Wartung und Pflege

Zeichen	181/2011
Status-Modellierung	intern geprüft
Status-Test	keine Änderung
Status Testgenerator	keine Änderung
Umsetzung	J

Aufnahme von Regelungen zur Authentifizierung von Absendern

Problemstellung

Für eine sichere Datenübermittlung im Meldewesen ist es erforderlich, dass der Empfänger einer XMeld-Nachricht prüft, ob der Absender einer Nachricht berechtigt war, diese zu versenden. So muss beispielsweise durch die empfangende Meldebehörde sichergestellt werden, dass eine Rückmeldungsnachricht 0201 von einer anderen Meldebehörde und nicht durch einen unbefugten geschickt worden ist.
Die für diese Prüfung zu verwendenden Verfahren der Authentisierung von Absendern mit Hilfe des DVDV sind in XMeld nicht beschrieben.

Lösung

Die Spezifikation wurde um die Beschreibung der zwei verwendeten Verfahren zur Authentisierung von Absendern ergänzt.

Antragsdetails

Antragsteller: OSCI Leitstelle
Erfasst am: 17.09.2009
Bezug: Spezifikation 1.5 – Anhang F

Analyse des Änderungsantrags

Die in XMeld verwendete Methode zur Authentifizierung des Absender einer OSCI-XMeld Nachricht mit Hilfe des DVDV ist aktuell nicht in der Spezifikation beschrieben.

Lösungsvorschlag im Änderungsantrag

Das vom BfJ verwendete mit dem DVDV bereits abgestimmte Verfahren zur Authentifizierung des Absenders einer OSCI-XMeld Nachricht sollte im Anhang F als verbindliche Methode der Authentifizierung beschrieben werden.

Bewertung

Bewertungskriterien									
Gesetzliche Vorgabe	Fehler	Eindeutigkeit	XÖV-Konformität	Erleichterung MB	Erleichterung AB	XMeld-Prozesse	Wartbarkeit	Fachlicher Aspekt	Detail
0	0	1	0	0	0	0	0	0	1

Aufwandsschätzung	
Modellierung	0,17
Test	0,17
Hersteller	0

Betroffene Dokumente	
Spezifikation	
Has	
Verwandte CRs	

Bewertet durch:EG W&P ***Bewertet am: EG09-11***

Änderung sinnvoll, aber nicht dringend

Bearbeitung

Wartend auf:

Betrifft	Aktivität	Status Mod	Status Test
Spezifikation	Umsetzung der Ergebnisse gemäß Bearbeitung von 2012-05-09 AG Mod	2012-05-14	2012-05-16
Spezifikation	Nachbearbeitung an Bild 20-2 gemäß 2012-05-16	2012-05-24	

Bearbeitet durch:BfJ ***Bearbeitet am: 2010-09-28***
Bearbeitungsdauer:

Im aktuellen Verfahren des BfJs wird mit dem AGS und der Kategorie "Meldebehörde" beim DVDV angefragt. Erst wird der AGS in der zurückgelieferten Liste mit AGSn gesucht. Danach vergleichen wir die zurückgelieferten Clientzertifikate, an Hand der Seriennummer, mit dem Zertifikat, mit dem die Nachricht durch die Meldebehörde verschlüsselt wurde. Sind AGS und Clientzertifikat in der Rückgabe entsprechend den Vorgaben vorhanden, so erteilen wir der Behörde den Status "berechtigt".

Realisiert haben wir das über ein Objekt der Klasse DVDVManager (DVDV SDK) mit der Methode FindAuthorityDescriptionRequest. Diese Methode erhält als Parameter einmal den AGS und als zweites die Kategorie, also Meldebehörde. Die Rückgabe der Methode wird nach obiger Beschreibung verarbeitet.

Bearbeitet durch: WS Wohnungswechsel ***Bearbeitet am: 2011-11-22***

Auf dem Workshop zum Thema Wohnungswechsel hat sich erneut der Bedarf für die Beschreibung der Abläufe der Authentifizierung herausgestellt. Bei gemeindeübergreifenden Umzügen innerhalb der Zuständigkeit einer Meldebehörde muss für den Empfänger der Nachricht die Zuständigkeit der Meldebehörde für die entsprechende Gemeinde geprüft werden.

Im Zuge der Diskussionen auf dem Workshop hat sich gezeigt, dass über das Zusammenspiel von OSCI-Transport und dem DVDV unterschiedliche Auffassungen existieren. In der weiteren Bearbeitung dieses Änderungsantrags soll das Verfahren der Authentifizierung der Absender und der Aspekt der Zuständigkeit aufbereitet und in der Spezifikation als verbindliches Verfahren beschrieben werden.

Bearbeitet durch: AG Modellierung ***Bearbeitet am: 2012-05-08***

1) Abschnitt 20.1.3, I, a – neuer dritter Absatz:

Auf Empfängerseite ist darüber hinaus die Authentifizierung hinsichtlich der DVDV-Behördenkategorie durchzuführen. Dafür stehen zwei unterschiedliche Varianten zur Verfügung, die beide geeignet sind, um Nachrichten unberechtigter Absender abzuweisen:

Variante a)

- Der Empfänger prüft, ob die Behördenkategorie des Senders für diesen Dienst berechtigt ist.
- Der Empfänger identifiziert über Behördenkennung und Behördenkategorie den Sender im DVDV (`FindAuthorityDescription`).
- Das DVDV übermittelt Informationen zu dem Sender. Sollte kein Eintrag im DVDV identifiziert werden können, kann der Sender nicht authentifiziert werden (RtS mit Schlüssel T070 und ggf. weiteren ergänzenden (Freitext-)Hinweisen).
- Der Empfänger vergleicht das vom DVDV erhaltene Clientzertifikat mit dem Senderzertifikat aus der Nachricht:
  - identisch: Sender ist authentifiziert – Nachricht verarbeiten
  - nicht id.: Sender ist nicht authentifiziert – RtS mit Schlüssel T070 und ggf. weiteren ergänzenden (Freitext-)Hinweisen

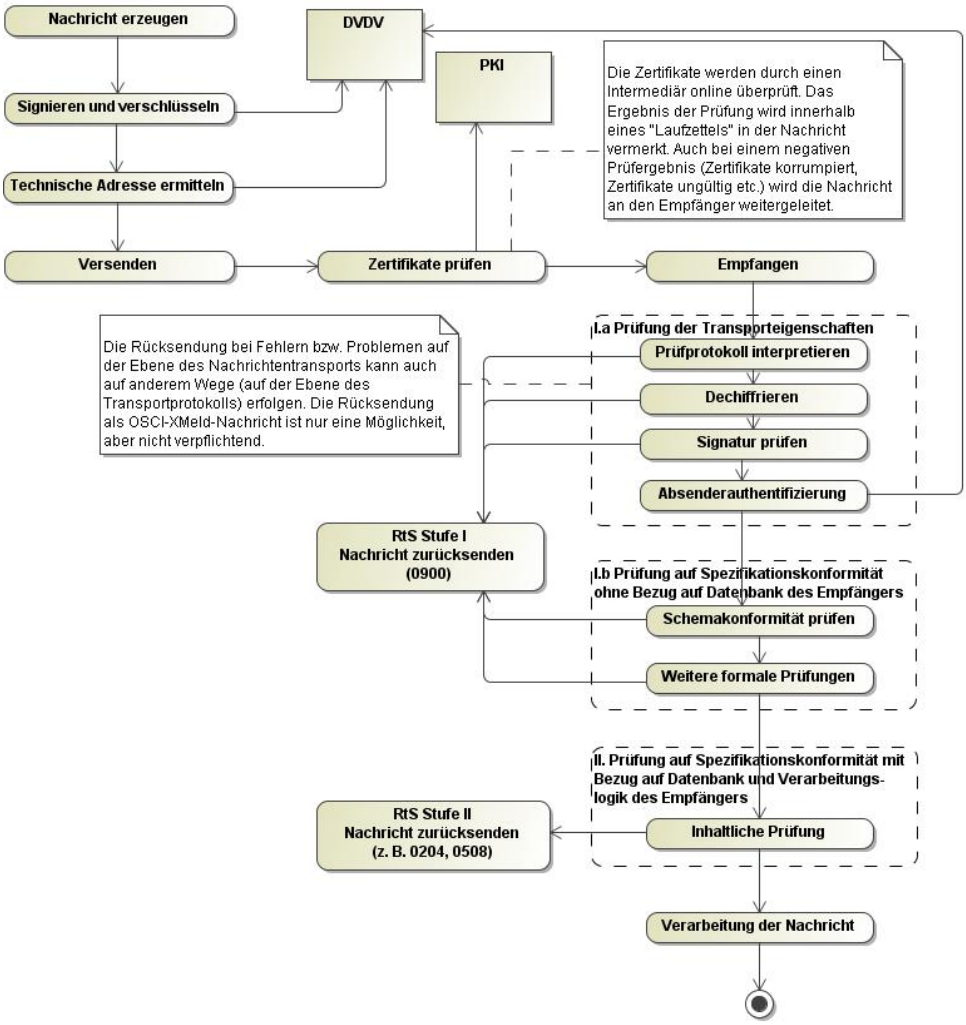
Variante b)

- Der Empfänger prüft, ob die Behördenkategorie des Senders für diesen Dienst berechtigt ist.

- Der Empfänger übermittelt dem DVDV das in der Nachricht enthaltene Zertifikat und die Behördenkategorie des Senders (`VerifyCategory`).
- Das DVDV übermittelt `true` oder `false` an den Empfänger:
  - `true`: Sender ist authentifiziert – Nachricht verarbeiten
  - `false`: Sender ist nicht authentifiziert – RtS mit Schlüssel T070 und ggf. weiteren ergänzenden (Freitext-)Hinweisen

2) Bild 20-2 erneuern:

In MagicDraw wurden Fehler korrigiert und der Aspekt der Authentifizierung aufgenommen. Das Bild muss aber noch in die Spez. übernommen werden:



Hinweis zu Ziffer 1) und 2): Entgegen dem Lösungsvorschlag wurde das Thema Authentifizierung nicht in Anhang F sondern in Kap. 20.1 beschrieben, da bei nicht erfolgreicher Authentifizierung eine RtS-Nachricht geschickt werden muss.

3) Zum Thema „Aspekte der Zuständigkeit“ aus dem Wohnungswechsel-Workshop vom 2011-11-22:

1. **Veröffentlichte AGS-Tabelle von destatis nicht ausreichend aktuell und ohne Angaben zur Historie**:
   Empfänger von Nachrichten können im Zweifel nicht mehr sicherstellen, dass der Sender mit einem jetzt geänderten AGS zuständig ist für einen gespeicherten,

veralteten AGS.
CR erstellen (ToDo 03 aus EG12-05)

2. **Umgang mit gemeindeübergreifenden Wohnungswechseln innerhalb von Verwaltungsgemeinschaften in der Kommunikation mit dem BZSt:**
   CR erstellen (ToDo 04 aus EG12-05)

Nach Einarbeitung der bearbeiteten Ziffern 1) und 2) ist dieser CR erledigt.

Bearbeitet durch: KoSIT/JH ***Bearbeitet am: 2012-05-09***

Für den *"Umgang mit gemeindeübergreifenden Wohnungswechseln innerhalb von Verwaltungsgemeinschaften in der Kommunikation mit dem BZSt"* muss kein neuer CR erstellt werden. Der Aspekt ist bereits in **CR 2011-263** "Klarstellung von Gemeindeverband / Verwaltungsgemeinschaft", der zum BMG-Release eingeplant ist.

Bearbeitet durch: Ullrich Bartels ***Bearbeitet am: 2012-05-14***

Die Ziffern 1 und 2 aus der Bearbeitung vom 2012-05-08 wurden umgesetzt, die Versionshistorie fortgeschrieben.

Bearbeitet durch: interne QS ***Bearbeitet am: 2012-05-14***

1) Die Frage wird aufgeworfen, warum die Änderungen nicht im Kapitel "Allgemeine Prozessmuster" aufgenommen worden ist. Dies soll zumindest im Rahmen der Neugliederung der Spezifikation noch einmal erörtert werden.

2) Bild 20-2: Kleine Korrekturen an der Abbildung:
   - Kontrollfluss „Absenderauthentifizierung“ -> „RtS Stufe I“ aufnehmen
   - Kontrollflüsse hervorheben, um den Unterschied zu den Objektflüssen darzustellen.

3) Abschnitt 20.3.1: Text wurde geprüft und ist aufgenommen worden.
4) Versionhistorie ist geprüft

Bearbeitet durch: KoSIT / HW ***Bearbeitet am: 2012-05-16***

Der CR gemäß der Bearbeitung vom 8.5.2012 Ziffer 3.1 ist als CR 23/2012 erfasst.
Das ToDo aus der Bearbeitung vom 8.5.2012 Ziffer 3.2 ist nicht als neuer CR erfasst worden. Es ist stattdessen in den CR 236/2011 eingeflossen.

Bearbeitet durch: Ullrich Bartels ***Bearbeitet am: 2012-05-24***

Bearbeitung gemäß interner QS vom 2012-05-16:

- Zu Ziffer 1: Es muss sichergestellt werden, dass im Rahmen der Neugliederung der Spezifikation dieser Punkt Berücksichtigung findet.
- Zu Ziffer 2: Die Korrekturen an Bild 20-2 wurden vorgenommen, eine Änderung der Versionshistorie war nicht notwendig.