



Software Design und Beratung G.m.b.H.

ARA Online-Meldung

*Integration und Praxiseinsatz der
sicheren digitalen Signatur*

ARA OM – Ausgangslage

Altstoff Recycling Austria (ARA)...

- ist Österreichs Verpackungssammel- & Verwertungssystem
- sammelt und verwertet 650.000 Tonnen Verpackungen aus Papier, Karton, Kunststoff, Glas, Metall, Verbund, Holz pro Jahr
- besteht seit 1993 und hat derzeit 13.100 Lizenznehmer
- bietet dem Lizenznehmer die Entpflichtung, der in Verkehr gesetzten Verpackungen

Voraussetzung ist die fristgerechte monatliche/quartalsweise Meldung der in Umlauf gebrachten Packstoffmengen.



ARA Meldung

ARA OM – Anforderungen & Ziele

- Webbasierte Erfassung von ARA Meldungen (ARA Online Meldung)
- Gewährleistung einer firmenmäßigen Zeichnung
- Unterstützung von Mehrfachsignaturen
- Basis Workflow-Unterstützung beim Lizenznehmer
- Basis Workflow-Unterstützung für ARA
- Rollenkonzept (Admin, Signator, Autor, Leser)
- Geringer Administrationsaufwand für ARA
- Meldungen jederzeit einsehbar
- Dezimieren des Versandaufwandes
- Dezimieren von Papier-Meldungen

ARA OM – Konzepte

- Zweistufiges Administrationssystem
- Intelligente Formulare
- eMail-Benachrichtigung mit Formular-Link
- OpenSource Betriebsplattform
- Kundenspezifisches Marketing
- Importschnittstelle für ARA-Editor
- Sichere (Mehrfach-) Signatur

ARA OM – Sichere Signatur

Komponenten für Digitale Signatur (BDC)

- Clientseitig: **hot:Sign**

Signaturumgebung und Secure Viewer für eine dem Signaturgesetz konforme sichere Signatur

Plattform: Win98, WinME, WinNT4.0, Win2K, WinXP

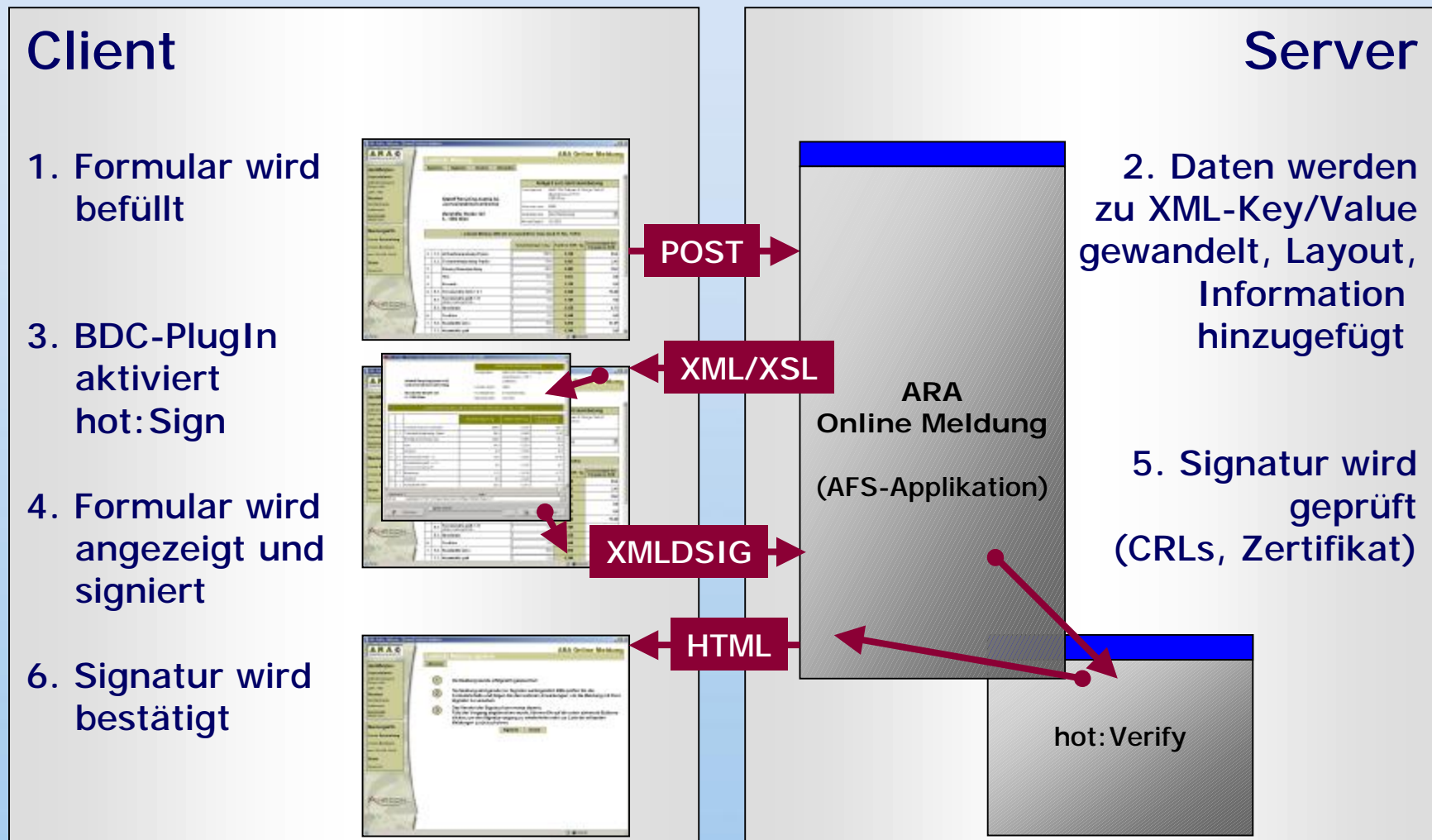
- Serverseitig: **hot:Verify**

Handling von CRLs

Verifizierung von Signaturen

Plattform: Linux, Solaris, weitere a. A.

ARA OM – Ablauf Sichere Signatur



ARA OM – Projekt & Status

- Projektpartner: ANECON G.m.b.H.,
ARA, A-Trust, BDC GmbH,
Bull AG, WKÖ
- Projektdauer: ~50 Personentage
- Online Meldung ab Mai 2003 im Echtbetrieb
(davor ½ Jahr erfolgreich im Probebetrieb)
- Derzeit 30 Pilotkunden
z.B. Coca-Cola, Inzersdorfer, Sony, ...
- Feedback von Anwendern sehr positiv
„Anwendung ist sehr einfach und benutzerfreundlich“

ARA OM – Masken

The image displays three overlapping screenshots of the ARA Online Meldung web application interface, showing the login process, user selection, and a waste report table.

Screenshot 1: Login Page

ARA Online Meldung - Microsoft Internet Explorer

ARA Online Meldung

Willkommen zur ARA Online Meldung

Schließen

Benutzername:
 Passwort:

Anmelden

Viel Spaß mit unserer Applikation!

TRUST

ANECON

Screenshot 2: User Selection Page

ARA Online Meldung - Microsoft Internet Explorer

ARA Online Meldung

Auswahlmenü

Benutzer

Identifikation

Lizenznehmer
ANECON Software 3
Design Center
LIZN - 1449

Benutzer
Name: Schmidt
E-Mail-Adresse: jacob.schmidt@anecon.com

Laufende Meldungen für Periode: [C: 2002]
 zirkuläre Meldung auslösen
 Letzte Laufende Meldungen
 Benutzerdaten
 System

Screenshot 3: Waste Report Page

ARA Online Meldung - Microsoft Internet Explorer

ARA Online Meldung

Laufende Meldung

Speichern Abbrechen

Identifikation

Lizenznehmer
ANECON Software 3
Design Center
LIZN - 1449

Benutzer
Name: Schmidt
E-Mail-Adresse: jacob.schmidt@anecon.com

Meldungsinformation

Letzte Beschreibung
von Miriam Behrend
am 14.05.2002 - 10:50

Status
neu

Anlage 9 zur Lizenzvereinbarung

Lizenznehmer: ARA/UN Software 3 Design Center
Abteilung: 4, 1 x 1
100 Wien

Lizenznummer: 4508

Kontaktperson: Miriam Behrend
E-Mail-Adresse: mir@anecon.com

Laufende Meldung 2002 gilt als Gültig im Sinne des § 11 Abs. 7 BSRG

	Gesamtmenge in kg	Tarife in EUR / kg	Lizenzgebühren über Periode in EUR
1. 1.1. Verkehrverpackung Papier	0,00	0,150	0,00
1.2. Transportverpackung Papier	0,00	0,263	0,00
2. Einweg-Glasverpackung	0,00	0,285	0,00
3. Holz	0,00	0,223	0,00
4. Keramik	0,00	0,290	0,00
5. 5.1. Unmetallische Stein > 3 l	0,00	0,260	0,00
5.2. Unmetallische groß > 3 l Metallgegenstände	0,00	0,180	0,00
5.3. Aluminium	0,00	0,133	0,00
6. Textilien	0,00	0,460	0,00

ARA OM – Projektbeschreibung

Integration und Praxiseinsatz der sicheren digitalen Signatur

Projekterfahrungen im B2B am Beispiel ARA-Online Meldung ein Projekt von ARA, Wirtschaftskammer Österreich (WKÖ), A-Trust und ANECON mit Einsatz von Bürgerkarte und Security Layer

1 Einleitung

Die vorliegende Vortragszusammenfassung beschäftigt sich mit Projekterfahrungen in bezug auf den Einsatz der sicheren digitalen Signatur in einem der ersten B2B-Projekte mit dieser Technologie: ARA-Online Meldung.

Schwerpunkte bilden dabei Zielsetzung, Architektur und Signaturhandling dieser B2B-Applikation, die Unterschiede und Gemeinsamkeiten von B2B- und eGovernment-Applikationen in bezug auf die digitale Signatur und der Einsatz von Bürgerkarte und Security Layer.

2 Projekt ARA „Online Meldung“

Beim Projekt „ARA Online Meldung“ handelt es sich um ein B2B-Projekt das die Durchführung von Altstoffmeldungen durch die ARA-Lizenznehmer über eine Web-Applikation ermöglicht. Umsetzungs-Partner bei diesem Projekt waren: ARA, Wirtschaftskammer Österreich (WKÖ), A-Trust, BDC und als Entwicklungspartner ANECON.

2.1 Basisfunktionalitäten der Online-Meldung

Basisfunktionalitäten der Applikation sind:

- Ausfüllen, Speichern, Löschen, Signieren der Meldungen
- Integration der sicheren digitalen Signatur (clientseitig, serverseitig)
- Rollenbasierte Benutzerverwaltung und ein einfacher Registrierungsprozess
- Automatisches Berechnen
- Automatisches Vorbefüllen relevanter Felder (Firmenbezeichnung, aktuelle Abgabeperiode auf Basis einer je nach Kunde monatsweisen oder quartalsweisen Abgabe)

2.2 Weitere wichtige Aspekte

Autoren- und Signatoren-Rollen werden für eine einfache Workflow-Unterstützung verwendet, sodass alle Signatoren eines Kunden beim Speichern einer Meldung per Mail von der zu signierenden Meldungen verständigt werden (inklusive Link zur betreffenden Meldung).

Security Aspekte beinhalten die schon erwähnte Sichere Signatur (A-Trust trust|sign, BDC hot:Sign), eine über MD5 gehashte Passwortablage und einen über SSL 128-bit gesicherten Online Zugriff.

2.3 Architektur

Die Architektur der Applikation besteht aus den folgenden Komponenten.

Auf den Client-PCs wird als Web-Browser Internet Explorer ab Version 5.x oder Netscape ab Version 4.x eingesetzt. Als Signatur-Client kommt BDC hot:Sign (durch A-SIT bescheinigt) zum Einsatz und als bescheinigtes Kartenlesegerät KOBIL KAAAN PROF.

Die für die Applikation in einer DMZ benötigten Server sind ein Webserver (Apache), ein Applikationsserver (Tomcat) und ein PKI Server (BDC hot:Verify). Zusätzlich wird der Host im ARA-LAN angebunden und der LDAP-Verzeichnisdienst der A-Trust vom PKI Server zur Verifikation von Signaturen herangezogen.

2.4 AneconFormSolution-Framework (AFS)

AFS ist ein Formularframework zur schnellen und effizienten Entwicklung von Internetapplikationen und damit die Essenz der ANECON-Erfahrungen aus umfangreichen und komplexen Internet-Applikationen. Dieses Framework übernimmt folgende Funktionalitäten in der ARA Online Meldung:

- Formulardesign/ -beschreibungen (JSP/XML) sowie Formularhandling
- Benutzerverwaltung: der Kunde erhält eine Administrator-Kennung und verwaltet seine User selbst
- Felder: Formatierungen, Validierungen, Berechnungen

Ein AFS Formulare System wie die beschriebene Anwendung ARA-Online-Meldung kann, mit Ausnahme der Signaturkomponenten, vollständig auf Open-Source Produkten (Linux, Apache, Tomcat, MySQL) betrieben werden.

2.5 Digitale Signatur

Die sichere Signatur benötigt ein sicheres Signaturverfahren, im ARA-Projekt wurde dies wie folgt umgesetzt:

Sicheres Viewing und Hashing

Auf dem Client kommt eine Signaturumgebung bzw. ein bescheinigter Secure Viewer von BDC zum Einsatz (hot:Sign 1.0) und ermöglicht eine dem Signaturgesetz konforme sichere Signatur (XMLDSIG)

Sichere Pin-Eingabe

Ebenfalls auf dem Client wird ein bescheinigter Kartenleser eingesetzt: KOBIL KAAAN PROF

Serverseitige Verifikation

Für die Verifikation von Signaturen und das Handling von widerrufenen Zertifikaten über CRLs wird der PKI Server hot:Verify (BDC) verwendet.

3 Signatur im e-Government

3.1 Erstellung und Verifikation der Signatur

Der Hauptunterschied zu B2B-Applikationen besteht darin, dass e-Government Anwendungen über den sogenannten *Security Layer* auf die *Bürgerkarte* zugreifen.

Die Verifikation der Signaturen verläuft im e-Government Fall im Prinzip genau wie bei B2B-Anwendungen; auch werden dabei keine bescheinigte Komponenten benötigt wie das beim Secure Viewing, Secure Hashing oder Sichere Pineingabe der Fall ist. Es gibt Produkte auf dem Markt die in bestehende und/oder neue Applikationen integriert werden können, z.B. IT Solution „ExpressConfirmation“, BDC „hot:Verify“

3.2 Bürgerkarte und Security Layer

Bei der Bürgerkarte handelt es sich um ein Konzept, um eine Schlüsseltechnologie für eGovernment. Ausprägungen der Bürgerkarte beinhalten die sichere elektronische Signatur, Identifikation, Authentifizierung durch Personenbindung, einen Security Layer. Verschiedene Token wurden angekündigt (e-card, Personalausweis, Studentenkarten, Bankkarten...), erstmals verfügbar ist die Bürgerkarte als trust|sign-Produkt von A-Trust.

Der Security Layer bildet die Schnittstelle zwischen Applikation und Bürgerkarte auf dem Client; die aktuelle Version ist 1.1.0 vom 31.8.2002. Hersteller von Standard Signatur-Komponenten sind in den Definitions-Prozess involviert. Existierende Security Layer Implementierungen sind bereits nahe am aktuellen Security Layer-Standard.

Fazit

Eine erste Bürgerkarten-Ausprägung, bescheinigte Kartenleser sowie geeignete Serversoftware für die Verifikation von Signaturen sind vorhanden, aktuelle Clients werden kurzfristig Security Layer-konform verfügbar sein.

Alles in allem besteht kein großer Unterschied in bezug auf die Integration der digitalen Signatur in B2B- bzw. in eGovernment-Projekten.