SUPPORT-INFORMATION

Umstellung Signaturverfahren (RSASSA-PSS) und Schlüsselverschlüsselung (RSAES-OAEP) bei EDIFACT-Nachrichten

Stand 13.11.2017

- proGOV Energy -

im Auftrag der
procilon GROUP

Gerd Hoffmann
procilon IT-Solutions GmbH

Inhaltsverzeichnis

1. Motivation und Risiken

1.1 Motivation

Spätestens ab dem 01.01.2018 muss die EDIFACT Kommunikation gem. den aktuellen Regelungen zum Übertragungsweg auf die in Anlage 5 des Beschlusses BK6-16-200 der Bundesnetzagentur genannten Verfahren umgestellt werden.
Hier der maßgebliche Auszug aus den Regelungen zum Übertragungsweg:

Zitatanfang

5.5.3 Algorithmen und Schlüssellängen für S/MIME

Es sind folgende Algorithmen und Schlüssel mit den genannten Schlüssellängen zu verwenden:

Signatur:
Hashfunktion (Hash algorithm): SHA-256 oder SHA-512 (gemäß IETF RFC 5754).
Signaturverfahren (Signature algorithm): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: RSASSA-PSS (gemäß IETF RFC 4056). Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden: sha256RSA / sha512RSA (RSASSA-PKCS1-v1_5) Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSASSA-PSS (gemäß IETF RFC 4056) RSA Schlüssellänge mindestens 2048 Bit

Verschlüsselung:
Inhaltsverschlüsselung (Content encryption): AES-128 CBC oder AES-192 CBC (gemäß IETF RFC 3565).
Schlüsselverschlüsselung (Key encryption): Grundsätzlich soll, sofern bei Sender und Empfänger verfügbar, eingesetzt werden: RSAES-OAEP (gemäß IETF RFC 3447). Vom 01.06.2017 bis 31.12.2017 muss zur Wahrung der Interoperabilität unterstützt werden: RSAES-PKCS1-v1_5 Ab 01.01.2018 muss ausschließlich eingesetzt werden: RSAES-OAEP (gemäß IETF RFC 3447) RSA Schlüssellänge mindestens 2048 Bit.

Zitatende

Die aktuellen und vollständigen Regelungen zum Übertragungsweg finden Sie hier: http://www.edi-energy.de/files2/EDI@Energy-Regelungen-zum-Übertragungsweg_v1.1_Lesefassung.pdf

1.2 Risiken

Uns liegt eine Bewertung des BDEW von Risiken und Fehlerquellen vor, die mit der Umstellung der Algorithmen verbunden sind.

Neben der geringen Verfügbarkeit der ab 01.01.2018 neu auszustellenden, mit RSASSA-PSS signierten Zertifikate, sind es vor allem die nicht verbindlich festgelegten Detail-Parameter, die für die eindeutige Konfiguration der neuen Algorithmen benötigt werden.

Der Verschlüsselungsalgorithmus RSAES-OAEP nach RFC 3560 benötigt mehrere Parameter:

- hashAlgorithm (Hash-Function)
- maskGenAlgorithm (Mask Generation Function) mit eigener Hashfunktion
- pSourceFunc (Encoding Parameter)

Grundsätzlich muss die Implementierung SHA-1 als Hashfunktion unterstützen. Allerdings sind hier auch die Hashfunktion SHA-256 und SHA-512 zugelassen. Sie müssen aber nach RFC nicht zwingend verwendet werden.

Der Signaturalgorithmus RSASSA-PSS nach RFC 4056 benötigt ebenfalls mehrere nicht definierte Parameter:

- hashAlgorithm (Hash-Function)
- maskGenAlgorithm (Mask Generation Function) mit eigener Hashfunktion
- saltLength
- trailerField.

Grundsätzlich muss die Implementierung SHA-1 als Hashfunktion unterstützen. Es kann aber ebenfalls SHA-256 und SHA-512 zur Anwendung kommen, dann allerdings für alle Hashfunktionen innerhalb der Signatur einheitlich.

Ebenso ist zu erwarten, dass nicht alle Marktpartner technisch in der Lage sind, die geforderten Algorithmen zu verarbeiten.

2. Umstellung E-Mail-Kommunikation

2.1 Generelles

Die im Kapitel 1 genannten Algorithmen müssen sowohl eingehend als auch ausgehend unterstützt werden.

Diese Algorithmen werden ab der proGOV Version 3.7.0 unterstützt. Stellen Sie also bitte sicher, dass Sie diese oder eine höhere Version einsetzen.

Sie erkennen die Version, in dem Sie sich an der proGOV WebAdmin anmelden. Auf der Startseite ist die eingesetzte Version im Feld „Systemübersicht“ dargestellt.

Der Maileingang nutzt die Aktionen „`DecryptSMIME`“ und „`VerifiySMIME`“ zur Entschlüsselung und Signaturprüfung. Diese Aktionen müssen nicht angepasst werden, da proGOV eingehend standardmäßig alle Algorithmen unterstützt.

Innerhalb des proGOV Regelwerkes werden die kryptographischen Funktionen für den Mailversand in den Aktionen „`EncryptSMIME`“ und „`SignSMIME`“ konfiguriert.

Je nachdem, welche Logik Sie verwenden, kann das Regelwerk unterschiedlich aufgebaut sein. Evaluieren Sie zuerst die Regeln, die die Signatur und Verschlüsselung für die Marktkommunikationsadressen steuern. Dies kann auch an mehreren Stellen im funktionalen Regelwerk vorkommen.

Sind Sie hier unsicher, können Sie auch das progov.log zu Rate ziehen. Hier werden die verwendeten Regeln geloggt.
Sind die Stellen evaluiert, ändern Sie die Aktionen wie in den folgenden Kapiteln beschrieben.

2.2 Aktion SignSMIME

Ändern Sie die Einstellung der Aktion „`SignSMIME`“ nur im Feld „`enableRSASSA-PSS`“, in dem Sie den Wert „`true`“ eingeben.

Bitte nehmen Sie keine Änderungen in den *Auswählbaren Attributen* vor.

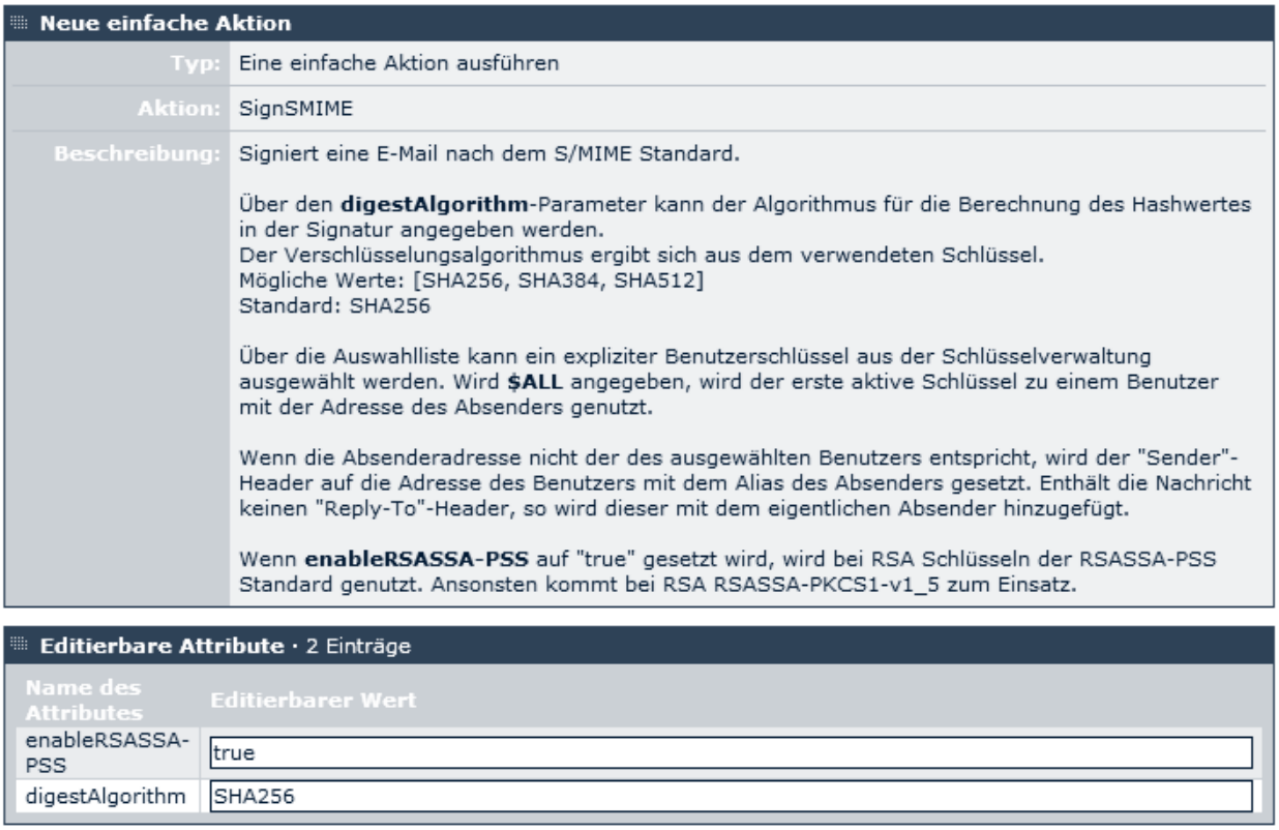


Abbildung 1: Aktion SignSMIME

2.2 Aktion EncryptSMIME

Ändern Sie die Einstellung der Aktion „`EncryptSMIME`“ nur im Feld „Key-Verschlüsselungsalgorithmus“, in dem Sie den Wert

„`RSA/NONE/OAEPWITHSHA1ANDMGF1PADDING`“[1]

eingeben. Bitte nehmen Sie auch hier keine Änderungen in den *Auswählbaren Attributen* vor.

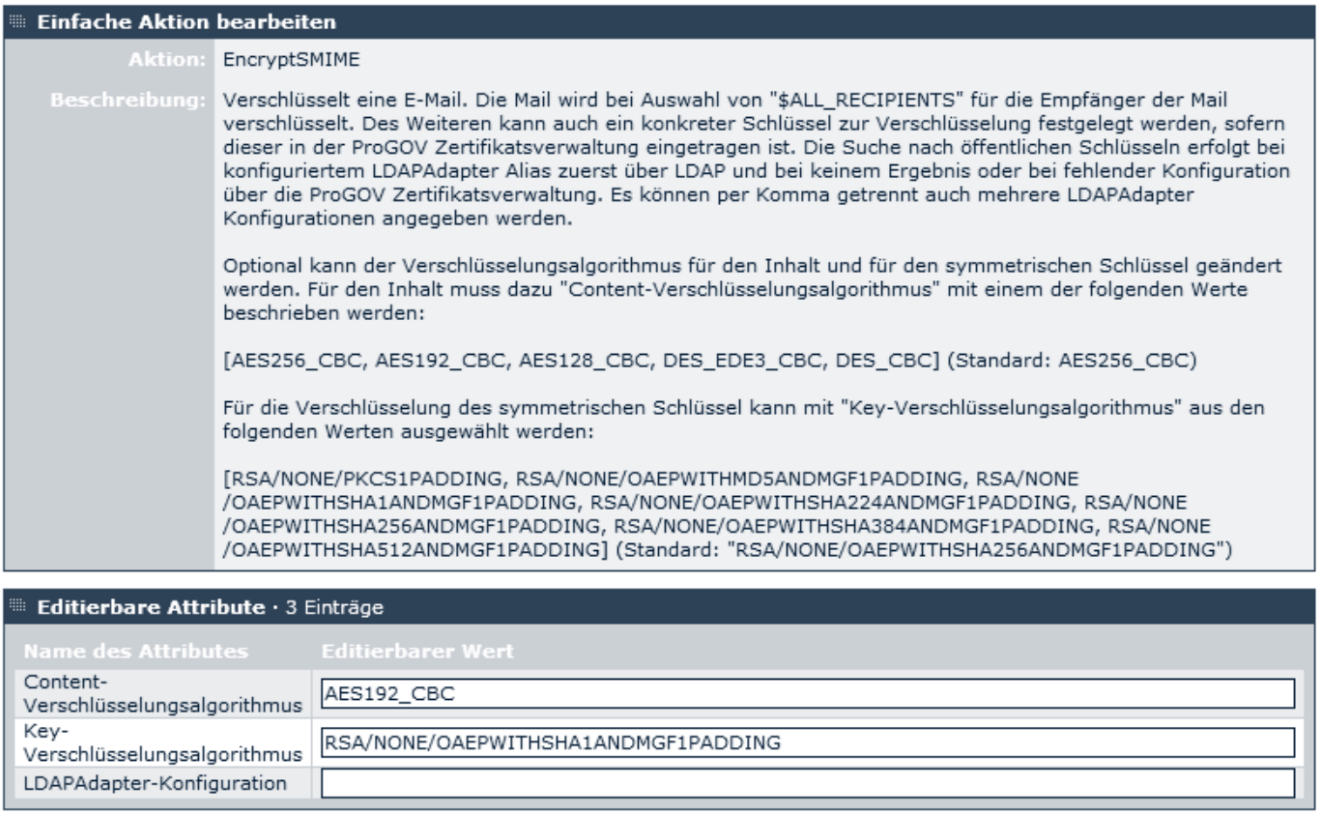


Abbildung 2: Aktion EncryptSMIME

[1] Die Empfehlung, diesen speziellen OAEP-Algorithmus zu verwenden, beruht auf der Risikoanalyse des BDEW sowie der Inhalte der entsprechenden RFC. Selbstverständlich kann hier jeder andere OAEP-basierte Algorithmus konfiguriert werden.

2.3 Globale Umstellung oder Marktpartner-individuelle Umstellung

In den letzten Tagen erhalten wir zahlreiche Supportanfragen, wo Mails von diversen Marktpartnern weitergeleitet werden, die Interoperabilitätstests durchführen möchten.
Dazu kann Sie prinzipiell niemand verpflichten, aber natürlich kann diese Funktionalität im Regelwerk abgebildet werden.

Fügen Sie einen Block vor den bisherigen Signatur- und Verschlüsselungsregeln ein, in dem Sie die speziellen Empfänger mit einem Matcher (beispielsweise mit „`RecipientIs`“ - hier Regel 21) identifizieren.

Der Regelblock kann dann wie folgt aussehen:

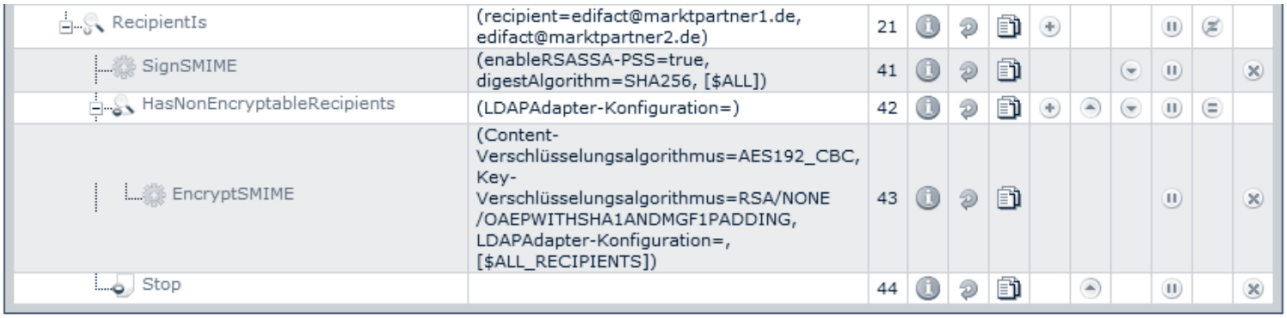


Abbildung 3: Regelblock für MP-individuelle Umstellung

Natürlich kann die Logik auch umgedreht werden, in dem Sie den individuellen Block für die Verwendung der alten Algorithmen einsetzen und global die neuen Algorithmen konfigurieren.

3. Umstellung AS2-Kommunikation

3.1 Generelles

Die im Kapitel 1 genannten Algorithmen müssen sowohl eingehend als auch ausgehend unterstützt werden. Diese Algorithmen werden ab der Version 3.6.1 des AS2Adapters unterstützt. Stellen Sie also bitte sicher, dass Sie diese oder eine höhere Version einsetzen.

Sie erkennen die Version, in dem Sie sich an der proGOV WebAdmin anmelden. Navigieren Sie über die Menüpunkte auf

```
Komponenten – proGOV Adapter – Anfragegesteuerte Adapter
```

Hier erkennen Sie die Version des AS2Adapter.

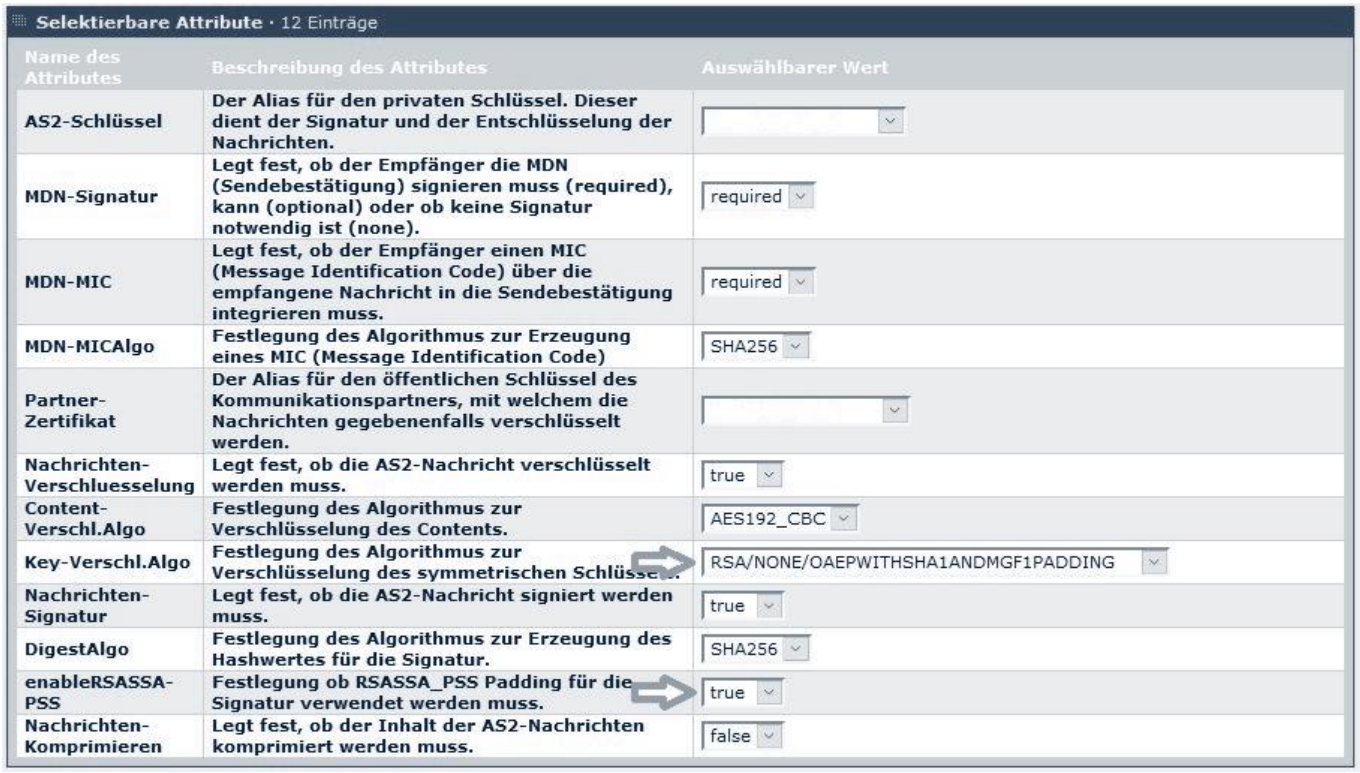
3.1 Umstellung in der AS2-Konfiguration

Die Algorithmen müssen dann in **JEDER** produktiven AS2-Konfiguration einzeln angepasst werden.

Navigieren Sie über die Menüpunkte auf

`Komponenten – proGOV Module – ServerKommunikationAS2`

und rufen jede Konfiguration einzeln auf und passen diese wie folgt an.



Selektierbare Attribute · 12 Einträge

Name des Attributes	Beschreibung des Attributes	Auswählbarer Wert
AS2-Schlüssel	Der Alias für den privaten Schlüssel. Dieser dient der Signatur und der Entschlüsselung der Nachrichten.	
MDN-Signatur	Legt fest, ob der Empfänger die MDN (Sendebestätigung) signieren muss (required), kann (optional) oder ob keine Signatur notwendig ist (none).	required
MDN-MIC	Legt fest, ob der Empfänger einen MIC (Message Identification Code) über die empfangene Nachricht in die Sendebestätigung integrieren muss.	required
MDN-MICAlgo	Festlegung des Algorithmus zur Erzeugung eines MIC (Message Identification Code)	SHA256
Partner-Zertifikat	Der Alias für den öffentlichen Schlüssel des Kommunikationspartners, mit welchem die Nachrichten gegebenenfalls verschlüsselt werden.	
Nachrichten-Verschluesselung	Legt fest, ob die AS2-Nachricht verschlüsselt werden muss.	true
Content-Verschl.Algo	Festlegung des Algorithmus zur Verschlüsselung des Contents.	AES192_CBC
Key-Verschl.Algo	Festlegung des Algorithmus zur Verschlüsselung des symmetrischen Schlüssels.	RSA/NONE/OAEPWITHSHA1ANDMGF1PADDING
Nachrichten-Signatur	Legt fest, ob die AS2-Nachricht signiert werden muss.	true
DigestAlgo	Festlegung des Algorithmus zur Erzeugung des Hashwertes für die Signatur.	SHA256
enableRSASSA-PSS	Festlegung ob RSASSA_PSS Padding für die Signatur verwendet werden muss.	true
Nachrichten-Komprimieren	Legt fest, ob der Inhalt der AS2-Nachrichten komprimiert werden muss.	false

Abbildung 4: Beispiel AS2-Konfiguration

Entscheidend sind hier die beiden Parameter „`Key-Verschl.Algo`“ und „`enableRSASA-PSS`“.
Bitte ändern Sie andere Parameter nur nach Absprache mit dem AS2-Kommunikationspartner.
Bitte ändern Sie keine Werte im Bereich *„Editierbare Attribute“.*

Ändern Sie den Wert des Parameters „`Key-Verschl.Algo`“ auf:

„`RSA/NONE/OAEPWITHSHA1ANDMGF1PADDING`“[2],

Ändern Sie den Wert des Parameters „`enableRSASA-PSS`“ auf:

„`true`“.

[2] Die Empfehlung, diesen speziellen OAEP-Algorithmus zu verwenden, beruht auf der Risikoanalyse des BDEW sowie der Inhalte der entsprechenden RFC. Selbstverständlich kann hier jeder andere OAEP-basierte Algorithmus konfiguriert werden.

4. Zeitpunkt der Umstellung

Den Zeitpunkt der Umstellung können Sie selbst festlegen. Allerdings gibt es einige Punkte zu beachten, insbesondere die Regeln für die Interoperabilität.

Entscheiden Sie sich für eine globale Umstellung der Algorithmen für alle Marktpartner, dann sollten Sie den Zeitpunkt so spät wie möglich, spätestens aber am 01.01.2018 00.00 Uhr durchgeführt haben. Stellen Sie erst nach diesem Datum um, erfüllen Sie die Vorgaben der Kommunikationsrichtline im Zeitraum von 01.01.2018 00.00 Uhr bis zur Umstellung nicht. Dies kann ggf. zu Beschwerden führen.

Stellen Sie zu zeitig um, kann es Probleme mit der Interoperabilität geben, Marktpartner könnten also eventuell Ihre gesendeten Nachrichten nicht entschlüsseln bzw. deren Signaturen prüfen.
Umstellung innerhalb der AS2-Kommunikation führen Sie bitte immer erst nach Rücksprache mit dem Kommunikationspartner durch.