Web Service based Transformation of Digital Signature Formats

Bernd Zwattendorfer

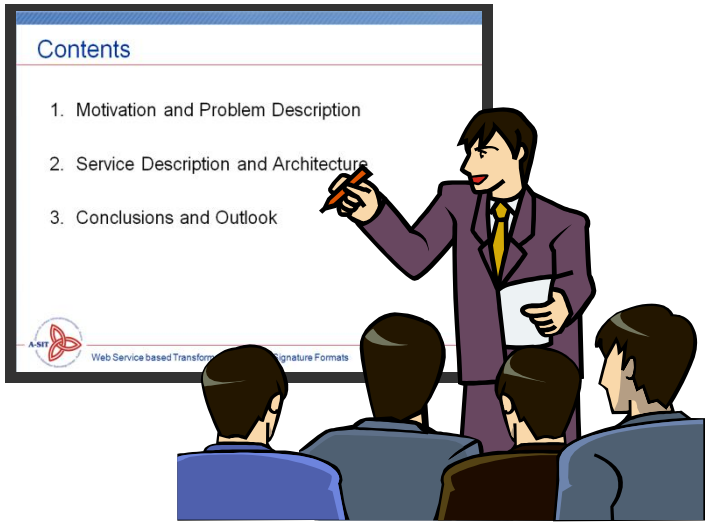
A-SIT

bernd.zwattendorfer@a-sit.at

www.a-sit.at

Contents

1. Motivation and Problem Description
2. Service Description and Architecture
3. Conclusions and Outlook



Motivation

- Moving to another country

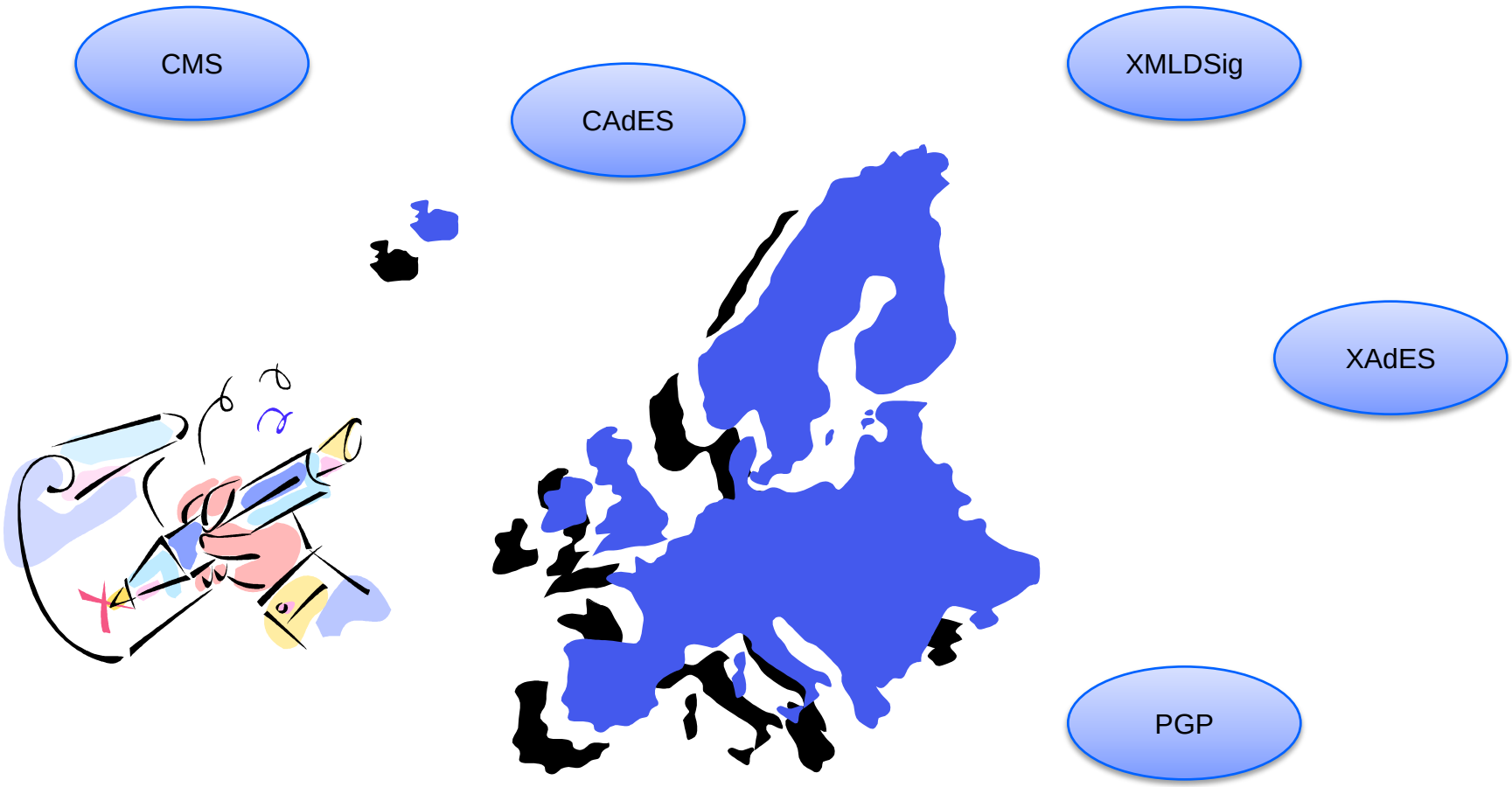
Poland

E-Government

Moving House Life Event

Ireland

Different Signature Formats



Different Signed Documents

BMI SU-ZMR
Hahngasse 8
1090 Wien

zmr zentrales melderegister

MELDEBESTÄTIGUNG
aus dem Zentralen Melderegister

PERSONENDATEN

Titel:	DI
Familienname:	Zwattendorfer
Vorname:	Bernd
Geschlecht:	Männlich
Geburtsdatum:	05.07.1980
Geburtsort:	Graz
Staatsangehörigkeit:	Österreich

Im Zentralen Melderegister scheinen folgende Meldedaten auf:

Wohnsitzqualität:	Hauptwohnsitz
Strasse:	Musterstraße 1
PLZ/Ort:	8051 Graz,04.Bez.:Lend
Ortsgemeinde:	Graz
gemeldet seit:	07.03.2007

BM.I	Signiert von	BMI SU-ZMR
	Datum	2007-04-13T21:10:06
	Zertifikat	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH, a-sign-corporate-light-02, AT (80524)
	Verfahren	urn:publicid:bmi.gv.at:ZP+bescheid+mb-1.2
Signaturwert		sqoaBfbBFz9UTDNZmjVg3slktXHm26teMse17UqSqdnFCfAhecpPhxXt9tmyszqv3 b2ryIOF4XPqO77K99wA3pDlS++xVarOBz8n5k14gM9QHBPx1FhoGVqf4d2R3BdEm vKU1exTNcyNASZRftjm/S1OG2p91s+hE+zgiumV6KXQ=

Weitere Hinweise zu dieser elektronischen Meldebestätigung finden Sie unte
/egovMB/info/mb_info.html,
Informationen zur Signatur unter https://meldung.cio.gv.at/egovM

Tagesdatum: 13.04.2007
Uhrzeit: 23:10:03

XML

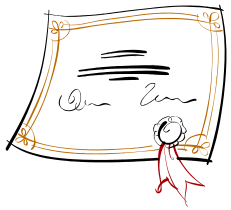
Blindtext

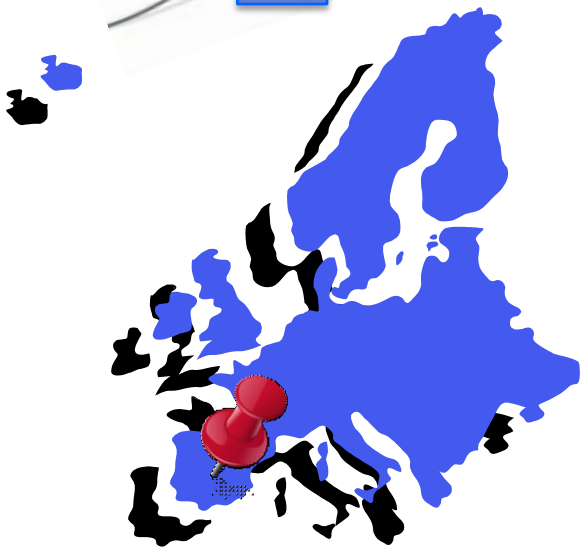
Streng dem definierten Wesen des Blindtextes folgend, fungiere ich als solcher und gebe mich unverbindlich inhaltsleer. In bedrückender Enge in vorgefertigte Masken gepresst friste ich ein freudloses Dasein auf dem schmalen Grat zwischen Nichtbeachtung und Bedeutungslosigkeit und habe doch eine Bitte: Handeln Sie Sinn stiftend für meine Existenz und lesen Sie mich.

Dokument unterschrieben
von: DI Thomas Knall
am: 31.03.2009 11:53

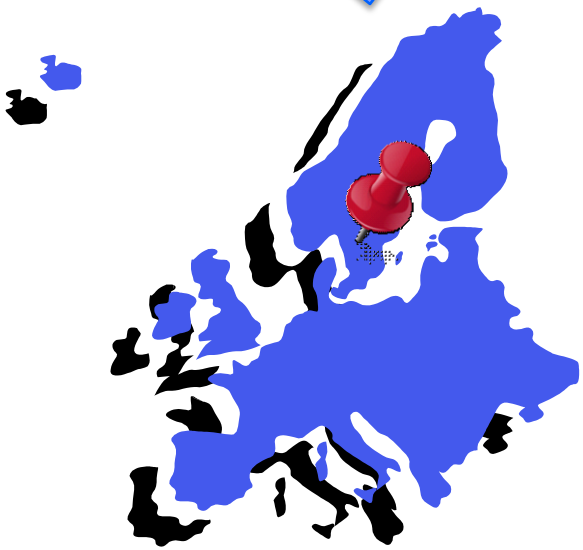
CMS

Cross-Border Document Exchange





Signature Transformation Service

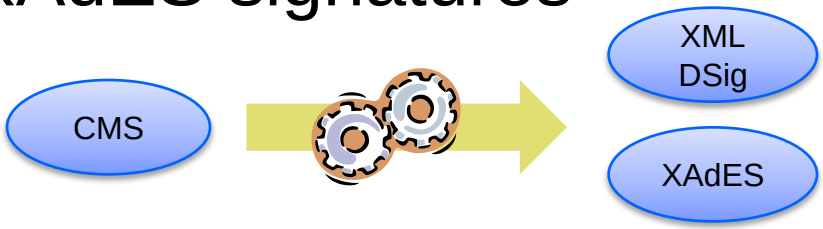


Same signature format?

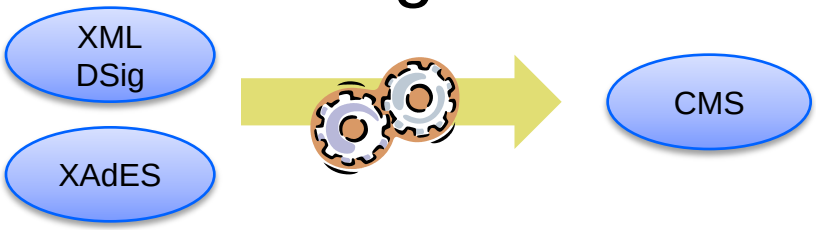
Signature remains valid?

Transformations

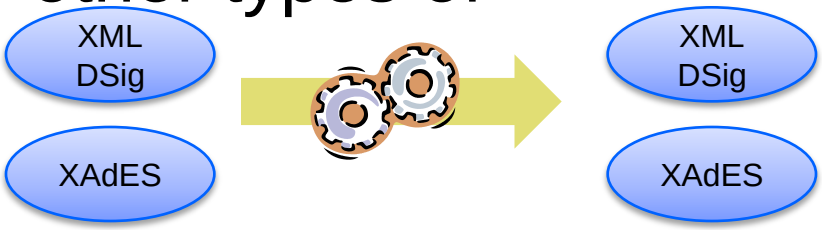
- CMS signatures to XML/XAdES signatures



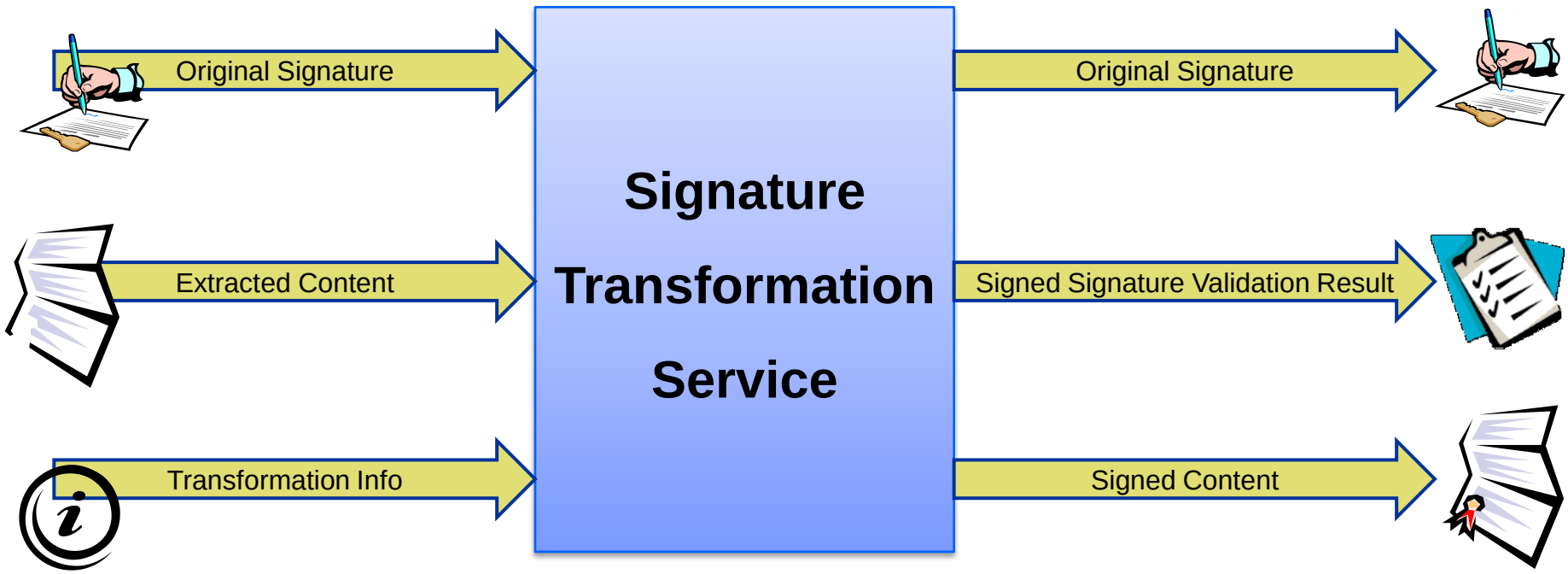
- XML/XAdES signatures to CMS signatures



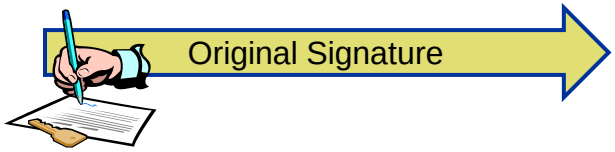
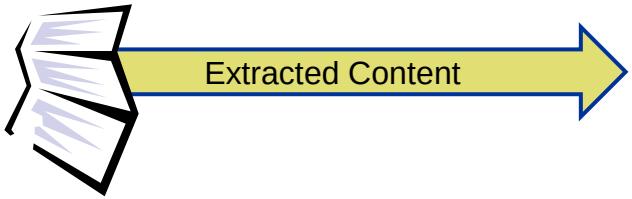
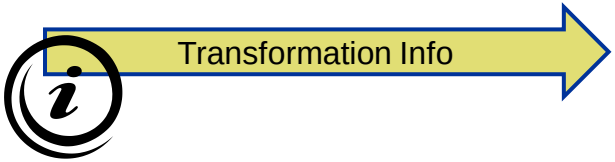
- XML/XAdES signatures to other types of XML/XAdES signatures



Signature Transformation Service



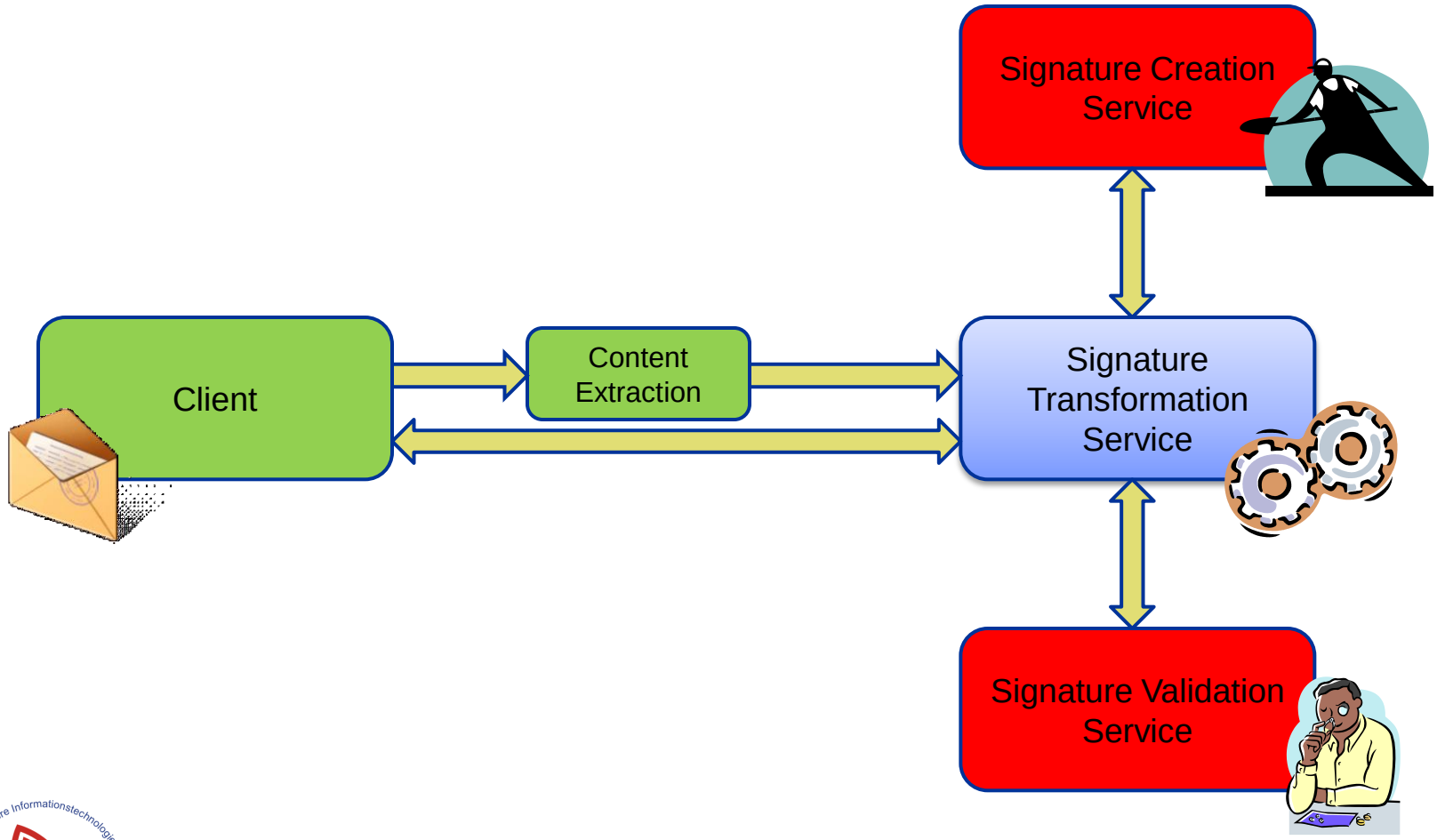
Signature Transformation Service

	• CMS-based signatures • XML-based signatures
	• XML encoded • Base64 encoded
	• ID for selection of trustable root certificates • Type of signature to create • ID for signature key

Signature Transformation Service

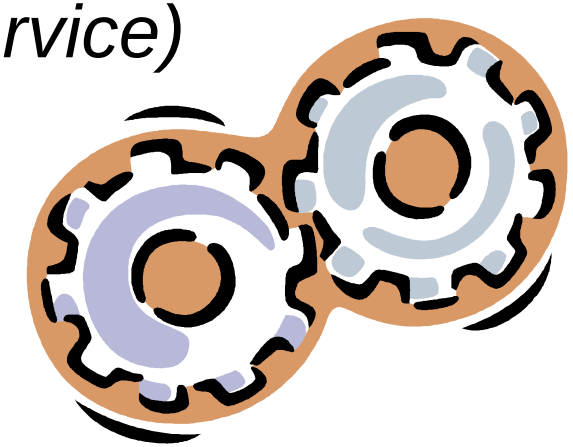
Original Signature 	• CMS-based signatures • XML-based signatures
Signed Signature Validation Result 	• CMS-based signatures • XML-based signatures • Error response
Signed Content 	• CMS-based signatures • XML-based signatures • Error response

Architecture



Transformation Process

1. Validation of the original signature *(Signature Validation Service)*
2. Creation of a signature over the verification result *(Signature Creation Service)*
3. Creation of a new signature over the extracted content *(Signature Creation Service)*



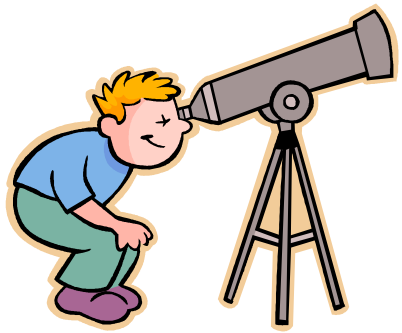
Signature Creation and Validation Service

- Based on Austrian open-source module MOA-SPSS
- SOAP/WSDL Web Service
- Supports CMS verification and XMLDSig signature creation/verification
- Extended to XAdES signature capabilities and CMS creation

Signature Verification	***Signature Creation***
• XMLDSig signatures • XAdES-BES signatures • XAdES-T signatures • XAdES-C signatures • XAdES-X signatures • CMS signatures	• XMLDSig signatures • XAdES-BES signatures • XAdES-T signatures • CMS signatures

Conclusions and Outlook

- Tested with official Austrian proof of residence (XML based)
- Operation by e-Notary Service
- OASIS - eNotarization Markup Language (ENML)



Thank You
for your attention!

Bernd Zwattendorfer

A-SIT
bernd.zwattendorfer@a-sit.at
www.a-sit.at