Standard e-Rechnungs-Webservice (SERWS) - Ideen

DI Philip Helger, BRZ

17.02.2015

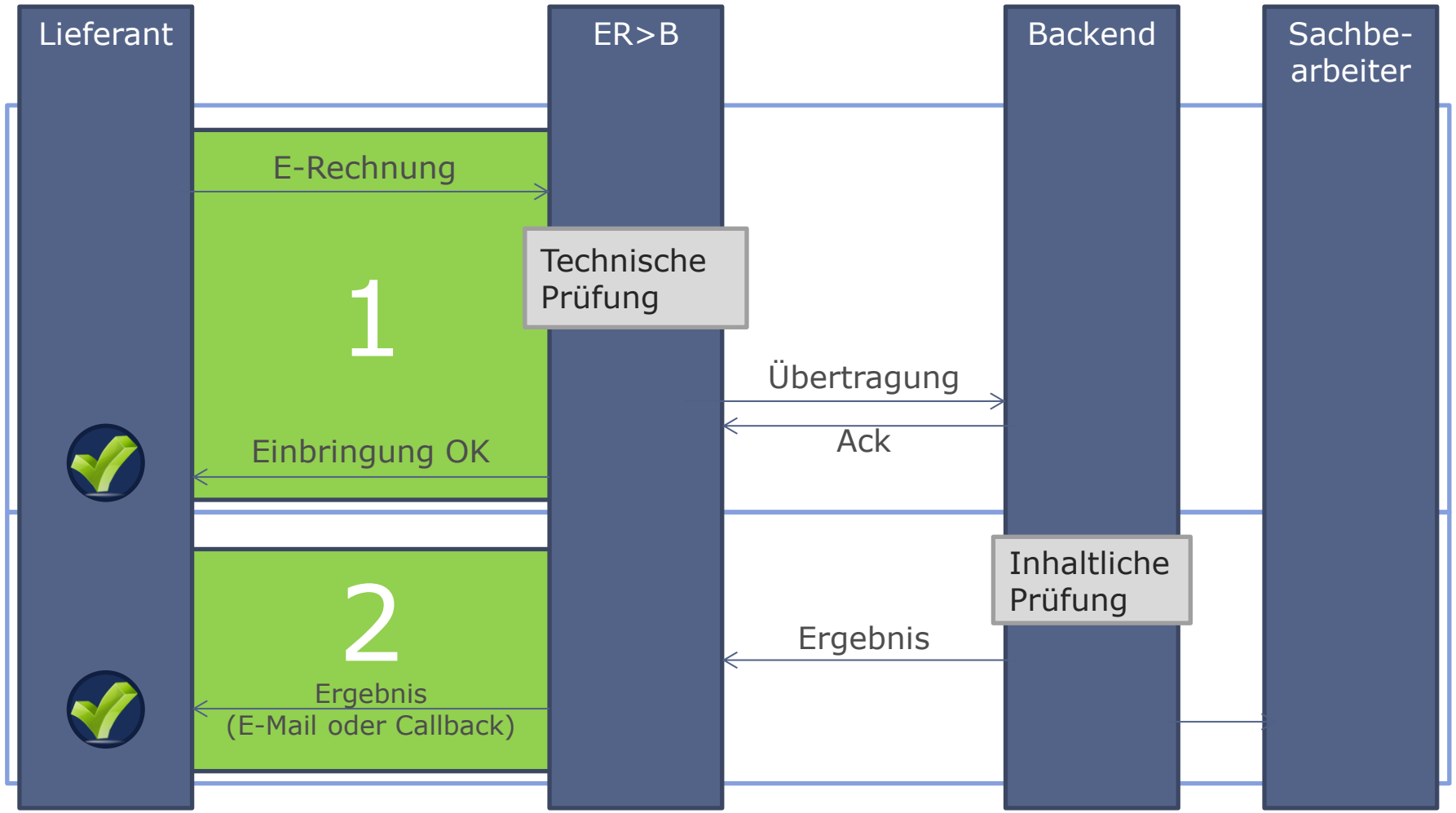
AGENDA

- Ausgangsbasis
  - Webservice bei E-RECHNUNG.GV.AT
- SERWS Ziele
  - Einheitliche Webservice-Schnittstelle für e-Rechnungs-Empfänger
  - Sicherheitsaspekte

ER>B WEB SERVICE

- Entgegennahme von e-Rechnungen in allen unterstützten Formaten (ebInterface und UBL)
- Einstellungsmöglichkeiten für die asynchrone Retourkommunikation definieren
- Einfache Testbarkeit
- Derzeit zwei Versionen im Einsatz

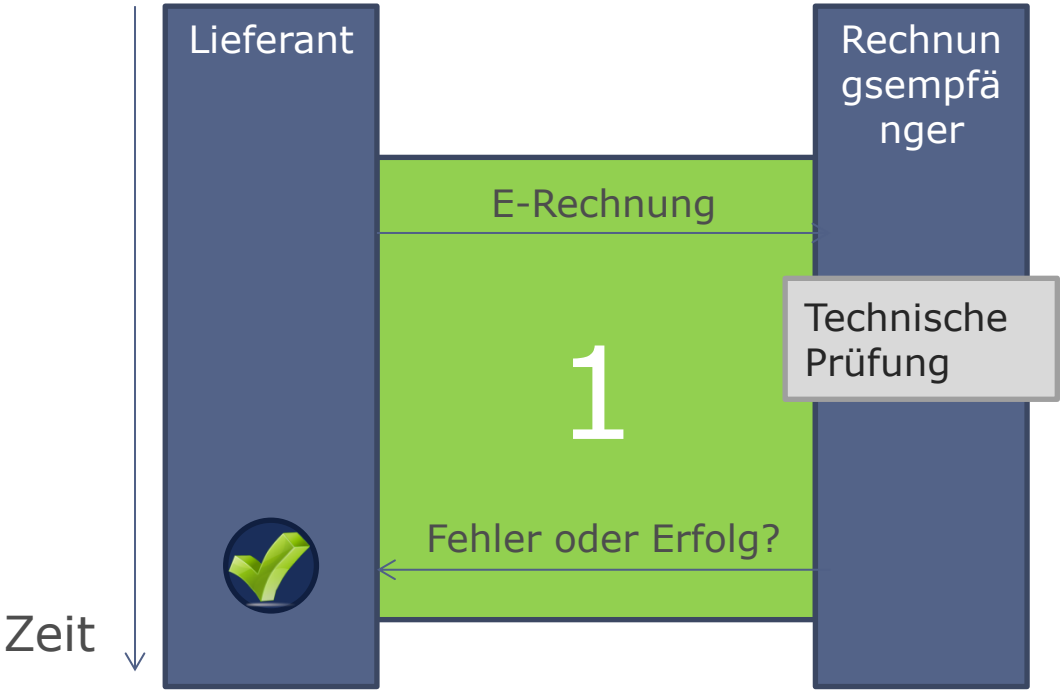
ER>B EINBRINGUNGSPROZESS (ASYNCHRON)



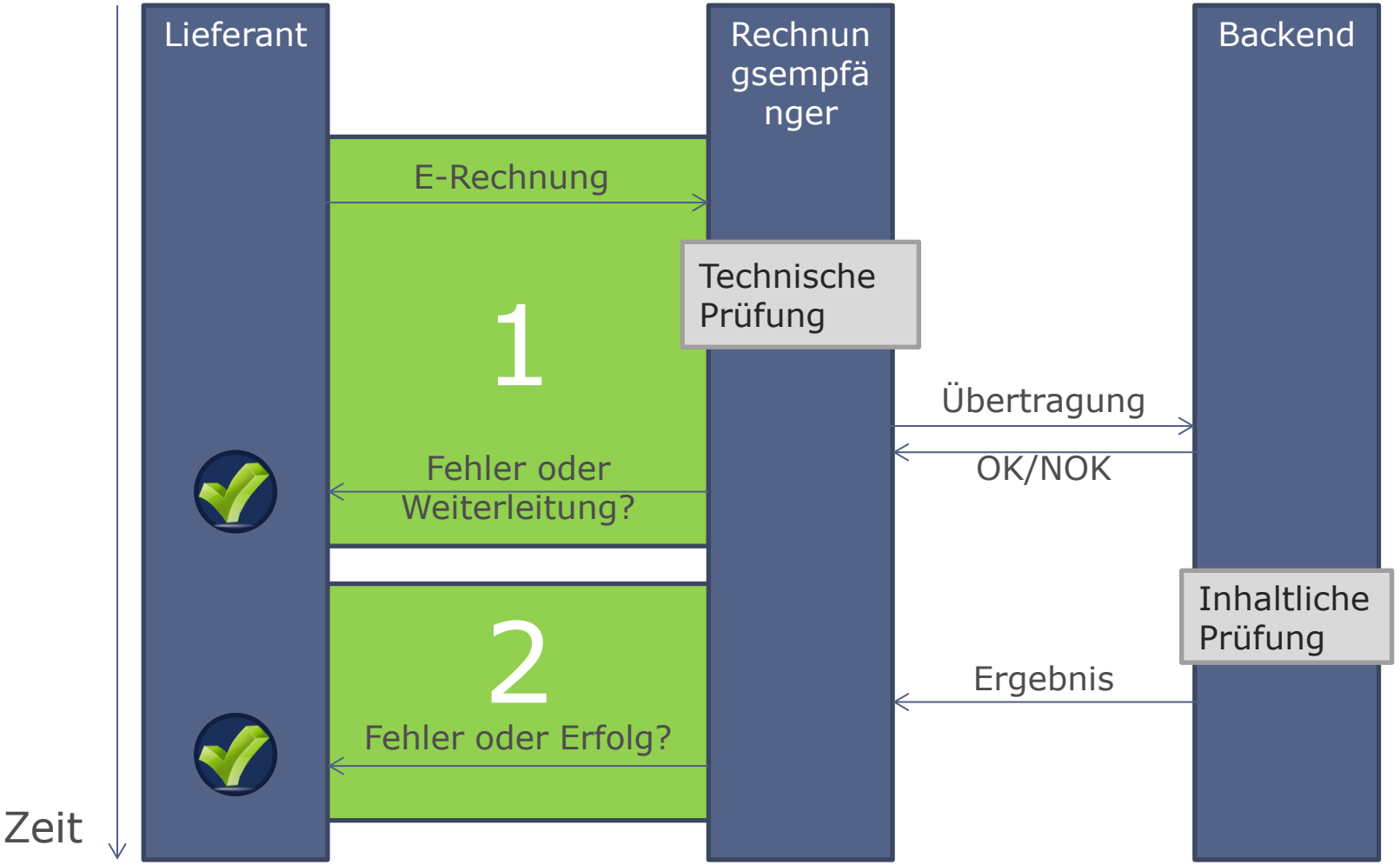
SERWS ZIELE

- Definition einer einheitlichen Webservice-Schnittstelle für e-Rechnungs-Empfänger
- Anforderungen
  - Beliebige strukturierte e-Rechnungen sollen übertragen werden können
  - Neben der e-Rechnung sollen auch Beilagen übermittelt werden können
  - Auch Adressierungsdaten sollen enthalten sein können („Header-Daten“)
  - Die Konfiguration des Aufrufs soll im Aufruf selbst enthalten sein
  - Es soll sowohl eine synchrone Verarbeitung als auch eine asynchrone Verarbeitung möglich sein
- Nicht berücksichtigt
  - Externe (zum Download bereitgestellte) Beilagen

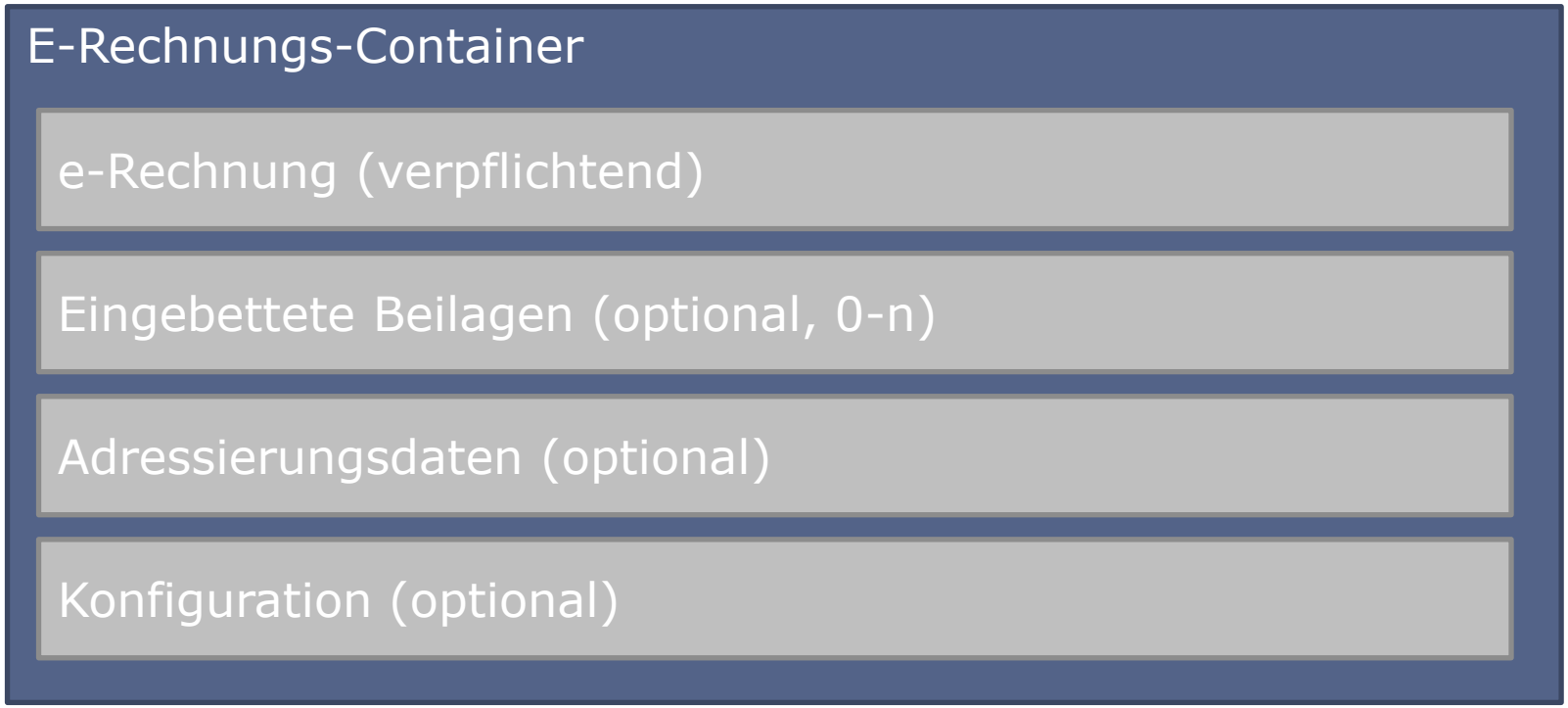
SYNCHRONE EINLIEFERUNG



ASYNCHRONE EINLIEFERUNG



ÜBERMITTELBARE DATEN



INHALT: E-RECHNUNG

- Ausschließlich strukturierte Formate?
- Nicht nur XML (z.B. EDIFACT)?
  - Am einfachsten durch Base64-Kodierung gelöst
- Immer wieder ein Hindernis: unterschiedliche Charsets zwischen Envelope und e-Rechnung
- Z.B. UBL enthält Beilagen im Dokument
- Sollen die unterstützten Formate limitiert werden oder soll z.B. auch PDF übertragen werden können?

INHALT: BEILAGEN

- Anzahl limitieren? Bund: 200
- Größe limitieren? Bund: 15 MB
- Dateitypen (MIME Types) limitieren? Bund: PDF, PNG, XML, XLS, XLSX
- Vorschlag: Base64-Codierung
- Dateiname empfehlenswert
- Inhaltsprüfung ob Dateityp gültig ist
- Virenscanner!

INHALT: ADRESSIERUNGSDATEN

- Eindeutige MessageID
  - Im Falle eines Re-Sends muss dieselbe Message ID verwendet werden
- Sender ID?
- Empfänger ID ?
- Evtl. 0-n „Intermediary IDs“? (für Service Provider)
- Evtl. Dokumententyp? (siehe @DocumentType)
- Zugangsdaten/Client Zertifikate?

INHALT: KONFIGURATION

- Technische Kontaktperson
- Flag ob Test- oder Produktiv-Übertragung?
- Zu verwendende Sprache (deutsch, englisch etc.)
- Asynchrone Variante
  - Einstellungen für die Rückkommunikation
  - Benutzerdefinierte Felder um die asynchrone Antwort mit der ursprünglichen Anfrage zu matchen

PROZESS: SYNCHRON VS. ASYNCHRON

- Synchron
  - Die Antwort der Einlieferung ist „Erfolg“ oder „Fehler“
  - Es muss ein Zeitlimit für das Warten auf die Antwort definiert werden
- Asynchron
  - Als Antwort der Einlieferung kann nur „Fehler“ oder „Weiterverarbeitung“ gesendet werden
  - Die Schnittstelle für die Kommunikation von Rechnungsempfänger zurück zum Rechnungssteller muss definiert werden („Callback“)
  - Erst der Status im „Callback“ ist final „Erfolg“ oder „Fehler“

ALLGEMEINE ANFORDERUNGEN

- Im Fehlerfall sollten dem Kontext entsprechende Fehlermeldungen ausgegeben werden
- Die Unterstützung von mindestens UTF-8 sollte Pflicht sein
- Ein Test-Endpunkt sollte von der AustriaPRO zur Verfügung gestellt werden
- Eine Liste von allen Empfängern die diese Schnittstelle verwenden, könnte zur Verfügung gestellt werden
- Die Prozessdetails (Timeout, Re-Send, synchron vs. asynchron) müssen noch definiert werden.

SECURITY ALLGEMEIN

- CIA Triade
  - Confidentiality – Vertraulichkeit
    - Daten dürfen lediglich von autorisierten Benutzern gelesen bzw. modifiziert werden, dies gilt sowohl beim Zugriff auf gespeicherte Daten, wie auch während der Datenübertragung
  - Integrity – Integrität
    - Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein
  - Availability – Verfügbarkeit
    - Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein
- Nichtabstreitbarkeit der Übermittlung (Non-repudiation)
- Sicherheit bei der Implementierung

SECURITY - VERTRAULICHKEIT

- Verschlüsselung auf Transportebene
  - TLS (SSL keine Option mehr)
  - Nachteil: keine End-to-end Security bei mehreren Knoten (z.B. Service Provider)
- Verschlüsselung auf Dokumentenebene
  - Entweder direkt im WS oder als eigenes Dokumentenformat
    - Im WS: WS muss alle Parameter kennen
    - Als Format: WS kann weiterhin inhaltsagnostisch sein

SECURITY - INTEGRITÄT

- Verwendung von elektronischen Signaturen
  - Sender signiert mit seinem Private Key
  - Empfänger überprüft mit Public Key des Senders

SECURITY - VERFÜGBARKEIT

- System für maximalen Durchsatz optimieren, um DoS-Attacken vorzubeugen
- Schutzmaßnahmen gegen bekannte Angriffe setzen
  - Rekursive Inhalte
  - Übergroße Daten
  - XML Entity Expansion

SECURITY - NICHTABSTREITBARKEIT

- Der Empfänger darf nicht abstreiten können, dass er die Rechnung vom Sender bekommen hat
- Nur kryptografische Nichtabstreitbarkeit und nicht juristische
- Umsetzung
  - Z.B. über gesicherte Logfiles
  - Über elektronische Signaturen

SECURITY - IMPLEMENTIERUNG

- Qualitätssicherung der Umsetzung (Penetration Test)
- OWASP Liste berücksichtigen
- Bei Verwendung von Zertifikaten müssen diese überprüft werden

OWASP WS SECURITY CHEAT SHEET

- Transport Confidentiality (TLS Verschlüsselung)
- Server Authentication (TLS)
- User Authentication (Username/Password oder Client-Zertifikat)
- Transport Encoding (SOAP)
- Message Integrity (Signaturen)
- Message Confidentiality (Verschlüsselung)
- Authorization (jeden Client)
- Schema Validation
- Content Validation
- Output Encoding (bei Weiterverarbeitung)
- Virus Protection
- Message Size (Größen Limit)
- Availability (Durchsatz, XML DoS protection)
- Endpoint Security Profile (WS-I Basic)

UMSETZUNGSGEDANKEN

- Standard soll für KMUs umsetzbar sein
- Sollen andere Protokolle als SOAP/HTTP unterstützt werden?
- Soll eine Zertifikatsinfrastruktur aufgebaut werden?
- Wie können die Sicherheitsanforderungen umgesetzt werden, ohne dass der Aufwand ins Unermessliche steigt?
- Soll nur die Schnittstelle definiert werden, aber jeder Umsetzer muss sich selbst um die Sicherheit kümmern?
- Bei erhöhter Komplexität sollte die OpenPEPPOL-Schnittstelle evaluiert werden, da diese bereits alles hat. Es könnte ein Parallel-PEPPOL in Betrieb genommen werden…

Vielen Dank für Ihre Aufmerksamkeit

philip.helger@brz.gv.at