COMPINIA IT SERVICES

AS2

Die neue EDI-Kommunikationstechnologie

IT-Symposium 2006 – Experten im Dialog
Düsseldorf

2E03 17.05.2006

Joachim Just

EDI-Standards - Formate

COMPINIA IT SERVICES

- Zum Teil schon sehr alt und eingebürgert
- Beschreiben Struktur und Format von EDI-Dokumenten
- Transport und Austausch von EDI-Dokumenten bleiben unberücksichtigt

EDI-Standards - Formate

- UN/EDIFACT – Electronic Data Interchange for Administration, Commerce and Transport
  - UN/CEFACT
  - 1988
- ANSI ASC X.12
  - ANSI Accredited Standards Commitee
  - 1982
- ebXML – electronic business XML
  - gesponsort von UN/CEFACT
  - 2001

EDI - Transportproblematik

- Bisher Übertragung über Punkt-zu-Punkt Verbindungen
- Verschiedene Protokolle (e.g. FTAM, Odette)
- Vom Sender zum Empfänger direkt (eher seltener)
- Vom Sender zum VAN-Provider und von dort zum Empfänger (e.g. X.400)
- Vorteil: Kein Unbefugter kann sich dazwischenschieben
- Statt teures VAN Peer-to-Peer Übertragung über das Internet
- Problem: Sicherheit und Zuverlässigkeit

EDI – Sicherheit und Zuverlässigkeit

- Was bedeutet Sicherheit?
  - Vertraulichkeit
  - Integrität
  - Authentizität (das Wichtigste!)
- Wie können diese Ziele erreicht werden?
  - Kryptographie
  - Verschlüsselung
  - Message Digest / Hash-Algorithmen
  - Signaturen

Kryptographie - Schlüssel

- Symmetrische Schlüssel
  - Klassische Bedeutung von Schlüssel
  - Schnell
  - Problem: Schlüsselmanagement (Austausch, Anzahl)
- Asymmetrische Schlüssel (public / private)
  - Public Key Cryptographie (PKC)
  - Nicht so schnell
  - Lösung des Schlüsselmanagementproblems (zusammen mit den Zertifikaten)

  - Public Key Infrastructure (PKI)

Kryptographie - Zertifikate

COMPINIA IT SERVICES

- Ausgangspunkt: Schlüsselverwaltung
- Man-in-the-Middle Problematik
- Certificate Authority (CA)
- Schritte zur Erstellung
  - Generieren des Schlüsselpaars
  - Certificate Signing Request (CSR)
  - CA generiert Zertifikat
- Format X.509 (RFC 2459)
- Hauptkomponenten
  - Gültigkeit
  - Issuer / Subject als Distinguished Names
  - Public Key des Subjects
  - Verwendungszweck (e.g. Verschlüsselung, Signierung)
  - Signatur der CA

Kryptographie – Symmetrische Schlüssel

COMPINIA IT SERVICES

- Stream Ciphers
  - RC4 – Ron Rivest, ~1975, 8-2048 Bit
- Block Ciphers
  - Normal 64 Bit Blöcke
  - DES – NBS / NIST, 1977, 56 Bit
  - 3DES(EDE) – ANSI, 1985, 168 Bit (effektiv 112 Bit)
  - RC2 – Ron Rivest, ?, variabel (normal 128 Bit)

Kryptographie – Asymmetrische Schlüssel

COMPINIA IT SERVICES

- 1976 Stanford:
  Whitfield Diffie, Martin Hellmann: New Directions in Cryptographie
- 1970-74 Großbritannien:
  Communications–Electronics Security Group (CESG)
- 1977:
  Ron Rivest, Adi Shamir, Len Adelman (RSA)

Kryptographie – Message Digest

COMPINIA IT SERVICES

- Hash-Algorithmus
- Irreversibilität
- Kollisionsresistenz
- MD5: Ron Rivest, 1991 (RFC 1991), 128 Bit
- SHA-1: NIST und NSA, 1994 (RFC 3174), 160 Bit

Kryptographie - Signaturen

- Hash-Algorithmus über den Text
- Verschlüsselt mit dem privaten(!) Schlüssel des Senders

Kryptographie - Literatur

- Eric Rescorla: SSL and TLS, Designing and Building Secure Systems, Addison-Wesley 2001
- Bruce Schneier: Applied Cryptography, John Wiley & Sons 1996
- Simon Singh: Geheime Botschaften, Carl Hanser 2000

AS – Applicability Statement

- IETF/EDIINT – Internet Engineering Task Force, Arbeitsgruppe „EDI over the Internet“
- AS1
  - Basierend auf SMTP
  - Email-System
  - Keine Echtzeit-Kommunikation
- AS2
  - Basierend auf HTTP(S)
  - Echtzeit-Kommunikation
- AS3
  - Basierend auf FTP
  - Wegen allgemeiner Sicherheitsproblematik von FTP nicht sehr verbreitet
- Allen gemeinsam S/MIME

AS2 - Standardisierung

- RFC 4130:
  MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)
  July 2005
  Dale Moberg, Cyclone Commerce
  Rik Drummond, Drummond Group Inc.
- Davor:
  Internet Draft (draft-ietf-ediint-as2-20.txt)
  21. Dezember 2004, expires May 2005
  Verfasser wie oben
- Begleitend:
  Internet Draft (draft-ietf-ediint-compression-05.txt)
  August 2005, expires February 2006
  Tery Harding, Cyclone Commerce

AS2 - Charakteristika

- Zielrichtung: gesicherter und zuverlässiger Austausch von Geschäfts-dokumenten (aber nicht ausschließlich)
- Maximalziel: Non-Repudiation of Receipt, deutsch: Nicht-Ablehnung
- Basiert u.a. auf RFC 2616 Hypertext Transfer Protocol
- Daneben auf einer Reihe von weiteren RFCs
  - (S/)MIME
  - EDI und XML Formate
  - Message Disposition Notification (MDN)

AS2 - Voraussetzungen

- Vereinbarung zwischen den beiden Partnern (Peer-to-Peer!) über:
  - URLs (einschließlich Port)
  - AS2-Namen
  - Austausch der Zertifikate

AS2 - Mechanismen

- Das Dokument wird als Daten in einem HTTP POST Request übertragen
- Von der Gegenseite erfolgt ein HTTP Response (mit Status) als Quittung auf Transport-Ebene
- Das Dokument kann
  - Unverschlüsselt oder verschlüsselt sein (HTTPS!)
  - Unsigniert oder signiert sein
  - Verschlüsselung und Signierung beliebig kombinieren
  - Keine MDN, eine unsignierte MDN oder eine signierte MDN anfordern
- Daraus lassen sich 12 Szenarien ableiten, die in RFC 4130 beschrieben sind
- Nur mit der letzten wird das Maximalziel der Non-Repudiation erreicht

AS2 – Mechanismen (Fortsetzung)

- Verwendete MIME-Typen:
  - Dokument selbst – application/EDIxxx oder application/xml oder beliebig
  - Verschlüsselung – application/pkcs7-mime
  - Signatur – multipart/signed, darin application/EDIxxx und application-pkcs7-signature
  - Verschlüsselung umhüllt Signatur
- Komprimierung
  - Nicht in RFC 4130 beschrieben
  - MIME-Typ – application/pkcs7-mime
  - Komprimierung dann Verschlüsselung oder umgekehrt
  - Letzteres sinnvoller

AS2 - MDNs

- MDNs sind Quittungen für gesendete Dokumente
- Sie können unsigniert oder signiert angefordert werden
- Sie können als synchrone oder asynchrone MDNs angefordert werden
- Beide haben die gleiche Struktur
- Synchrone MDNs werden als Daten im HTTP Response der gleichen TCP/IP-Verbindung übertragen
- Asynchrone MDNs kommen als HTTP Request (POST) in einer neuen TCP/IP-Verbindung, die vom Peer aufgebaut wird
- Dieser HTTP Request muß vom ursprünglichen Sender standardmäßig mit einem HTTP Response beantwortet werden

AS2 – MDNs (Fortsetzung)

- Asynchrone MDNs abhängig von der Anforderung versendet über:
  - SMTP
  - HTTP, auch an eine andere URL
  - HTTPS, auch an eine andere URL

AS2 – MDNs (Fortsetzung)

- Synchronous AS2-MDN
  [Peer1] ----(connect)----> [Peer2]
  [Peer1] -----(send)------> [Peer2] [HTTP Request [AS2-Message]]
  [Peer1] <---(receive)----- [Peer2] [HTTP Response [AS2-MDN]]

- Asynchronous AS2-MDN
  [Peer1] ----(connect)----> [Peer2]
  [Peer1] -----(send)------> [Peer2] [HTTP Request [AS2-Message]]
  [Peer1] <---(receive)----- [Peer2] [HTTP Response]
  [Peer1]*<---(connect)----- [Peer2]
  [Peer1] <--- (send)------- [Peer2] [HTTP Request [AS2-MDN]]
  [Peer1] ----(receive)----> [Peer2] [HTTP Response]

  * Note: An AS2-MDN may be directed to a host different from that of the sender of the AS2 message. It may utilize a transfer protocol different from that used to send the original AS2 message.

AS2 – HTTP-Erweiterungen/Modifikationen

- Zusätzliche AS2-spezifische HTTP-Header
  - AS2-Version: 1.0 oder 1.1 (Komprimierung wie in RFC 3274 definiert)
  - AS2-From: <AS2-Name>
  - AS2-To: <AS2-Name>
- AS2-spezifisch interpretierte HTTP-Header
  - Disposition-notification-to: xxx@example.com
    Zur Anforderung einer MDN (Email-Adresse beliebig!)
  - Receipt-delivery-option: http://www.example.com oder https://www.example.com oder mailto:as2@example.com
    Zur Anforderung einer asynchronen MDN mit Zielangabe
  - Disposition-notification-options:
    signed-receipt-protocol=optional,pkcs7-signature;
    signed-receipt-micalg=optional,sha1,md5
    Zur Anforderung einer signierten MDN

AS2 - Produkte

- Open Source
  - OpenAS2 – Java, nicht komplett, hosted auf SourceForge, eingeschlafen (?)
  - Openediint – Java, Status unbekannt, hosted unter ObjectWeb
- Kommerzielle und zertifizierte
  - Zahlreiche, meist zusammen mit EDI-Applikationen
  - U.a., z.T. Mit mehreren Produkten
    - Cleo
    - Compinia – ComAS2
    - Cyclone
    - IBM
    - iSoft
    - iWay
    - Seeburger
    - Sterling Commerce

AS2 - Zertifizierung

- Durchgeführt von der Drummond Group Inc. (DGI) www.drummondgroup.com
- 2 Testrunden jährlich
- 2 Phasen
  - Conformance Test
  - Interoperability Test
- Erfolgreiche Teilnehmer erscheinen auf der Webseite der DGI und müssen ihr Produkt vermarkten
- Die Zertifizierung bezieht sich nur auf eine bestimmte Produktversion
- Nicht ganz billig ($13.500 bzw. $10.000)

AS2 – Das Ende

Danke!

Ihre Fragen bitte.