

# Web Service based Transformation of Digital Signature Formats

Bernd Zwattendorfer

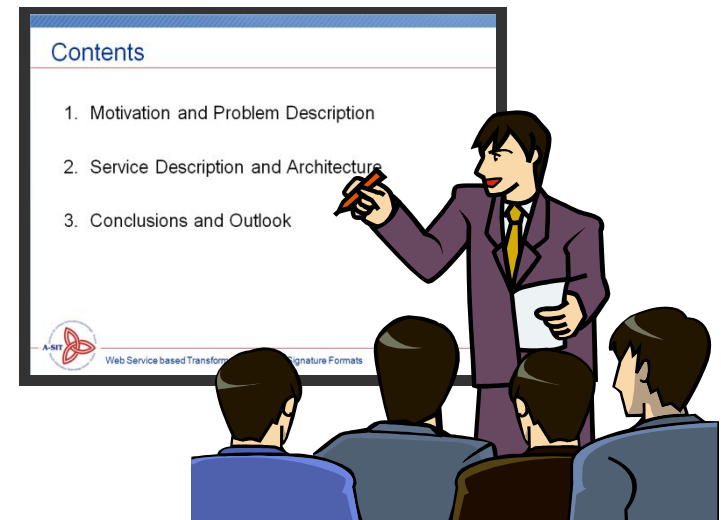
A-SIT

[bernd.zwattendorfer@a-sit.at](mailto:bernd.zwattendorfer@a-sit.at)

[www.a-sit.at](http://www.a-sit.at)

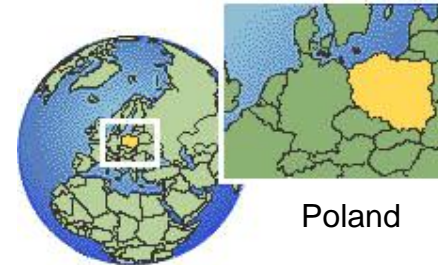
# Contents

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

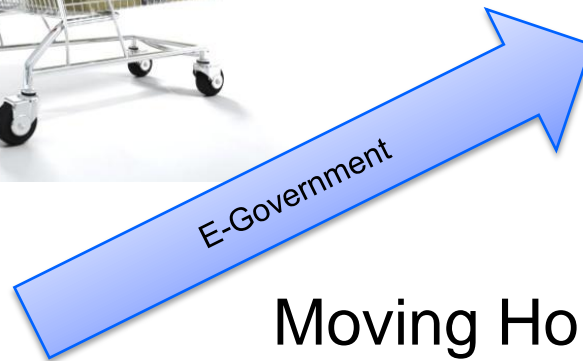


# Motivation

- Moving to another country



Poland

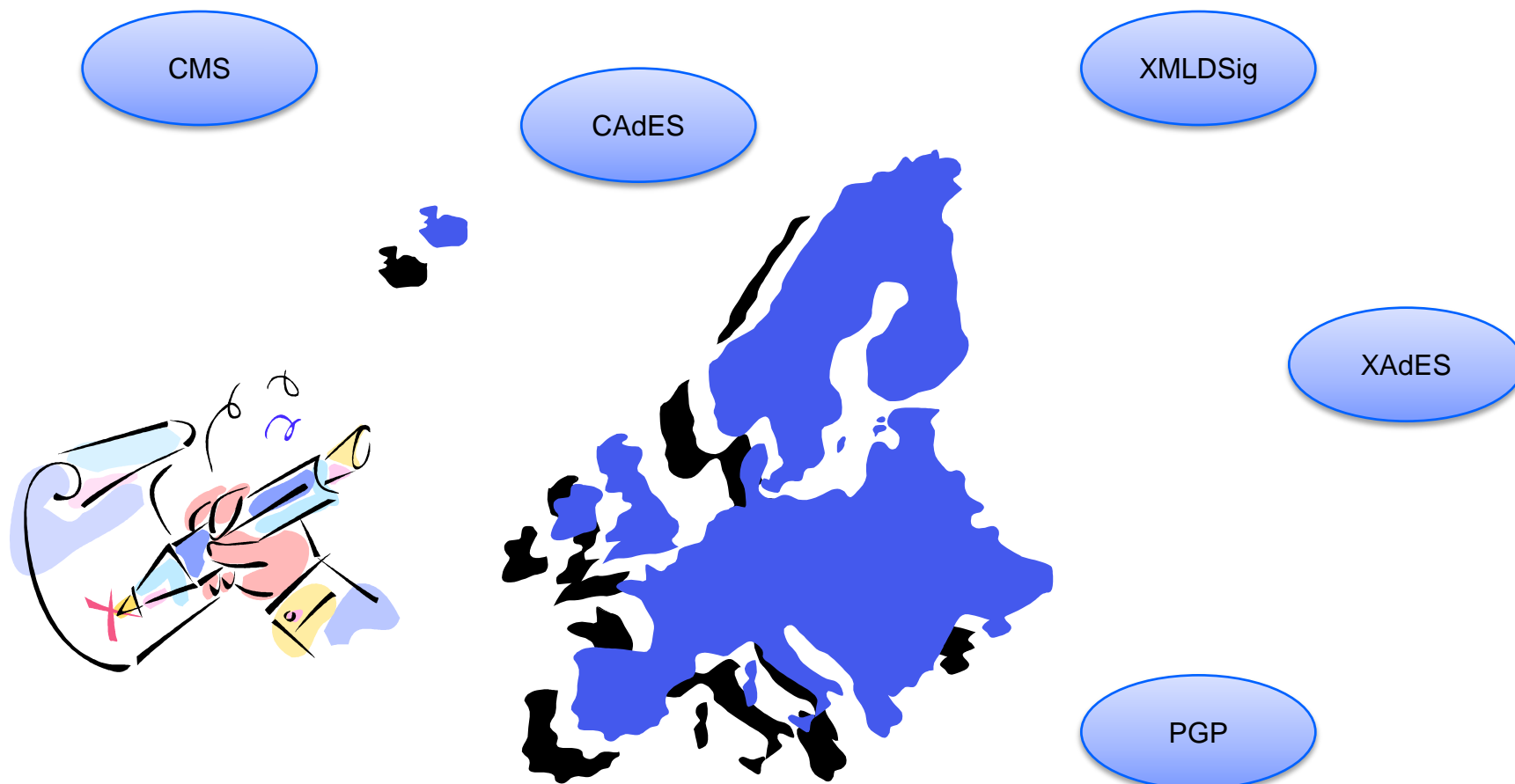


Moving House Life Event



Ireland

# Different Signature Formats



# Different Signed Documents

BMI SU-ZMR  
Hahngasse 8  
1090 Wien

**zmf**  
zentrales melderegister

**MELDEBESTÄTIGUNG**  
aus dem Zentralen Melderegister

**PERSONENDATEN**

Titel: DI  
 Familienname: Zwettendorfer  
 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

	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	eqoa8tb8Fz90TDMZm3Vg3s1ktX3ba26eMee170qSgdnFC2AhecpPhxXt9tmyzqv3 bzry10F4XpQ077K99wA3pd15+xxVar0Bz8nSkt4gM9QRBpx1FhoGVqf4d2R3Bd8m vR0LexTNoYwAS2REtjyW51002p91s+hE+eg1um/6KXQ=	

Weitere Hinweise zu dieser elektronischen Meldebestätigung finden Sie unter [/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 inhaltloser, 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 Krogg  
 am: 31.03.2009 11:53

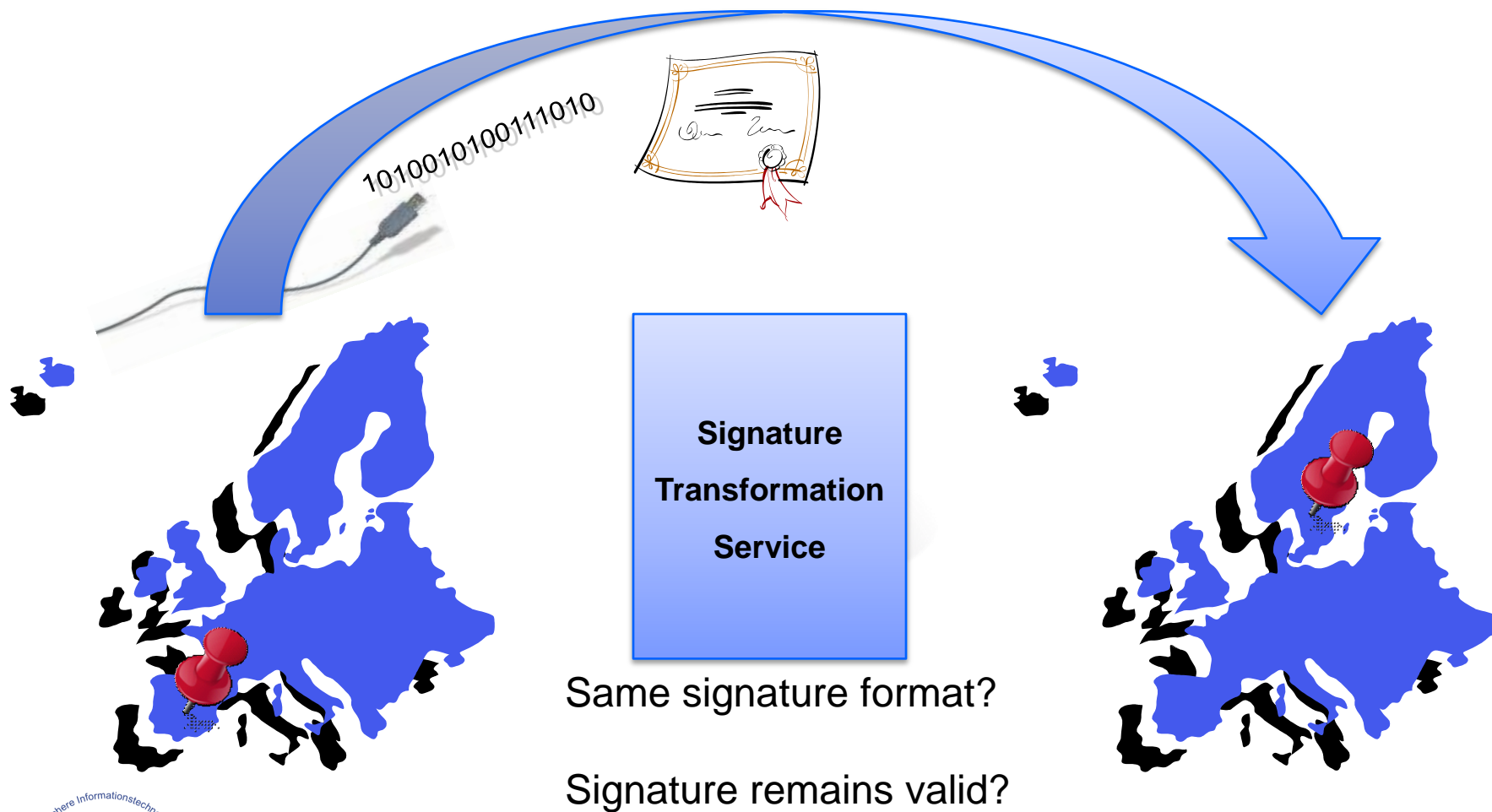
*Signiert*



CMS

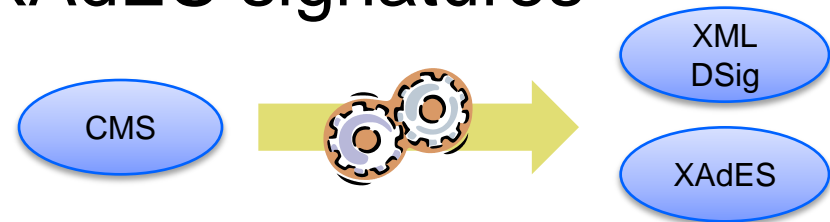


# Cross-Border Document Exchange

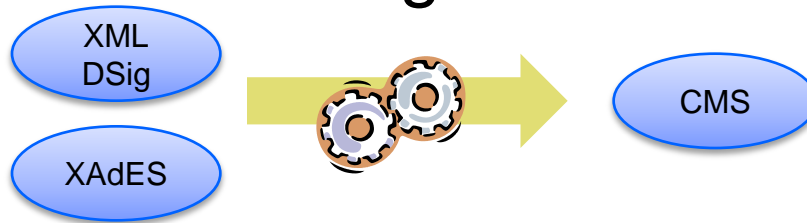


# Transformations

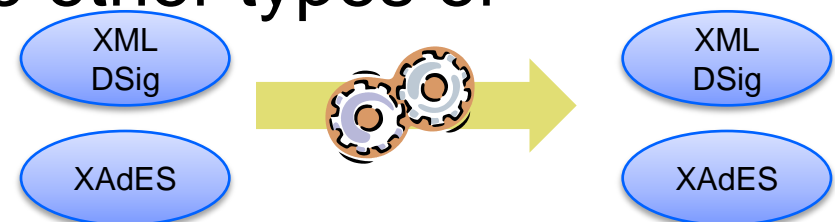
- CMS signatures to XML/XAdES signatures



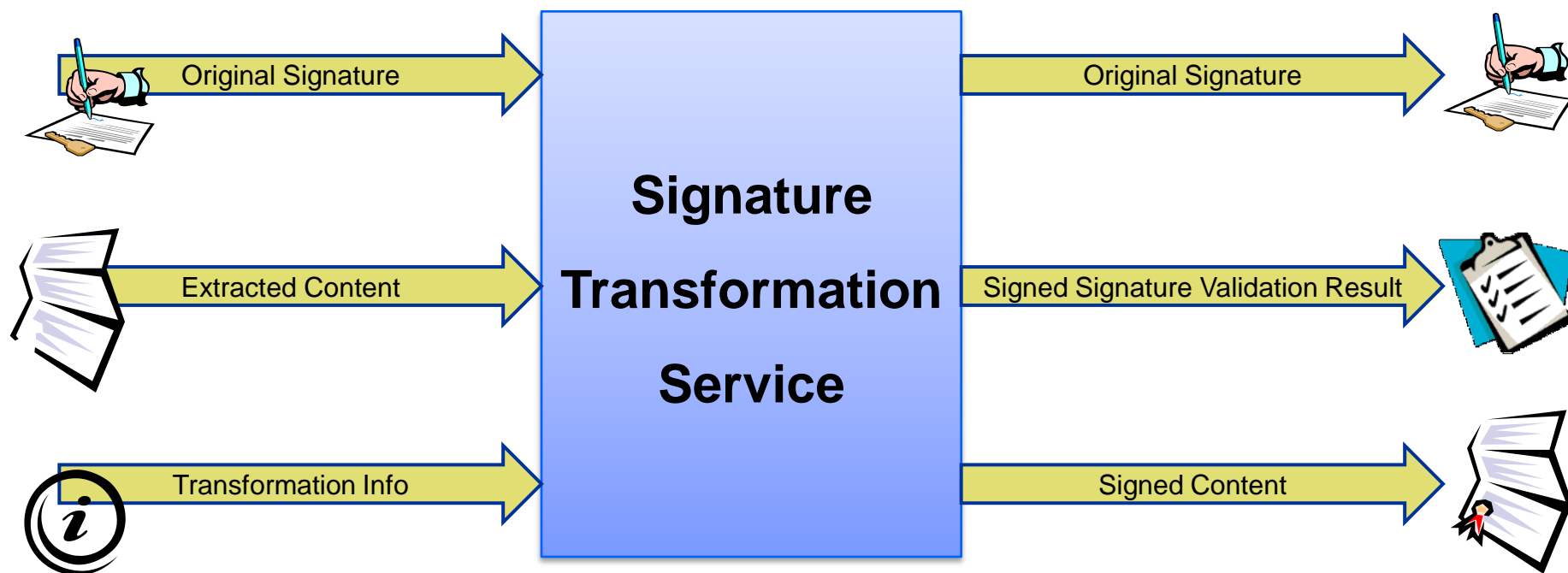
- XML/XAdES signatures to CMS signatures



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






# Signature Transformation Service

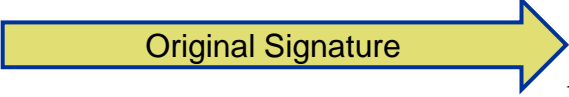

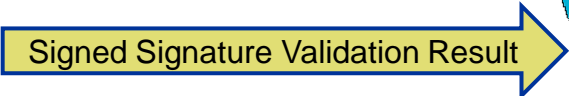







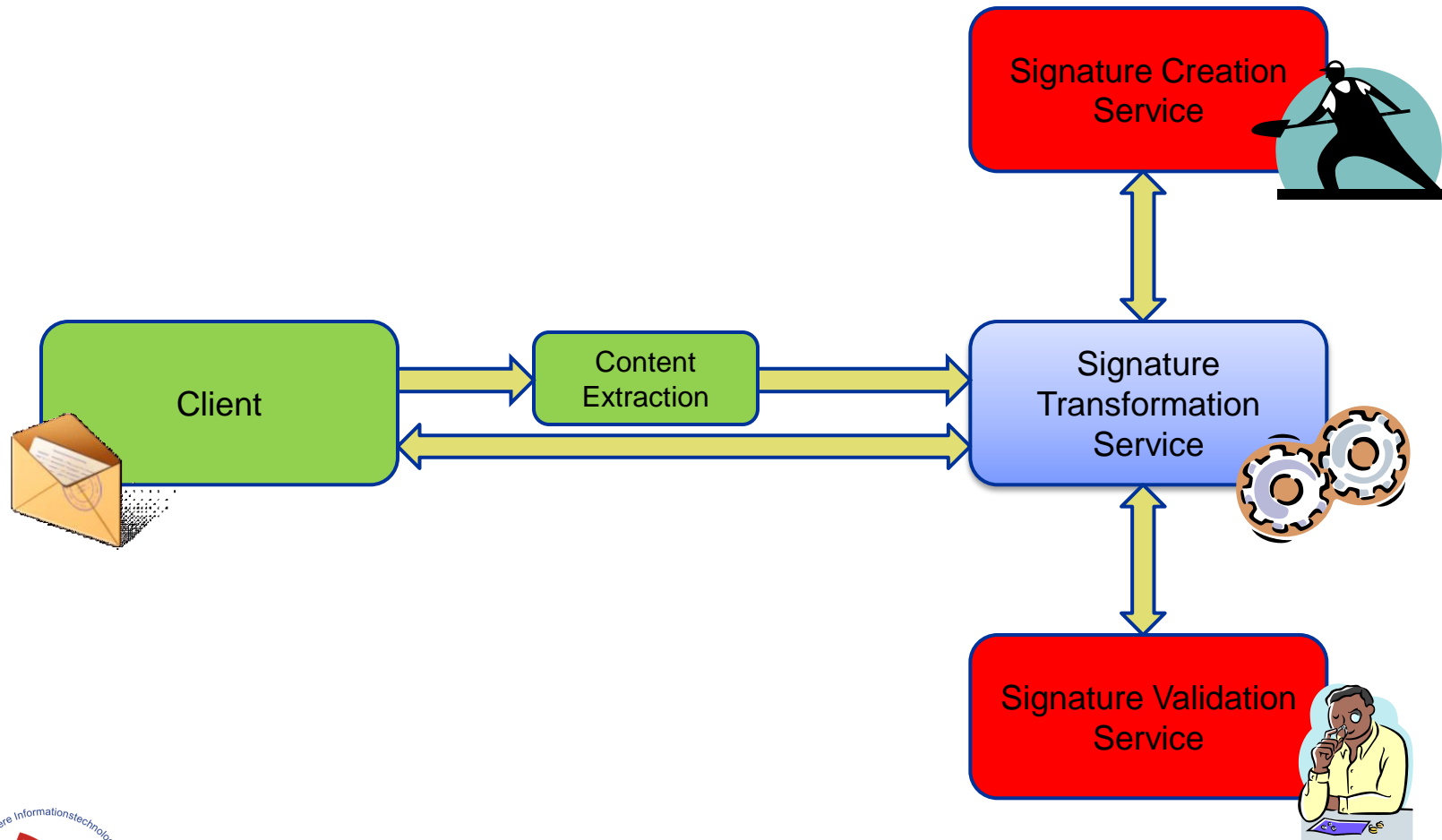
# Signature Transformation Service

 <p>Original Signature</p>	<ul style="list-style-type: none"><li>• CMS-based signatures</li><li>• XML-based signatures</li></ul>
 <p>Extracted Content</p>	<ul style="list-style-type: none"><li>• XML encoded</li><li>• Base64 encoded</li></ul>
 <p>Transformation Info</p>	<ul style="list-style-type: none"><li>• ID for selection of trustable root certificates</li><li>• Type of signature to create</li><li>• ID for signature key</li></ul>

# Signature Transformation Service

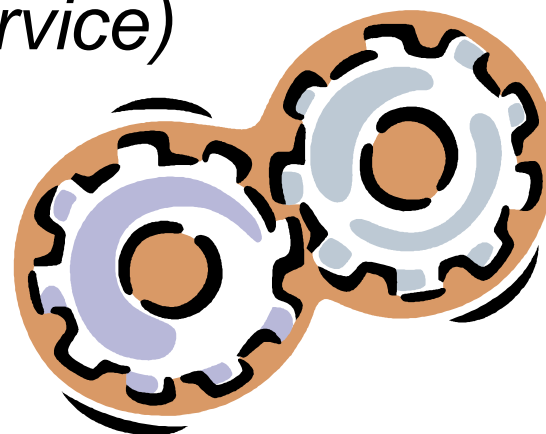
 <p>Original Signature</p>	 <ul style="list-style-type: none"><li>• CMS-based signatures</li><li>• XML-based signatures</li></ul>
 <p>Signed Signature Validation Result</p>	 <ul style="list-style-type: none"><li>• CMS-based signatures</li><li>• XML-based signatures</li><li>• Error response</li></ul>
 <p>Signed Content</p>	 <ul style="list-style-type: none"><li>• CMS-based signatures</li><li>• XML-based signatures</li><li>• Error response</li></ul>

# 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*)



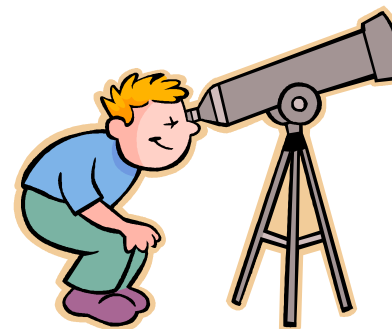
# Signature Creation and Validation Service

- 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

<i><b>Signature Verification</b></i>	<i><b>Signature Creation</b></i>
<ul style="list-style-type: none"><li>• XMLDSig signatures</li><li>• XAdES-BES signatures</li><li>• XAdES-T signatures</li><li>• XAdES-C signatures</li><li>• XAdES-X signatures</li><li>• CMS signatures</li></ul>	<ul style="list-style-type: none"><li>• XMLDSig signatures</li><li>• XAdES-BES signatures</li><li>• XAdES-T signatures</li><li>• CMS signatures</li></ul>

# 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