DITEC - Data Information technology & Expert Consulting

ofil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnosti Profil Spoločnos

DITEC je vedúcim integrátorom informačných technológií. Svojim zákazníkom poskytujeme komplexné služby v oblasti nasadzovania a prevádzky informačných systémov.

DITEC
Data Information Technology & Expert Consulting

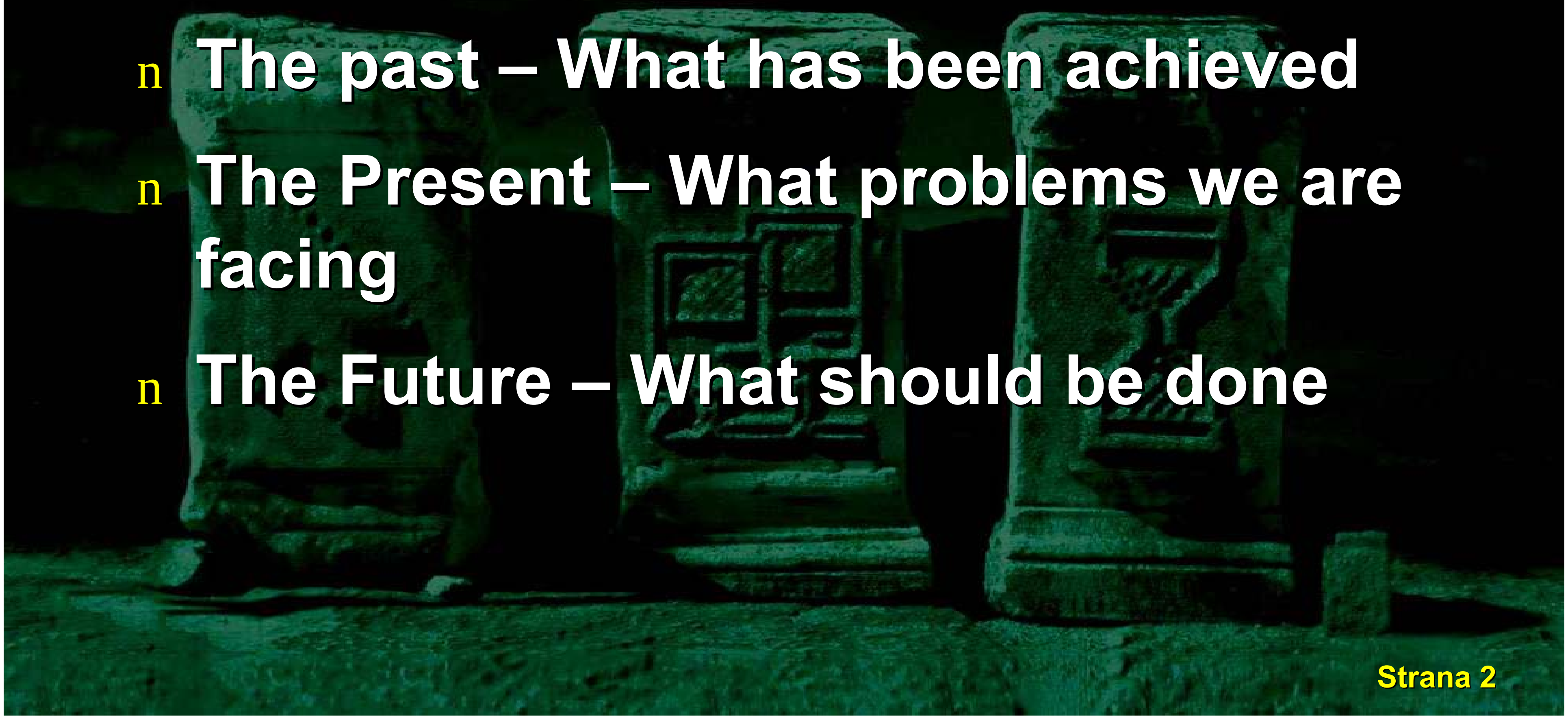
DITEC je firma s tradíciou. Počas svojej existencie sme sa vypracovali na stabilný subjekt, ktorý je dôveryhodným a dlhodobým partnerom významných organizácií.

On Interoperability Issues of Electronic Signature

Pavol Frič

Content

- Motivation
- The past – What has been achieved
- The Present – What problems we are facing
- The Future – What should be done



1. Motivation

- Strategic goals stated at the EU Level
  - Building of information society should:
    - provide a basis for competetiveness and economic growth
    - build better place for living and higher quality of life
  - Europe is aiming towards an integrated service market and pan-european e-services
    - Digital Agenda for Europe
  - this goal strongly depends on the possibility of performing legal acts electronically
    - usually based on electronic signature, as defined by legislation

2. The Past – What has been achieved

- Legislative codification of electronic signature
  - Directive 1999/93/EC on a Community framework for electronic signatures (13 December 1999)
- Other acts related to electronic signature at the European level
  - standardisation activities of EU bodies
  - Directive 2006/123/EC on services in the internal market (12 December 2006)
    - » 2009/767/ES facilitating the use of procedures by electronic means through the ‘points of single contact’ (publishing of TSL)

Directive 1999/93/EC

- Purpose
  - to promote cross-border legal recognition of electronic signatures
  - to ensure a free circulation within the internal market of e-Signature products and services
- Business model
  - allow legal admissibility of any kind of electronic signature whilst allowing legal equivalence of QES with a handwritten signature
  - have the market decide on the technical fulfillment of requirements and presume compliance with requirements and standards

- Types of electronic signature
  - “Basic“ electronic signature
  - „Advanced“ electronic signature
  - „Qualified“ electronic signature
    - » having the same legal value as a hand-written signature
- Role of Commission
  - Par. 27 - two years after its implementation the Commission will carry out a review of this Directive
    - » to ensure that the advance of technology or changes in the legal environment have not created barriers
    - » to examine the implications of associated technical areas
  - Art. 7.2 - make proposals to achieve the effective implementation of standards and international agreements applicable to certification services

- Role of Member States
  - Art. 3.7. - Member States may make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory.
  - Art. 13.1 - Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive before 19 July 2001

On Interoperability Issues of Electronic Signature

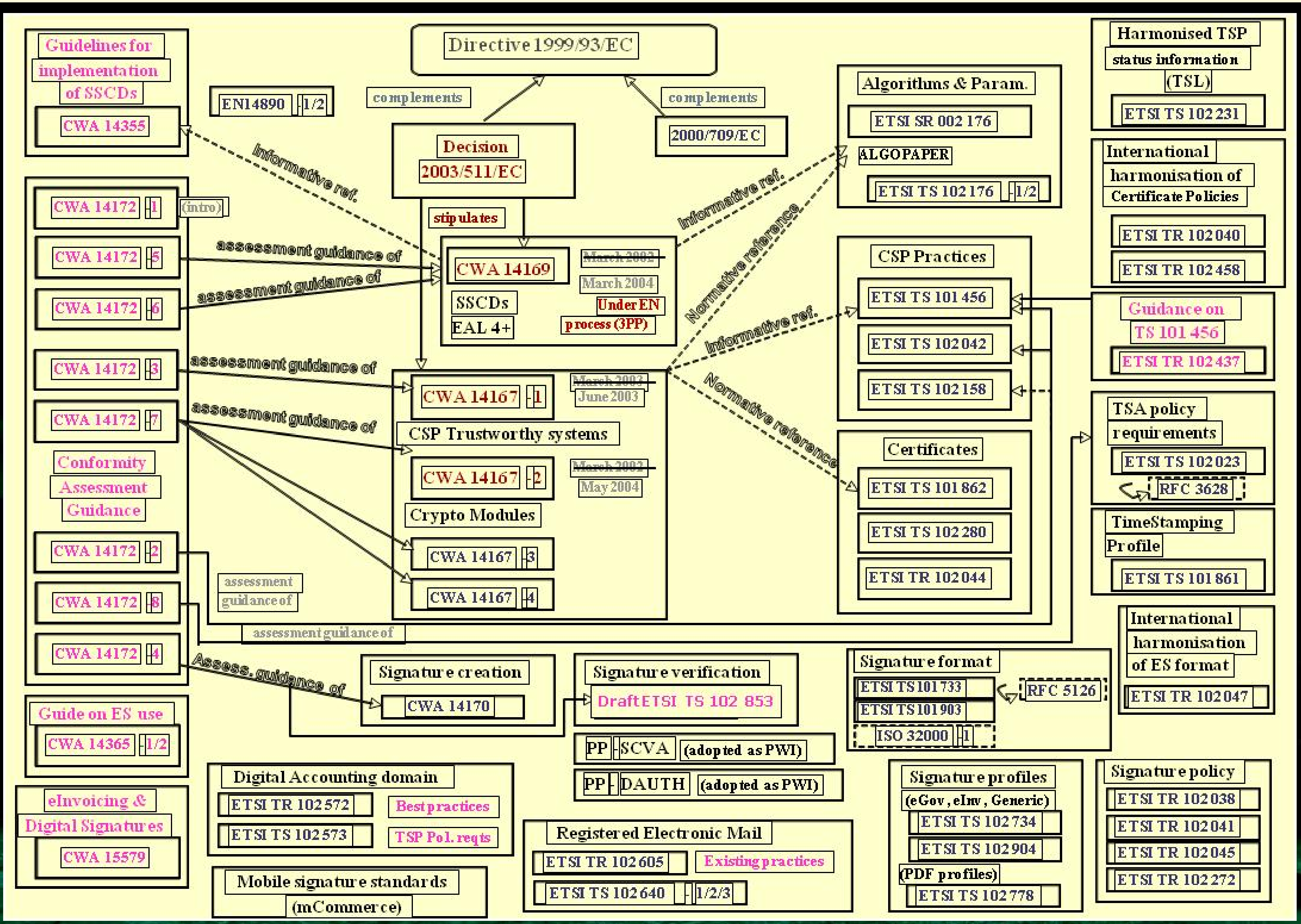
- **Consequences of Directive approach**
  - Member states adopted national law based on the Directive
    - » Directive too general, local provisions are country specific
- **Positive and negative points**
  - Positive
    - » it exists
    - » is important foundation to work on as a common legal and technical set of practices allowing legal recognition of eSignatures all over Europe
  - Negative
    - » lack of precise requirements (Directive or set of standards) leading to different interpretations in Member States
    - » result - incompatible applications and interoperability problems

Standardisation activities

- Standardisation activities on EU level:
  - CEN – European Committee for Standardisation
    - » CWA-CEN workshop agreement
  - ETSI – European Telecommunications Standards Institute
    - » ETSI TS – ETSI technical specification
  - EESSI – European Electronic Standardisation Initiative
- Commision decision 2003/511/EC
  - On publication of reference numbers of generally recognised standards for electronic signature products

DITEC
Data Information Technology & Expert Consulting

On Interoperability Issues of Electronic Signature



Guidelines for implementation of SSCDs
CWA 14355

CWA 14172 -1 (intro)
CWA 14172 -5
CWA 14172 -6
CWA 14172 -3
CWA 14172 -7
Conformity Assessment Guidance
CWA 14172 -2
CWA 14172 -8
CWA 14172 -4

Guide on ES use
CWA 14365 -1/2

eInvoicing & Digital Signatures
CWA 15579

EN14890 -1/2

Directive 1999/93/EC
complements
complements
Decision 2003/511/EC
2000/709/EC
stipulates

Informative ref.
assessment guidance of
assessment guidance of
assessment guidance of
assessment guidance of
assessment guidance of
assessment guidance of
Assess. guidance of

CWA 14169
SSCDs
EAL 4+
~~March 2002~~
March 2004
Under EN process (3PP)

CWA 14167 -1
~~March 2003~~
June 2003
CSP Trustworthy systems
CWA 14167 -2
~~March 2003~~
May 2004
Crypto Modules
CWA 14167 -3
CWA 14167 -4

Signature creation
CWA 14170

Signature verification
Draft ETSI TS 102 853

PP -SCVA (adopted as PWI)
PP -DAUTH (adopted as PWI)

Digital Accounting domain
ETSI TR 102 572
Best practices
ETSI TS 102 573
TSP Pol. reqts

Mobile signature standards (mCommerce)

Registered Electronic Mail
ETSI TR 102 605
Existing practices
ETSI TS 102 640 -1/2/3

informative ref.
Normative reference
informative ref.
Normative reference

Algorithms & Param.
ETSI SR 002 176
ALGOPAPER
ETSI TS 102 176 -1/2

CSP Practices
ETSI TS 101 456
ETSI TS 102 042
ETSI TS 102 158

Certificates
ETSI TS 101 862
ETSI TS 102 280
ETSI TR 102 044

Signature format
ETSI TS 101 733
ETSI TS 101 903
ISO 32000 -1
RFC 5126

Signature profiles (eGov, eInv, Generic)
ETSI TS 102 734
ETSI TS 102 904
(PDF profiles)
ETSI TS 102 778

Harmonised TSP status information (TSL)
ETSI TS 102 231

International harmonisation of Certificate Policies
ETSI TR 102 040
ETSI TR 102 458

Guidance on TS 101 456
ETSI TR 102 437

TSA policy requirements
ETSI TS 102 023
RFC 3628

TimeStamping Profile
ETSI TS 101 861

International harmonisation of ES format
ETSI TR 102 047

Signature policy
ETSI TR 102 038
ETSI TR 102 041
ETSI TR 102 045
ETSI TR 102 272

- Results of standardisation activities
  - lots of standards that are not organised in an consistent and comprehensive way
    - » problems when implementing electronic signature products
  - main problems identified
    - » standards rather complex
    - » too many standards (neverthenless some gaps remain)
    - » If/though providing necessary information, it is hard to find it
  - practical problems
    - » “too much flexibility“ e.g. E-signature formats and profiles – implementation requires to support many variations, with significant impact on implementation costs

Directive 2006/123/EC

- Purpose
  - – to create a common and open market for services in EU
- Basics
  - – 52 - Member States should provide means of completing procedures and formalities by electronic means. The fact that it must be possible to complete those procedures and formalities at a distance means, in particular, that Member States must ensure that they may be completed across borders

- **Member states shall:**
  - **Art 6.1. - MS shall ensure that it is possible for providers to complete procedures and formalities through points of single contact**
  - **Art 8.1. – MS shall ensure that all procedures and formalities related to access to a service activity and to the exercise thereof may be easily completed, at a distance and by electronic means, through the relevant point of single contact**
  - **Art 34.1 - The Commission, in cooperation with MS, shall establish an electronic system for the exchange of information between MS, taking into account existing information systems**

Commision decision 2009/767/EC

- Member states shall
  - Art 1.1. – MS may require, for the completion of certain procedures and formalities through the points of single contact, MS may require use of advanced electronic signatures based on a qualified certificate by the service provider
  - Art 1.2. - MS shall accept any AES based on a qualified certificate, for the completion of the procedures and formalities, without prejudice to the possibility for MS to limit this acceptance to AES based on a qualified certificate if this is in accordance with the risk assessment

On Interoperability Issues of Electronic Signature

- – Art 1.3. – MS shall not make the acceptance of AES based on a qualified certificate, subject to requirements **which create obstacles to the use**, by service providers, of procedures by electronic means through the points of single contact
- – Art 2.1. - each MS **shall establish, maintain and publish a ‘trusted list’** containing the minimum information related to the certification service providers issuing qualified certificates to the public who are supervised/accredited by them

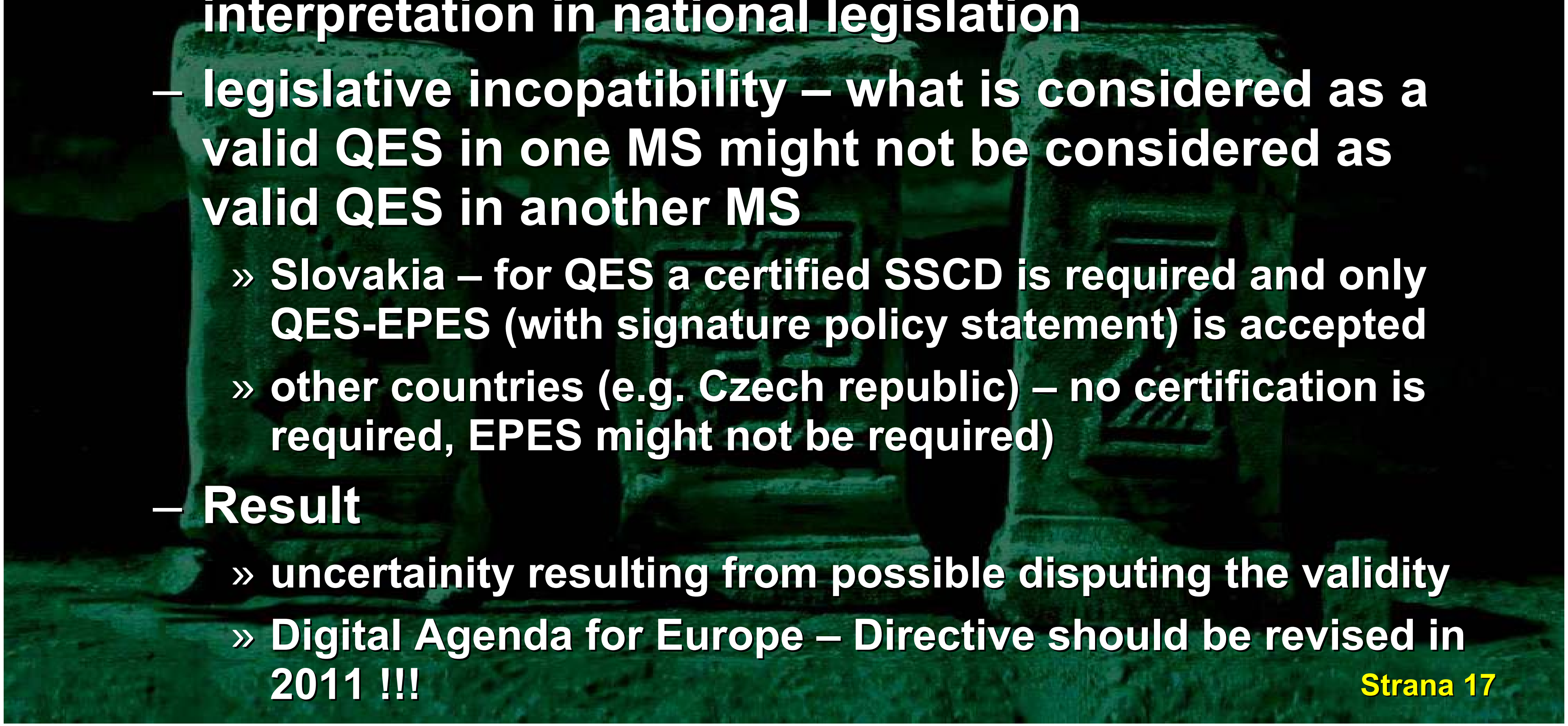
- What does this mean
  - – QES should be accepted
  - – BUT – **QES is used to represent electronic legal document or legal act – are these valid according to legislation environment ?**

3. The Present – Problems to be faced

- **Relevant assessment documents**
  - Study on standardisation aspects of eSignature (2007)
  - IDABC Preliminary study on mutual Recognition of eSignatures for eGovernmental applications
- **Main problems identified**
  - interoperability – both on legislative and technical level

Legislative level

- Directive heritage
  - too general formulations resulting in various interpretation in national legislation
  - legislative incopatibility – what is considered as a valid QES in one MS might not be considered as valid QES in another MS
    - » Slovakia – for QES a certified SSCD is required and only QES-EPES (with signature policy statement) is accepted
    - » other countries (e.g. Czech republic) – no certification is required, EPES might not be required)
  - Result
    - » uncertainity resulting from possible disputing the validity
    - » Digital Agenda for Europe – Directive should be revised in 2011 !!!



Broader scope

- electronic signature is a tool for assuring legal validity of docuuments and acts, it is not a goal
- formal requirements for validity of such act defined by national legislation
  - requirements on mandate or authorisation of acting person
  - declaration of person identity (e.g. Official signature certification by notary, citizen ID in certificate, etc.)
- result – problems with legal act validation when electronic form (of a legal act or document) with electronic signature is used
  - solely validating person/body is responsible for consequences of such validation (possitive or negative) result and further acting based on that

Technical level

- Standardisation activities heritage
  - too many standards and too many options in standards – which options should be really supported ?
    - problem is not signature creation, but signature validation
  - current activities not heading towards reducing abundant variability, but to standardise everything that is on the market
    - unfounded and high financial costs for building solutions supporting all possible options

- AdES reference format (proposal for a meeting of TG on e-Procedures)
  - MS will support QES and AdES based on QC
  - reference format should facilitate cross-border interoperability
  - proposed reference format:
    - » CAdES/XAdES/PAdES BES or EPES as minimum
    - » MS can choose between three above mentioned formats for creation of QES, but have to support all three formats for verification
  - the problem is not only in signature format, but in signature profiles, as the format definition provides enormous flexibility
    - » signature profile is important for signature validation

- **XAdES interoperability examples**
  - **Signature policy - BES vs. EPES**
    - **in some countries BES is not accepted as an equivalent of hand-written signature (e.g. Slovakia)**
  - **Signature topology**
    - **reference format requires support for Enveloped, Enveloping and Detached**
    - **Enveloped (signature within signed document) is document type specific !!!**
  - **Canonicalisation method, Transforms**
    - **several methods have to be supported concurrently**
  - **Digest method, Signature method**
    - **a reference to national laws**
    - **problem with interoperability (e.g. transition period from SHA1 to SHA2, or RSA 1K to RSA 2K different in MS)**

- XAdES interoperability examples
  - ZIP container – used for detached signature for interoperability purposes ?
    - Representing real needs ?
      - multiple signatures for multiple documents ?
      - ZIP is file oriented, problems with structuring more complex relations
    - Effective for real usage ?
      - XAdES mainly used for XML documents
      - XML document and detached XAdES should be „wrapped“ into ZIP
      - ZIP container tramsformed into XML message that is commonly used in business processes
- Results
  - standards definitions do not always reflect real business requirements
  - who will pay for it ?

4. The Future – What should be done

- **Problems identified – the priority of their solution**
  - establishing „interoperability“ at legislative level
  - preparing real interoperable standards
  - solving real problems related with digital signature practical usage

Interoperability at legislative level

- at EU level
  - legal act interoperability
    - » legal act valid on one member state should/must have a proven validity also in another member state
  - qualified electronic signature interoperability (harmonisation of e-Signature Directive consequences)
    - » Definition of clear interoperability requirements in Directive fundamental revision
- at MS level
  - adopting corresponding changes into MS legislation

Standardisation

- Changing the approach towards standardisation
  - prioritising real business needs, involving experts from different business areas
  - significantly lowering the complexity of what has to be supported
  - aiming towards a clear unified standard
    - not standardising everything what is available and conform to the wishes of business lobbyists (PAdES ?)

What should be the standardisation aims:

- standardisation deliverables should
  - support the process of designing, developing, operating and managing ES applications or services
  - cover requirements of all types of ES stakeholders (end-users, application/ service provider, supporting industry)
- provide a sufficient set of requirements, criteria or guidelines to ensure:
  - a correct implementation meeting the Directive requirements against the targeted type of electronic signature
  - correct implementation that is interoperable at the national, European and international levels enabling cross-borders and cross-applications secure communications, whatever is the appropriate or chosen technology

Solve real problems

- Addressing real business problems
  - long-term archivation of electronic documents with electronic signature
- Supporting all involved subjects
  - providing methodical guidelines for effective electronic signature implementation
  - standardisation in other business areas (e.g. Invoicing)

Thank you.

Questions ?