Beispiel Dokumente mit Personen Bezug dürfen aus Datenschutzgründen unverschlüsselt nicht per E-Mail verschickt werden.

2 Verschlüsselungsmöglichkeiten

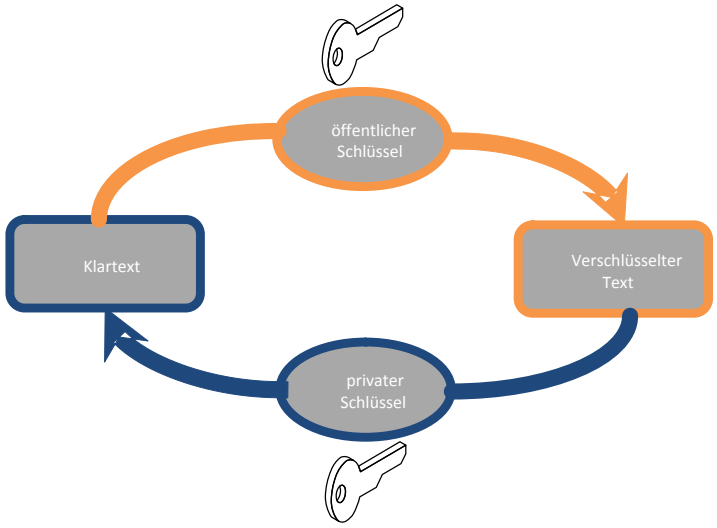
Der LWL bietet aktuell drei Möglichkeiten an, Informationen sicher zu übertragen.

2.1 Asynchrone Verschlüsselung (S/MIME-Standard)

Der LWL hat die Möglichkeit, über ein sogenanntes Verschlüsselungs-Gateway E-Mails sicher zu versenden.
Bei der asynchronen Verschlüsselung wird ein öffentlicher Schlüssel zum Verschlüsseln und der persönliche Schlüssel zum Entschlüsseln verwendet. Somit ist es erforderlich, dass der LWL und der Kommunikationspartner ihre öffentlichen Schlüssel austauschen.

Mit Hilfe des öffentlichen Schlüssels kann nun eine E-Mail samt Anhang verschlüsselt nach dem S/MIME-Standard versendet werden. Zur Verschlüsselung genügt ein geeigneter Mail-Client (z.B. Outlook oder Thunderbird).

Hier eine vereinfachte schematische Darstellung der Verschlüsselungstechnik:



Was ist ein öffentlicher Schlüssel?
Der öffentliche Schlüssel kann jedermann zum Verschlüsseln einer E-Mail oder einer Datei zur Verfügung gestellt werden.

Was ist ein privater Schlüssel?
Der private Schlüssel wird für die Entschlüsselung einer verschlüsselten E-Mail oder Datei benötigt. Dieser ist, wie der Name schon sagt, privat und sollte daher keinesfalls an Dritte weitergegeben werden.

Wie kann ich dem LWL verschlüsselte E-Mails schicken?

1. Laden Sie den öffentlichen Schlüssel des LWL auf der Kontaktseite des LWL-Internetauftritts (http://www.lwl.org/LWL/Der_LWL/Kontakt') herunter. Alternativ bitten Sie Ihren IT-Dienstleister den öffentlichen Schlüssel des LWL in die Mail-Infrastruktur aufzunehmen.
2. Installieren Sie den Schlüssel im Zertifikatsspeicher Ihres Computer-Betriebssystems (z.B. Windows). Hierzu doppelklicken Sie auf die Zertifikatsdatei, klicken im dann

erscheinenden Fenster auf "Zertifikat installieren" und folgen dann den Anweisungen des Assistenten.

Fertig. Der öffentliche Schlüssel des LWL hat sich automatisch in den Zertifikatspeicher installiert. Ab jetzt können Sie E-Mails an den LWL mit einem geeigneten Mailprogramm wie Outlook oder Thunderbird verschlüsselt versenden.

Wie kann der LWL mir verschlüsselte E-Mails schicken?

Ein so genanntes S/MIME- oder E-Mail-Zertifikat ist bei verschiedenen Dienstleistern erhältlich. Neben kostenlosen Zertifikaten (vor allem für Privatnutzer) gibt es diverse Angebote, die mit 20 bis 100 EUR/Jahr zu Buche schlagen, wobei sich die teureren Varianten eher an Business-Nutzer richten.

Wenn Sie ein Zertifikat erworben und den privaten Schlüssel in Ihr System integriert haben, können Sie uns den öffentlichen Schlüssel zur Verfügung stellen oder uns einen Hinweis geben, wo dieser heruntergeladen werden kann.

Wir speichern Ihren öffentlichen Schlüssel in unserem Verschlüsselungs-Gateway. Im Anschluss können wir auch Ihnen verschlüsselte E-Mails zusenden.

Die Vorteile von S/MIME

Zusammenfassend lässt sich sagen, dass nach S/MIME verschlüsselte E-Mails folgende Vorteile bieten:

- E-Mails werden vor dem Mitlesen durch Dritte geschützt
- Die Identität des Absenders kann überprüft werden
- Die Unversehrtheit der Nachricht kann überprüft bzw. nachträglich manipulierte Mails aufgedeckt werden

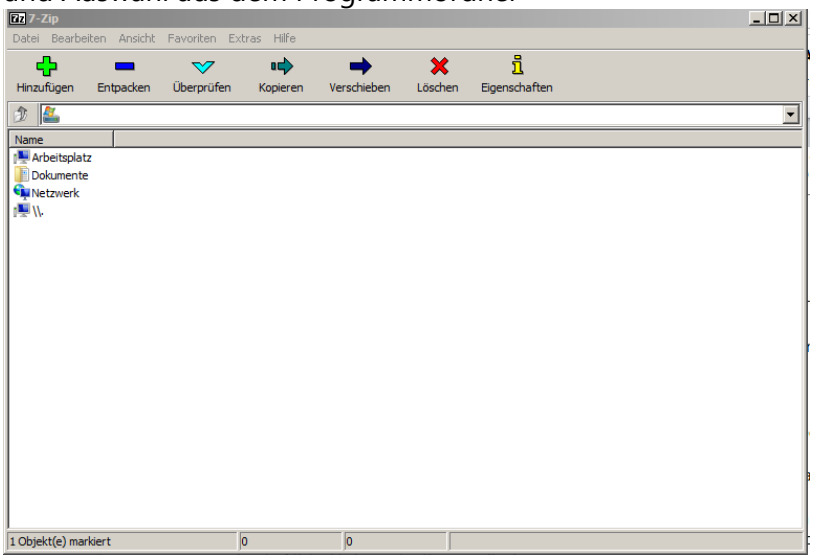
2.2 7-Zip

7-Zip ist ein kostenloses Open Source-Pack-Programm, das neben ZIP und RAR auch viele weitere Komprimierungsformate unterstützt.
Die mit Hilfe von Pack-Programmen erzeugten Dateien (Container-Archive) können auch mit einen Passwort gesichert bzw. verschlüsselt werden. Der AES-Verschlüsselungsalgorithmus mit einer Schlüssellänge von 256 Bit wird vom Bundesamt von Informationssicherheit (BSI) als hinreichend sicher angesehen.
Hinweis: Es wird nicht die E-Mail an sich, sondern nur das Container-Archiv (=Anhang) verschlüsselt. Ferner muss der Schlüssel für das Container-Archiv separat dem Kommunikationspartner mitgeteilt werden.

An dieser Stelle soll kurz per Screenshots dargestellt werden, wie das Tool in der Praxis funktioniert. Dafür ist es erforderlich, dass Sie sich dieses kostenfreie Tool aus dem Internet

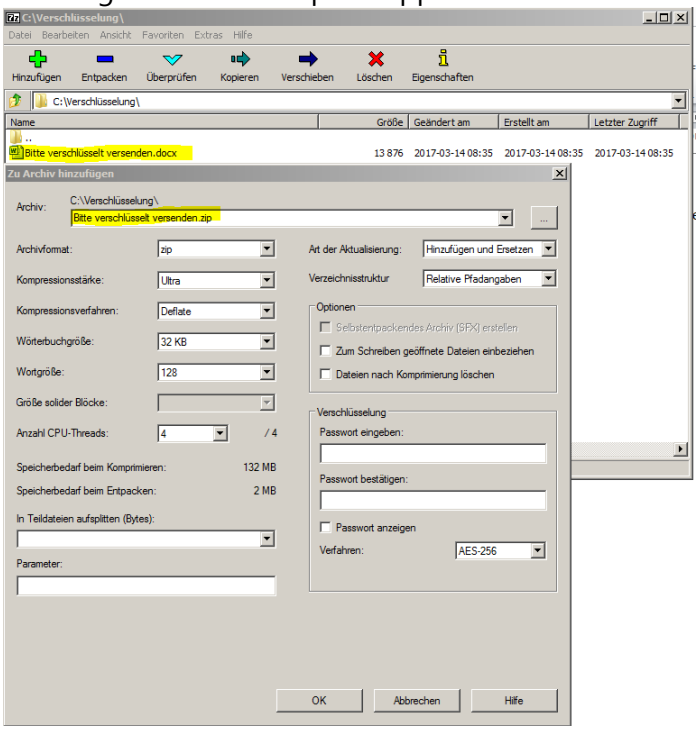
herunterladen und auf ihrem Computer installieren. Eine mögliche Quelle dazu ist: https://www.heise.de/download/

1. **Start des Programm** durch Doppelklick auf das Programm Icon auf dem Desktop und Auswahl aus dem Programmordner

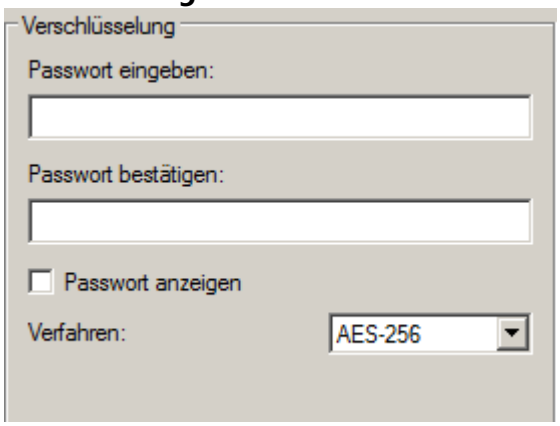


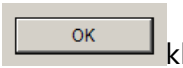
2. Klick auf **„Hinzufügen“**

3. **Auswahl des Dokumentes** aus dem üblichen Dateiverzeichnis, die verschlüsselt übertragen werden soll per Doppelklick:



4. **Passwort vergeben:**



Wir empfehlen ein mindestens 8-stelliges Passwort zu wählen, welches Ziffern und/oder Sonderzeichen enthält. Anschließend auf 

klicken.

5. 7-Zip erstellt im gleichen Ordner/Verzeichnis eine Containerdatei, die als Anhang einer normalen E-Mail mit verschickt werden kann. Dieser Anhang kann nur nur durch das separat mitgeteilte Passwort geöffnet werden.

Hinweis: Die eigentliche E-Mail bleibt unverschlüsselt!

3 Alternativen

3.1 De-Mail

Sie können den LWL auch über seine zentrale De-Mail-Adresse erreichen. De-Mail ist auf E-Mail basierendes elektronisch verschlüsseltes Transportsystem. Dabei können Dokumente verbindlich und vertraulich an einen Kommunikationspartner, der ebenfalls eine De-Mail-Adresse besitzt, übersandt werden.

Bei De-Mail ist garantiert, dass die Identitäten von Absender und Adressat eindeutig nachgewiesen und nicht gefälscht sind.
De-Mail Lösungen werden von großen Kommunikations-Providern angeboten. Im geschäftlichen Umfeld bieten auch hier verschiedene Provider Business-Lösungen an. Bitte haben Sie Verständnis, wenn wir Ihnen hier keine Vorschläge für De-Mail-Anbieter machen können.

Den LWL erreichen sie unter folgender De-Mail Adresse:

lwl@lwl.de-mail.de

Bei weitergehenden Fragen rund um De-Mail empfehlen wir Ihnen die Informationsseiten des Bundesamtes für Informationssicherheit (BSI).

3.2 Weitere Alternativen

Selbstverständlich können Sie sich zum Thema Verschlüsselung durch einen IT-Dienstleister beraten lassen. Bitte haben Sie Verständnis, dass wir Ihnen hierzu keine Empfehlungen geben können.

4 Nutzen

Durch die Nutzung der verschlüsselten E-Mail-Kommunikation erwarten wir auch einen wirtschaftlichen Nutzen. Kosten für Papier und Porto würden entfallen. Ebenfalls reduziert sich der Aufwand für die Erstellung der Papierbriefe, da das Kuvertieren der Briefe, sowie die Zustellung per Post entfällt. Die Vorgaben des § 3a Verwaltungsverfahrensgesetz NRW bleiben hiervon unberührt.
Nicht zu unterschätzen ist die zeitnahe Bereitstellung von Informationen, die für die weitere Bearbeitung in den Geschäftsprozessen benötigt werden.

Die verschlüsselte Kommunikation unterstützt die Forderung des Datenschutzes, sensible personenbezogene oder geschäftskritische Informationen nur mittels eines sicheren Übertragungsweges auszutauschen.

5 Ansprechpartner beim LWL

Möchten Sie uns Ihren öffentlichen Schlüssel bereitstellen, nehmen Sie bitte Kontakt mit dem jeweiligen Fachbereich auf, mit dem Sie verschlüsselt kommunizieren möchten. Dieser leitet Ihre Informationen an unseren IT-Dienstleister weiter.