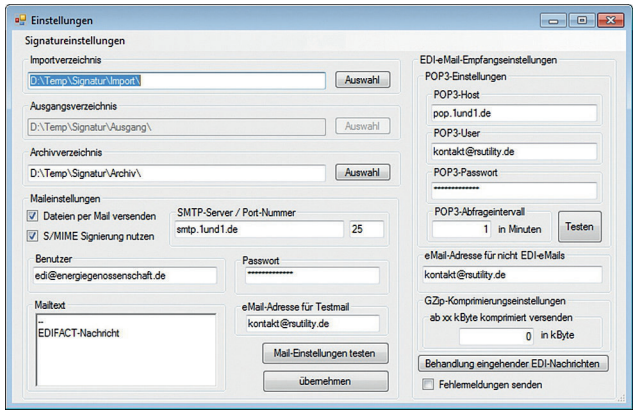


Einstellungen

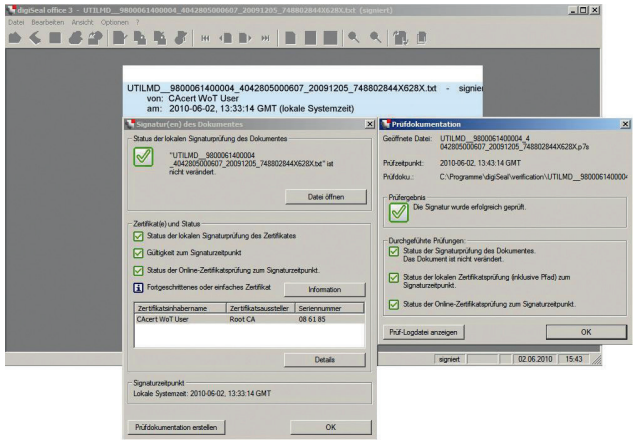
Im Bereich Einstellungen kann das Import-, Archiv- und bei Bedarf das Ausgangsverzeichnis ausgewählt werden. Bei der Auswahl <Dateien per Mail versenden> ist die Angabe eines Ausgangsverzeichnisses nicht erforderlich.

Adressdaten

Die eMail-Adressdaten des Senders und Empfängers werden anhand der ILN-Nummern und deren Position im Dateinamen der EDI-Nachricht automatisiert aus einer strukturierten CSV-Datei ausgelesen und zugeordnet. Dabei ist die Angabe einer eMail-Adresse als CC-Empfänger möglich. Es ist zu beachten, dass ein Verschlüsseln von eMails nur möglich ist, wenn Zertifikate aller Empfänger verfügbar sind.

Überprüfung von EDI- und Signatur-Dateien

Die von dem Programm signierten und versendeten Dateien können nach dem Versenden auf dem lokalen Computer des Empfängers jederzeit mit offiziell zugelassenen und von der Bundesnetzagentur bestätigten Programmen verifiziert und überprüft werden und entsprechen damit zu 100% der EDI-Kommunikationsrichtlinie:



EDI- Signatur-/eMail Cockpit-Software Professionell-Version

Um die Regeln zum Übertragungsweg zu erfüllen, kann die EDI-Signatur-/eMail Cockpit-Software Professionell-Version zusätzlich zu den o.g. Aufgaben auch komprimierte .gz-Dateien verschlüsselt (per S/MIME) und signiert (per S/MIME und/oder Dateisignierung) versenden sowie automatisiert:

- eMails von einem Postfach empfangen,
- prüfen, ob die Absender eMail mit dem Marktpartner übereinstimmt,
- verschlüsselte Nachricht entschlüsseln,
- gz-Dateien entpacken,
- mittels der S/MIME-Signatur die Nachricht auf Authentizität und Integrität prüfen,
- das zur S/MIME-Signierung verwendete Zertifikat auf Gültigkeit prüfen,
- Signierung mittels Signaturdatei erkennen,
- die EDI-Nachricht mit Hilfe der Signaturdatei auf Authentizität und Integrität prüfen,
- das zur Signierung verwendete Zertifikat auf Gültigkeit prüfen,
- prüfen, ob dem Empfänger das Zertifikat bekannt ist und er es akzeptiert hat,
- nicht-EDI-Nachrichten und fehlerhafte Nachrichten auf Wunsch an ein anderes Postfach weiterleiten.

Zusätzliche Funktionen:
- umfangreiche Optionen zur Zertifikatsprüfung,
- einfacher Import der Marktpartnerliste/Option zur Bearbeitung der Marktpartnerliste.

Die Software kann jedem CRM-System vorgeschaltet werden und die empfangenen Daten entweder über ein Austauschverzeichnis oder über einen Programmaufruf übergeben.

Whitepaper EDIFACT-Signatur-, Verschlüsselungs- und Mailcockpit

Funktionsumfang:	Verschlüsselung, Signierung sowie eMail-Versand von EDIFACT-Nachrichten und Prüfung empfangener eMails gemäß den Regeln zum Übertragungsweg des deutschen Energiemarktes.
Plattform:	.Net MS-Windows

techn. Mindestanforderung:

Betriebssystem:	Windows XP, Vista, Windows 7
Hardware (min)	Arbeitsspeicher 1 GB, CPU 1 GHz, Festplatte 70 GB
Hardware (empf.)	Windows-Leistungsindex > 4,5 Arbeitsspeicher > 1 GB, CPU > 1,6 GHz 4 Festplatten, je > 100 GB, (RAID-0+1-Konfiguration)

RS Utility Service UG (haftungsbeschränkt)
Hauptstr. 1
06772 Gräfenhainichen OT Möhlau

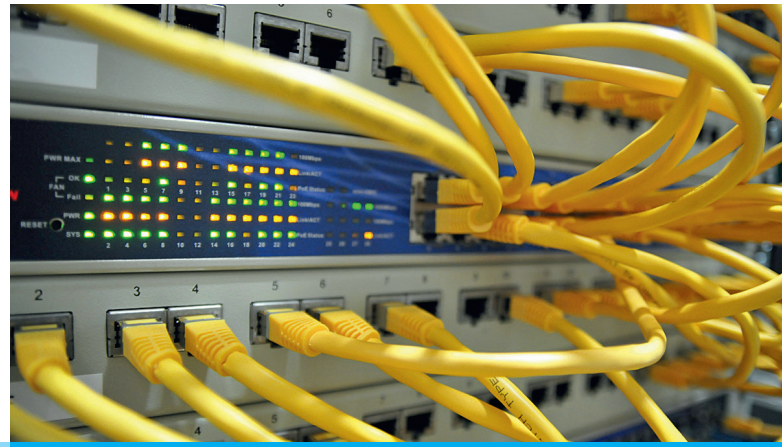
Tel: +49 (0) 34953 12326
eMail: kontakt@rs-utilityservice.de
Internet: www.rs-utilityservice.de

Softwarelösungen

RS Utility Service UG

EDI-Signatur-/ eMail Cockpit

EDIFACT-Signatur-, Verschlüsselungs- und eMailcockpit Software



- sichere Verschlüsselung und Signierung Ihrer eMails
- Prüfung eingehender eMails auf Authentizität und Integrität
- Versendung/Empfang von EDI-Nachrichten gemäß den Regelungen zum Übertragungsweg
- unterstützt
  - RSASSA-PSS-signierte Zertifikate
  - S/MIME RSASSA-PSS-Signatur
  - S/MIME RSAES-OAEP-Verschlüsselung

  optional verfügbar
  - Anbindung an das AS2-Datenübertragungssystem der RS Utitilty Service
  - SMS-Benachrichtigung bei Übertragungsfehlern
- schnelle Übersicht über Ihre EDI-Daten
- kein zusätzlicher Security-Server nötig
- Log-Informationen ermöglichen schnelle Fehleranalyse

Besonderheiten der EDIFACT-Kommunikation

Gemäß der EDI-Kommunikationsrichtlinie gibt es spezifische Vorgaben zur Nutzung von Verschlüsselung und Signatur bei EDIFACT-Kommunikation.

Für die Verschlüsselung der EDI-eMail ist S/MIME zu verwenden. Dann werden Signaturdatei und die EDIFACT-Nachricht an die eMail angehängt und versendet. Für die Verschlüsselung der die EDIFACT-Nachricht ist S/MIME zu verwenden. Weitere Nachrichten dürfen an eine EDIFACT-eMail nicht angehängt werden.

Das EDIFACT-Signatur-, Verschlüsselungs- und Mailcockpit übernimmt die Signierung, Verschlüsselung und Versendung von EDI-Nachrichten gemäß der EDI-Kommunikationsrichtlinie.

Die Anbindung an interne Systeme erfolgt über Austausch- bzw. Importverzeichnisse. Zusätzlich erfolgt eine Archivierung der bearbeiteten EDI-Dateien. Die in der EDI-Kommunikationsrichtlinie vorgegebene Vorgehensweise entspricht den finanzrechtlichen Vorschriften zum Versenden von elektronischen Rechnungen und damit dem deutschen Signaturgesetz.

Durch die Vorgaben der EDI-Kommunikationsrichtlinie gemäß dem Signaturgesetz kann z.B. die Authentizität einer EDIFACT-Nachricht in jedem auf den Empfang der Nachricht folgenden Verarbeitungs- und Prozessschritten verifiziert und geprüft werden. Damit entsprechen die Vorgaben der EDI-Kommunikationsrichtlinie der Forderung, dass die Authentizität und Integrität einer EDIFACT-Nachricht jederzeit unabhängig von der Art der Übertragung verifiziert werden kann.

So entfällt aber im Rahmen der EDIFACT-Kommunikation die Verwendung sogenannter „Security-Server“, welche die gesamte eMail signieren und die Signatur als zusätzliche Signaturdatei an die eMail anhängen.

Mit dem EDIFACT-Signatur-, Verschlüsselungs- und Mailcockpit werden die Vorgaben der EDI-Kommunikationsrichtlinie in Bezug auf Signierung und Verschlüsselung von EDIFACT-Nachrichten gesetzeskonform umgesetzt, indem die EDIFACT-Nachrichten automatisiert gemäß der EDI-Kommunikationsrichtlinie auf Wunsch signiert, verschlüsselt und dann automatisiert versendet werden.

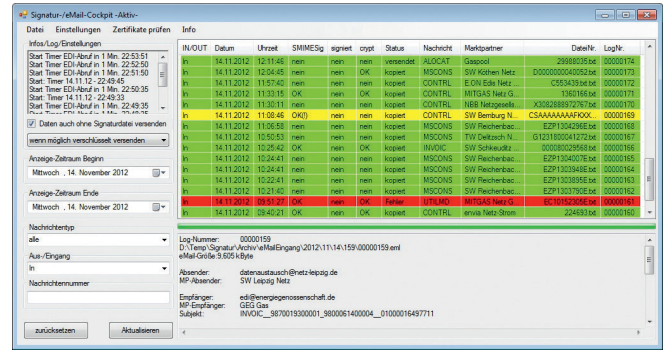
EDIFACT-Signatur-, Verschlüsselungs- und Mailcockpit Grundlagen

Die Signierung und Verschlüsselung erfolgt in der Regel über private und öffentliche Schlüssel, welche in sogenannten elektronischen Zertifikaten gespeichert sind. Da elektronische Zertifikate grundsätzlich strukturierte, textbasierte Dateien sind, können diese Zertifikate mit jedem beliebigen PC erzeugt werden. Solche selbst erzeugten elektronischen Zertifikate ohne die Anbindung an eine öffentlich zugängliche Public Key Infrastruktur (PKI) können jedoch nicht überprüft werden. Unabhängig davon kann jeder solchen selbst erzeugten Zertifikate vertrauen, wenn ihm der Aussteller persönlich bekannt ist.

Bei elektronischen Zertifikaten, welche von sogenannten Zertifizierungsstellen (Trustcenter) ausgegeben werden, wird die Identität des Besitzers des elektronischen Zertifikates von der Zertifizierungsstelle bestätigt. Gleichzeitig kann über eine öffentlich zugängliche PKI jederzeit die Gültigkeit eines elektronischen Zertifikates überprüft werden.

Mit der Herausgabe eines elektronischen Zertifikates beglaubigt die Zertifizierungsstelle de facto, dass das herausgegebene elektronische Zertifikat tatsächlich dem angegebenen Inhaber, vergleichbar einem Personalausweis, gehört. Rechtlich kann der Empfänger damit darauf vertrauen, das mit elektronischen Zertifikaten signierte Daten tatsächlich von dem Absender kommen, welcher als Inhaber im elektronischen Zertifikates eingetragen ist.

Technisch ist die Integrität der Absenderidentifikation mittels eines elektronischen Zertifikates jedoch daran gebunden, dass ausschließlich der Besitzer des Zertifikates über den privaten Schlüssel verfügt. Jeder, der den privaten Schlüssel eines Zertifikates kennt, kann sich als Inhaber des elektronischen Zertifikates und z.B. als Absender einer mit dem elektronischen Zertifikat signierten Datei ausgeben.



Hauptformular

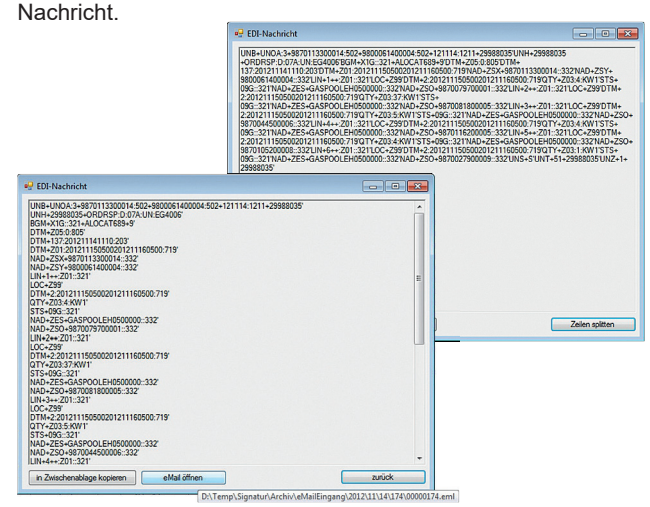
Das Hauptformular ermöglicht eine schnelle Übersicht über die erfolgreiche Verarbeitung von EDI-Daten und deren Versendung. Hinzu kommen diverse Einstellungs- und Suchfunktionen um einzelne EDI- Nachrichten aufzulisten. Im unteren Bereich werden die Log-Informationen über die Bearbeitung von EDI-Nachrichten angezeigt und ermöglichen eine schnelle Fehleranalyse z.B. bei fehlenden und ungültigen Zertifikaten.

Auf der linken Seite können individuelle Einstellungen zur Anzeige von bearbeiteten EDI-Nachrichten eingegeben werden, welche mit dem Button <Aktualisieren> in der Liste angezeigt werden. Hinzu kommen Log-Informationen im oberen linken Bereich des Formulars.

Als Option besteht nicht nur die Möglichkeit, ausgehende EDI-Nachrichten zu signieren und EDI-eMails zu verschlüsseln. Das EDI-Signatur-Cockpit prüft bei eingehenden EDI-eMails auch die Signaturen auf Gültigkeit, entschlüsselt und entzippt automatisch eMails und EDI-Nachrichten. Weiterhin ist eine Suchfunktion implementiert, mit welcher sich EDI-Nachrichten z.B. nach Nachrichtennummer, Zeitraum und Nachrichtentyp anzeigen lassen.

Anzeige von EDI-Nachrichten

Mittels Doppelklick auf eine Zeile der in der Liste angezeigten EDI-Nachrichten öffnet sich ein neues Fenster mit dem Inhalt der EDI-Nachricht. Durch Anklicken des Buttons <Zeilen splitten> wird die EDI-Nachricht zeilenorientiert angezeigt und ermöglicht eine schnelle Überprüfung des Inhaltes der EDI-Nachricht.



Anzeige verfügbarer elektronischer Zertifikate

Über das Menü <Signatureinstellungen> ist die Anzeige aller verfügbaren elektronischen Zertifikate mit der Information, ob ein privater Schlüssel zum Signieren verfügbar ist, möglich. Nutzbar sind Zertifikate:

a) des Zertifikatsspeichers des Benutzers
b) des Zertifikatsspeichers des Computers
c) Zertifikate, welche als Datei vorliegen