



Study on the Standardisation Aspects of eSignatures – INFSO 2006-0034




NISSG Meeting
16/06/2008
Brussels, Belgium

Agenda

- Consortium – Team of Experts
- Study Objectives
- Survey results
- Was the business model right ?
- Recommendations
- Conclusions

Consortium – Team of Experts



- 
 - Prime contractor
 - With the persons of **Sylvie Lacroix** and **Olivier Delos**, two recognised senior e-Security and e-Signatures consultants
- 
 - Sub-contractor
 - With the person of **Prof. Patrick Van Eecke**, one of the most recognised legal experts in the IT field, and in particular in the regulatory framework of e-Signatures
- 
 - Sub-contractor
 - With the persons of **Michael Custers** and **Wim Janin**, specialists in marketing and communication surveys.

Study Objectives Overview

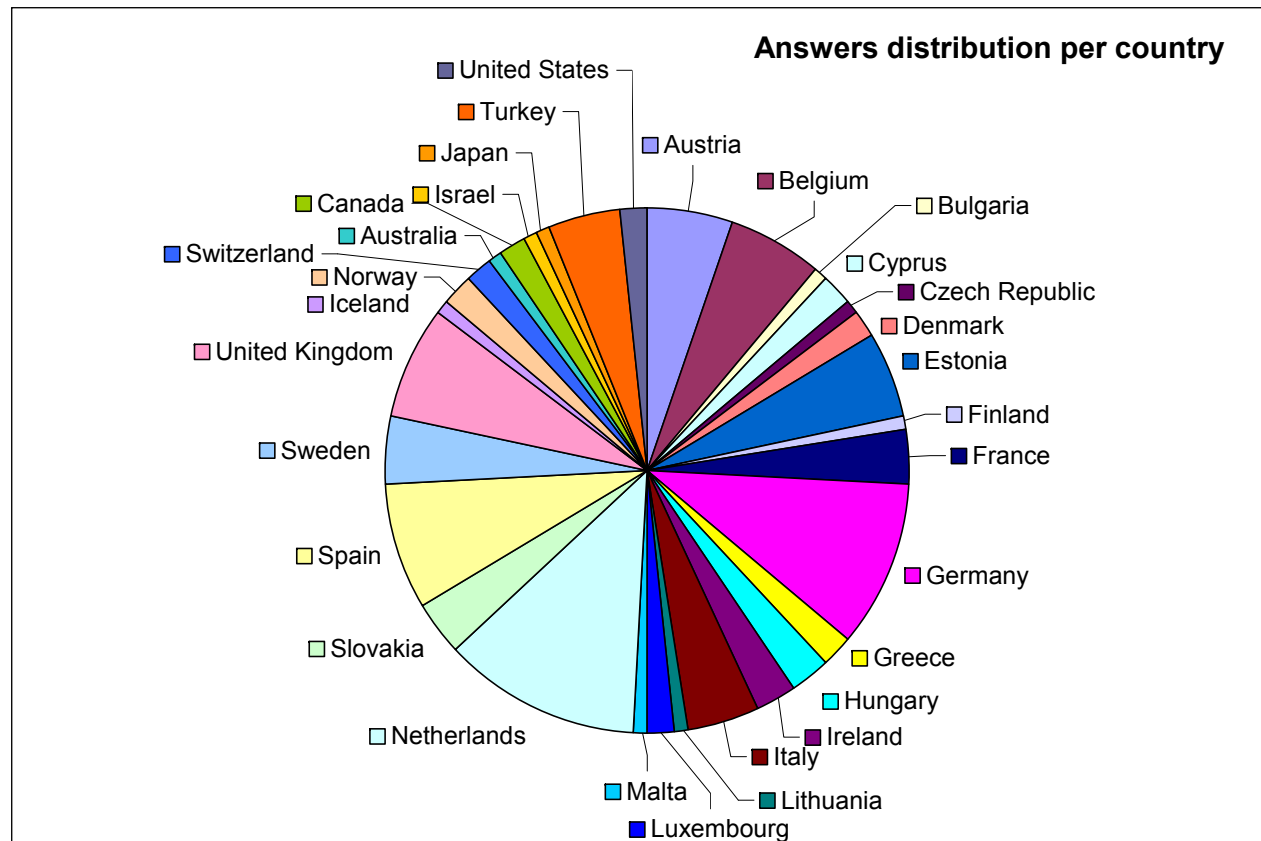
- Study context:
 - Directive 1999/93/EC
 - *Facilitating the use of electronic signatures and contributing to their legal recognition*
 - *Harmonising legal framework*
 - Set of electronic signature standards (CEN & ETSI within EESSI initiative)
 - To further facilitate use of electronic signatures
 - To ensure minimum interoperability between implementations
- Study objective:
 - Ensure the in-depth analysis of the technical requirements aimed to support the review of the operation of the EC Decision 2003/511 *referencing generally recognised standards for which complying products are presumed to be in conformity with Annex II(f) and Annex III of the 1999/93/EC Directive.*

The service contract should include

- First part: Analysis of eSignatures applications in EU & EEA
 - Which technologies are used ? Which are emerging ?
 - Are applications based on generally recognised standards mentioned in the Decision?
 - Which other standards/tech. specs are used ?
 - Are different standards available outside EU ?
 - Does the use of referenced standards guarantee interoperability ?
 - How have MS used the Decision in their legal text ?
- Second part: Analysis of the adequacy of the standardisation model proposed by 1999/93/EC Directive, the reference of generally recognised standards, to ensure interoperability of eSignature products and services in the Internal Market
- Third part: Conclusions and recommendations
 - For the standardisation activities linked to the Directive
 - For the standardisation model linked to the Directive
- Supported by interviews with MS, users, main suppliers and std organisations

Survey results: Respondents identification

EU countries	
Austria	6
Belgium	7
Bulgaria	1
Cyprus	2
Czech Republic	1
Denmark	2
Estonia	6
Finland	1
France	4
Germany	12
Greece	2
Hungary	3
Ireland	3
Italy	5
Latvia	0
Lithuania	1
Luxembourg	2
Malta	1
Netherlands	14
Poland	1
Portugal	0
Romania	1
Slovakia	4
Slovenia	0
Spain	9
Sweden	5
United Kingdom	8
EEA countries	
Iceland	1
Liechtenstein	0
Norway	2
Switzerland	2
Other countries	
Australia	1
Canada	2
Israel	1
Japan	1
Turkey	5
United States	2
TOTAL	118



- 118 full entries: 110 from 24 EU countries, 5 from 3 EEA countries, 12 from other countries (5 from TR)

Survey results: Respondents identification

- Interviewees spread over different categories:
 - Application or Service Provider or supporting industry (36%),
 - Certification Service Providers (CSP) or CSP supporting industry (22%),
 - Public Authorities & Member States Policy makers (11%), and
 - Opinion leaders from standardisation bodies (6%).
 - No citizen end-user
- Interviewee company size:
 - 46% with less than 100 employees
 - 29% with 100 < employees < 1000
 - 25% with more than 1000 employees

Survey results: Context & Reasons for using ES

- 73% of respondents are using ES
- 9% plan to use ES
- 18% do not intend to use ES

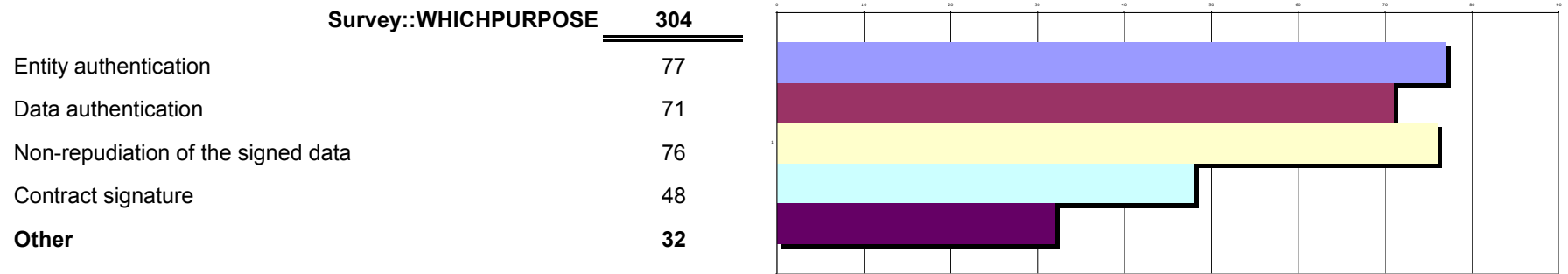
- Domain of ES use:
 1. eGovernment
 2. Document signing (PDF, MS Office, emails)
 3. eBanking/Finance, eInvoicing, eProcurement

- Advanced services: archiving of eSignatures
- Mobile ES based on ETSI TS in two countries (LT, TR)

Survey results: Context & Reasons for using ES

- From respondents using ES (or planning to use), they do it for:

For what purpose are you using or implementing electronic signatures in your application?



- Entity authentication is worthy to be noted as when correlated with ES type, it appears to be based on AES and even QES
- Majority of use in Open Systems (57%)
- Implementation: QES (40%), AES (38%), SES (17%)

Survey results: Context & Reasons for using ES

- PKI is, surprisingly or not, the most used technology (90%)
- 60% of the signature implementations rely on SSCDs
- When applicable half of the implementation rely on eID cards
- 88% of respondents using ES are making use of validation services (OCSP and/or CRLs)
- Long term validity of the ES is offered in 55% of the cases (confirming (s)low awareness of criticality of such services)
- Expected promising technologies:
 - Mobile & wireless technologies
 - Centralised signature creation devices (SSCD ?)

Survey results: Reasons for **not** using ES

- Primarily because they believe there is no real business need for it
- Secondly because it seems difficult to implement
- Thirdly because they believe market is not mature enough

Survey results: Use of ES standards

- Large majority is making use of standards (82,5%)
 - 73% is using EU standards
 - 27% is using other standards but often in complement to EU standards. Other standards used:
 - IETF, PKIX RFCs, ISO standards, XMLSIG
 - National Standards: ISIS-MTT in Germany only, SEID in Norway and Sweden

- Reasons why not using EU standards in ES:
 1. Do not perceive the benefit to use them
 2. Lack of awareness
 3. Other framework available

Survey results: Opinion on standards complexity

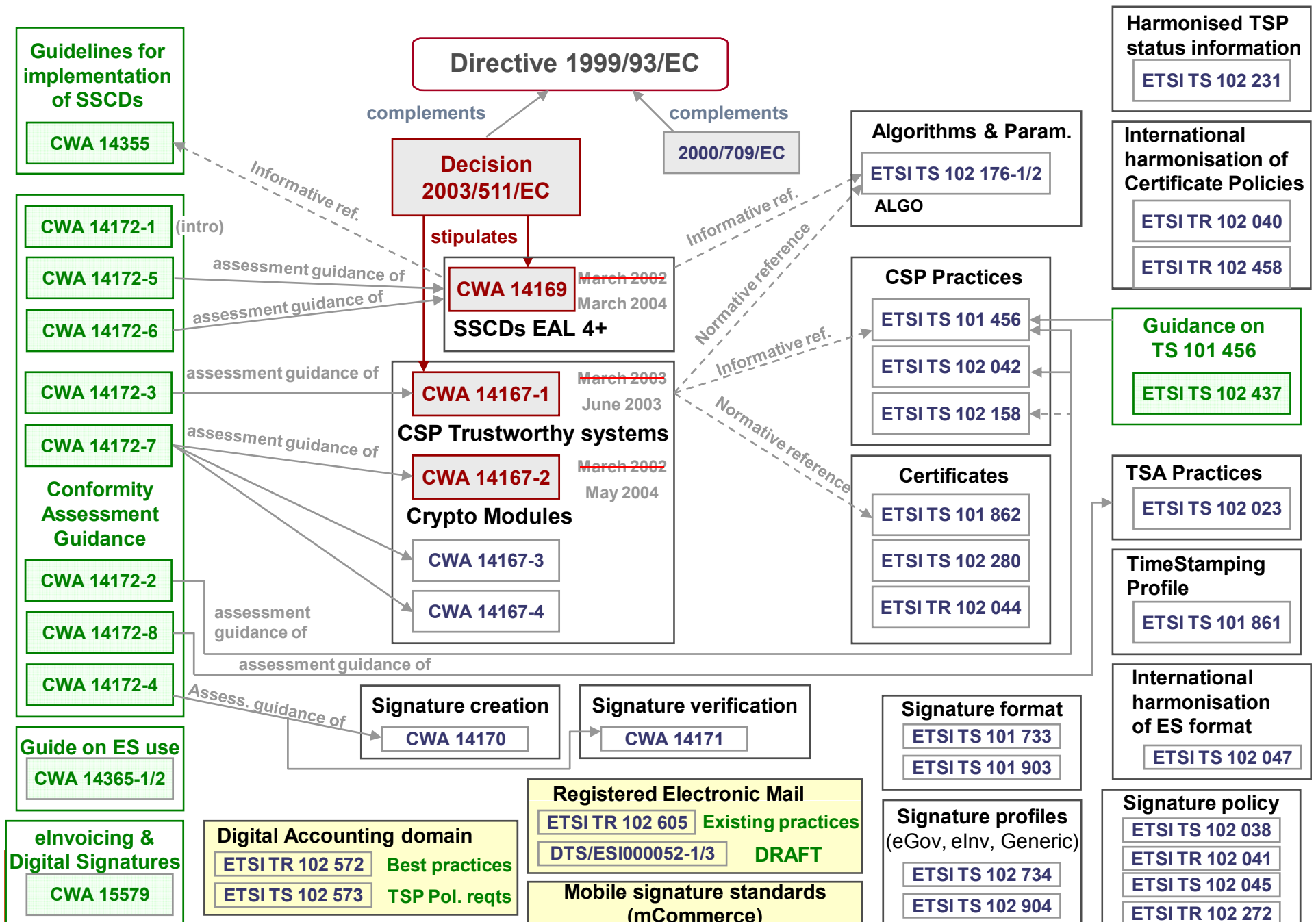
- More than 87% of respondents were familiar with EU Standards in ES
- From these familiar respondents, opinion on complexity clear shows that they find the standards:
 - Rather or Too complex
 - Too numerous (with still even some identified gaps)
 - While providing sufficient completeness of information
 - Lack of explanations on coherence between standards
 - Difficult to find them
 - Related guidelines or implementation samples not sufficient or not good enough

Survey results: Opinion on standards complexity

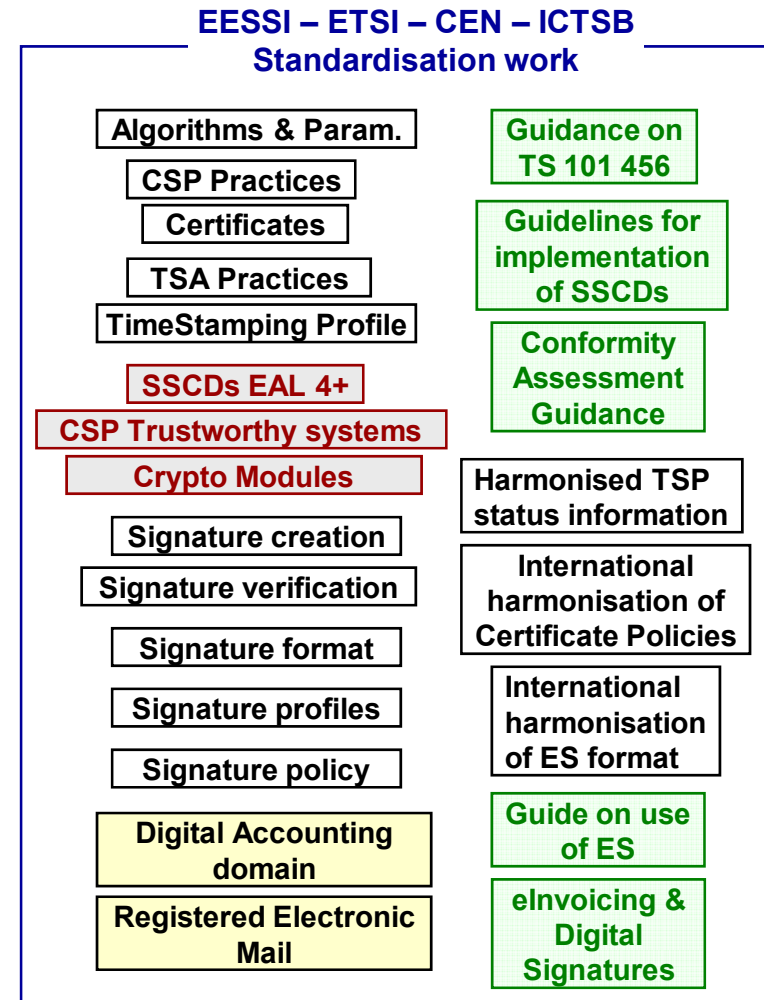
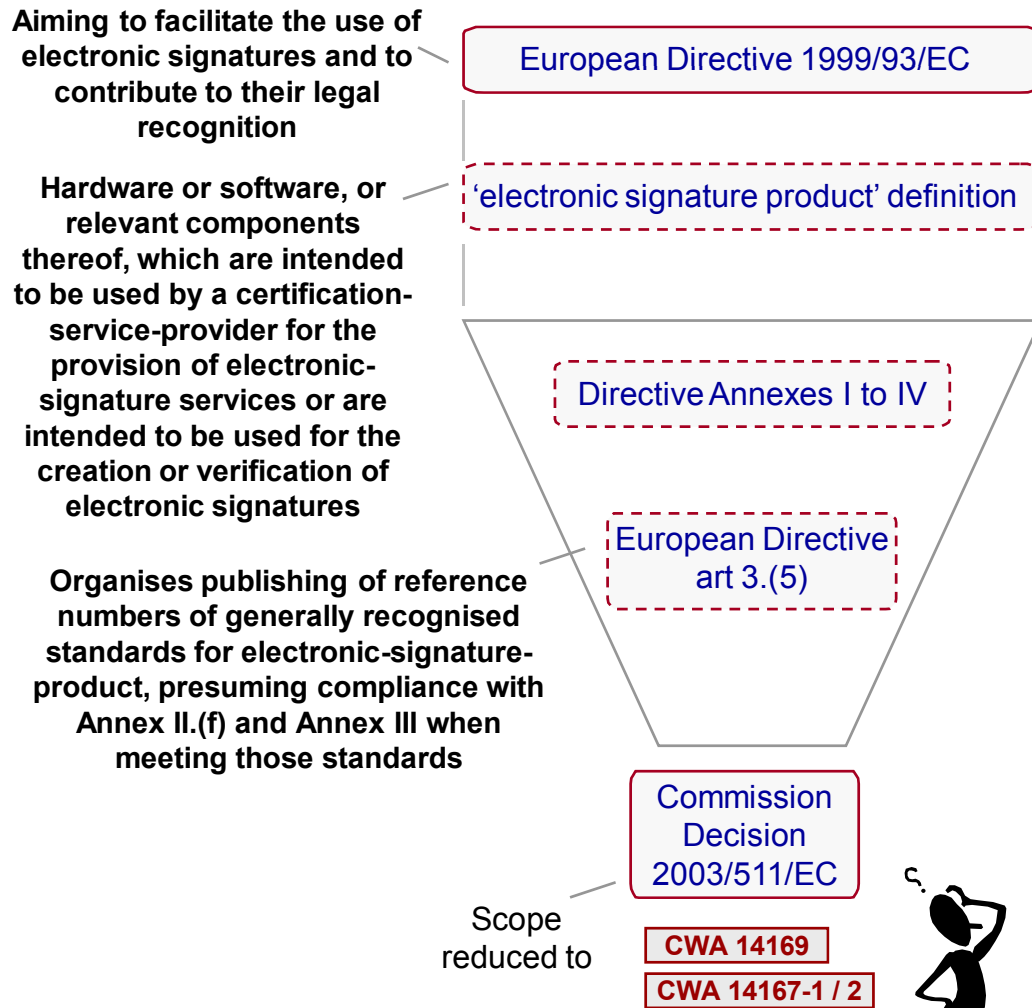
- Expressed opinions
 - Business and practice based standards wanted
 - Too many possible implementation options > < interoperability
 - Too many possible interpretations
 - Too academic not enough business practice
 - Not enough high level straight-talking description to help newcomers
 - Not self explanatory
 - No implementation samples,
 - Not enough commercially available standards compliant software
 - Lack of clear link with the laws
 - International dimension required (outside EU)
 - True standards wanted (not only deliverables)
 - One single easy to access and to understand eSignature standards repository
 - (+ mapping with other frameworks)

EU eSignature Standardisation Work overview

(© SEALED, 2007)



Adequation of published recognised standards vs market needs



Non-CSP party willing to operate/implement (qualified) electronic signatures

- Which standard(s) to comply with when designing or selecting an e-Signature application ?
- How to be sure that resulting implementation is in line with legal recognition of QES / AES ?
- How to be certified or controled against this ?

Survey results: Usefulness of EU ES standards

- Usefulness of EU ES standards is more encouraging:
 - 74% affirms that standards help them to comply with laws
 - 60% claim standards are at least slightly helpful to meet their business needs

Survey results: Market expectation on standards

- Regarding ES standardisation approach, a majority of respondents are seeking
 - a **formal way of working**
 - encompassing a list of standards and
 - guidelines to follow and
 - Possibly accompanied by an official certification
- Expectations from the standards
 - Reach a maximum level of interoperability (within and beyond EU)
 - Reach legal recognition
 - Better link with standards
 - Better link between standards themselves
 - Easy implementation and clear set of guidelines

Survey results: Marketing aspects

- Perceived reasons for slow market activity in (Q)ES
 - Complexity of the technology
 - Complexity of related standards (not based on business practices)
 - This induces high market prices & costly implementations
 - For which no perceived business benefit compared to existing solutions
 - → resulting in too few applications

 - However high growth in # of applications experienced in DE, CZ, IT as pushed by
 - Law
 - eGov initiatives
 - Service oriented business models

 - Lack of promotion and awareness

Survey results: Marketing aspects

- Marketing and promotion of ES standards
 - Efforts of Commission are considered insufficient
 - Promotion and marketing efforts around ES standards are expected from
 1. The Commission 27,6%
 2. Member States 21,9%
 3. Industry 21,4%
 4. ESOs 18,2%
 5. Others 10,9%

Survey results: Consolidation of ESO respondents

- Standardisation process is not understood or even known (not only to target users of deliverables)
 - 4 ETSI members (only) can initiate work on a subject
 - Work item participants are not interested to serve community interests but their own (commercial) interest and technological advance
 - Call for comments not always widely published
 - Drafting a standard is always a compromise between interest and academic quality of documents
- Agreement on the fact that standardisation process should be more driven by the business
 - Business \neq Sole industry
 - Business = whole set of business domain stakeholders
- Agreement on taking into consideration costs/benefits aspects

Survey results: Consolidation of ESO respondents

- Recognition will come from the business
 - Business needs & practices + legal constraints
= supporting technical specifications

Standardisation work must be **driven by the real business requirements**, clearly **mapped to the legal requirements** in order to ensure the legal compliance when this is possible, and standards should give the **appropriate technical and economical implementation guidance** in order to have good quality implementation (not highest quality but appropriate quality with regards to cost/benefit and appropriate risk mitigation in the covered business domain) with a **maximised level of interoperability**.

- Less options & more guidance as a key to practical interoperability

Survey results: Conclusions

- Business & practices derived standards
 - Business needs + legal constraints
= supporting technical specs
 - Single documents getting coherence between existing standards on specific themes
 - Implementation profiles, guidelines, samples
 - Mapping with laws
- International dimension required
- True standards
- ES standards repository (single, easy access, free, up to date)
- Promotion by EC (and others)
 - Recognition of standardisation work and mapping with Directive
 - Marketing

Was the business model right ?

- **Successful model for what has been published**
 - Decision 2003/511/EC focused on one part of elements covered by definition of “electronic signature products” (Dir, art 2.11), i.e.:
 - CSP issuing (qualified) certificates (with presumed legal compliance with Annex II.f)
 - SSCD (with presumed legal compliance with Annex III)
 - After having experienced strong difficulties, Qualified CSPs market is becoming quite mature, stabilised and even flourishing like in Italy, Germany, or Spain
 - 71 QCAs are active in 15 EU countries
 - Main drivers: eGov applications and national eID schemes
 - Dominant use of published standards (CW 14167 ½, CWA 14169) and of those normatively or informatively referenced (e.g. ETSI TS 101 456, 101 862, 102 176 ½)

Was the business model right ?

- **Incompletely implemented business model**
 - Lack of transparency
 - Lack of definition or requirements related to the whole set of “electronic signature products”
 - Referencing issue
 - Lack of formal standards
- **Business issues related to the eSignatures standards**

(Not business practice, too complex, neither real standards nor referenced, approval process, not self explanatory, no clear link with Directive)
- **Interpretation of Directive and ESO deliverable not managed globally**
- **Lack of marketing and promotional efforts**

Was the business model right ?

Thus the system of

- Referencing a few standards, and by referencing them giving them more legal value (i.e. Presumption of conformity),
- Producing other standard deliverables but not referencing them, and thus not giving them more legal value,
- Limiting the standardisation work to CWA and not EN (no real standards)

has caused lots of confusion in the market.

Was the business model right ? Referencing issue

“electronic signature product” & referenced standards

Definition of “electronic signature product” Directive 1999/93/EC	Types of “electronic signature product”	Decision 2003/51/EC	New Decision	Existing standards
<p>‘electronic-signature product’ means:</p> <ul style="list-style-type: none"> • hardware or software, • or relevant components thereof, • which are intended to be used by a certification-service-provider for the provision of electronic-signature services • Or are intended to be used for the creation or verification of electronic signatures; 	<p>Used by Certification-service-provider</p> <ul style="list-style-type: none"> • Issuing qualified certificates • Issuing non qualified certificates <p>Used by Other CSPs</p> <ul style="list-style-type: none"> • Timestamping Services • (Long Term) Archiving Services • Registered Electronic Mail • ... <p>Creation or verification of ES</p> <ul style="list-style-type: none"> • SSCD • Other HW based applications • Other SW based applications 	<p>✓</p> <p>(✓)</p> <p>✗</p> <p>✗</p> <p>✗</p> <p>✗</p> <p>✓</p> <p>✗</p> <p>✗</p>	<p>✓</p> <p>✓</p> <p>✓</p> <p>✓</p> <p>—</p> <p>—</p> <p>✓</p> <p>✓</p> <p>✓</p>	<p>✓</p> <p>✓</p> <p>✓</p> <p>✓</p> <p>In prépa.</p> <p>—</p> <p>✓</p> <p>To be reviewed</p>

Was the business model right ? Referencing issue

- Without changing the directive, it is not possible to publish references to generally recognised standards in the OJ **ensuring legal compliance**, other than standards relating to Annex II (f) and Annex III
- Without changing the directive, it seems possible to publish in the OJ references to generally recognised standards relating to all types of electronic signature products, but without ensuring legal compliance for those not relating to Annex II(f) or Annex III. Legal basis for this publication is in our opinion article 3.5, sentence 1
- Without changing the directive, it seems possible to publish in the OJ references to standards (not necessary “generally recognised”) related to Signature Verification Devices (SVD) in order to include and cover all aspects of this type of electronic signature products. Legal basis for this publication is in our opinion article 3.6 while it is true that SVDs are already part of electronic signature products and can thus be covered by 3.5, sentence 1

Recommendations

- Legal & policy recommendations
- Standardisation related recommendations
- Quick wins on Qualified CA recognition and QES validation
- Marketing related recommendations
- Implementation of the recommendations
– organisational model

Legal & Policy recommendations

- **No directive review**
 - Would allow EU institutions to adapt some rules to reality
 - But not recommended
 - As cumbersome and time consuming procedures
 - May re-open lengthy discussions between Member States
 - May introduce market disruption from changes and time to reassess products
 - **Significant improvements clearly possible without changes**
- **New Commission Decision** for better referencing of standardisation deliverables

Legal & Policy recommendations

- **New Commission Decision**

- Amending or repealing Decision 2003/511/EC
- Updating list of generally recognised standards ensuring compliance with Annex II(f) and Annex III
- Adding a list of generally recognised standards for all types of electronic signature products
 - but explicitly stating that no legal compliance is presumed as per art 3.5
- Including adding a list of generally recognised standards for signature verification devices in the light of Annex IV
 - but explicitly stating that no legal compliance is presumed as per art 3.5
- Adding a list of generally recognised standards relating to AES originating in third countries
 - but explicitly stating that no legal compliance is presumed as per art 3.5

Quick wins on Qualified CA recognition and QES validation

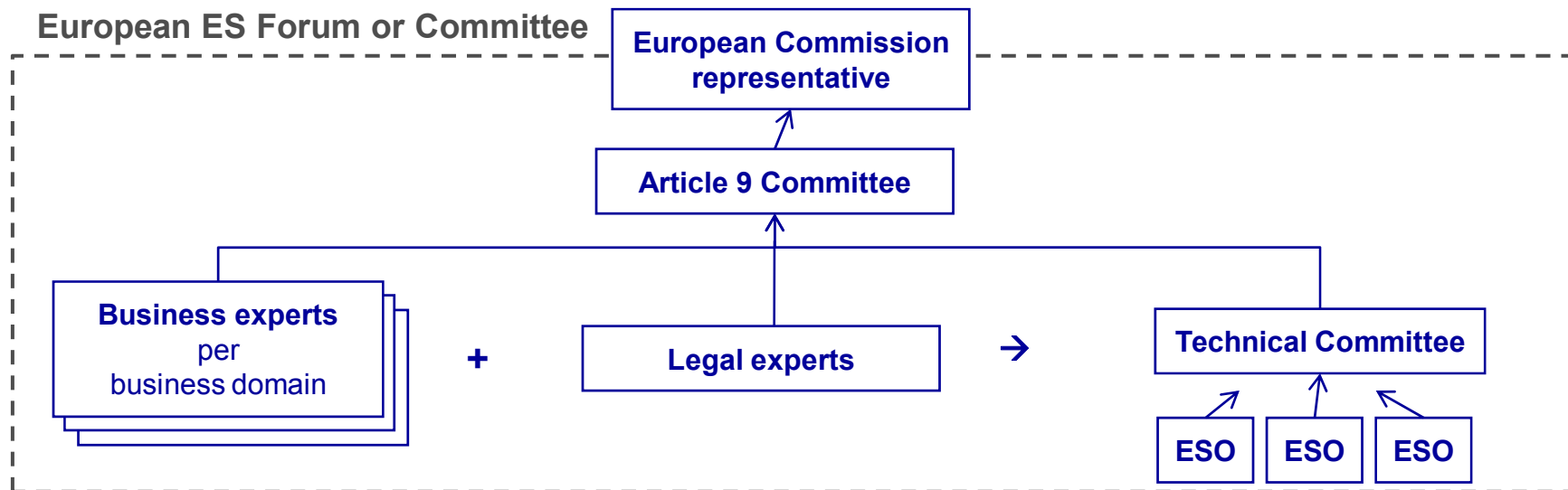
- Collect name and addresses of all accredited (art.11 1.c) **and** non accredited but supervised Qualified CAs from all Member States and EEA countries
- For each (group of) technical QCA from these supervised or accredited legal entities, collect the following information
 - Issuing CA identifying information (e.g., CN, O, C)
 - Certificate Policy identifier (CPS) and repository location (an English version should be at least available)
 - Presence of the ETSI TS 101 456 QCP+ certificate policy identifier in the end-user qualified certificates
 - Presence of the QCStatement extension in the end-user qualified certificates
- **May not be harmonised without finetuning of supervision/accreditation rules**
- Officially publish and maintain the list of all supervised and accredited QCAs with the above collected information per QCA

Standardisation recommendations

- Global reshaping of existing standardisation framework:
 - **Business needs + legal constraints**
= supporting technical specs
 - For all “electronic signatures products” (art 2.12) and covering AES (not only QES)
- Organised under the form of an European ES Forum or Committee
 - Organising the restructuring of the eSignature standardisation per ES product categories
 - Organising the appropriate referencing

Global re-shaping & reviewing of eSignature standards

Business drive (requirements) → within legal framework(s) → supported by technical specifications (standards)



Business needs

+

Legal constraints

→

Set of supporting technical specifications (standards)

Business needs
organised
around
**electronic
signature product
categories**
and
**per Business
domain**

+

**Generic legal
requirements** applicable
to all ES product
categories
and /or business domains

**Specific legal
requirements** per ES
category and/or
business domain

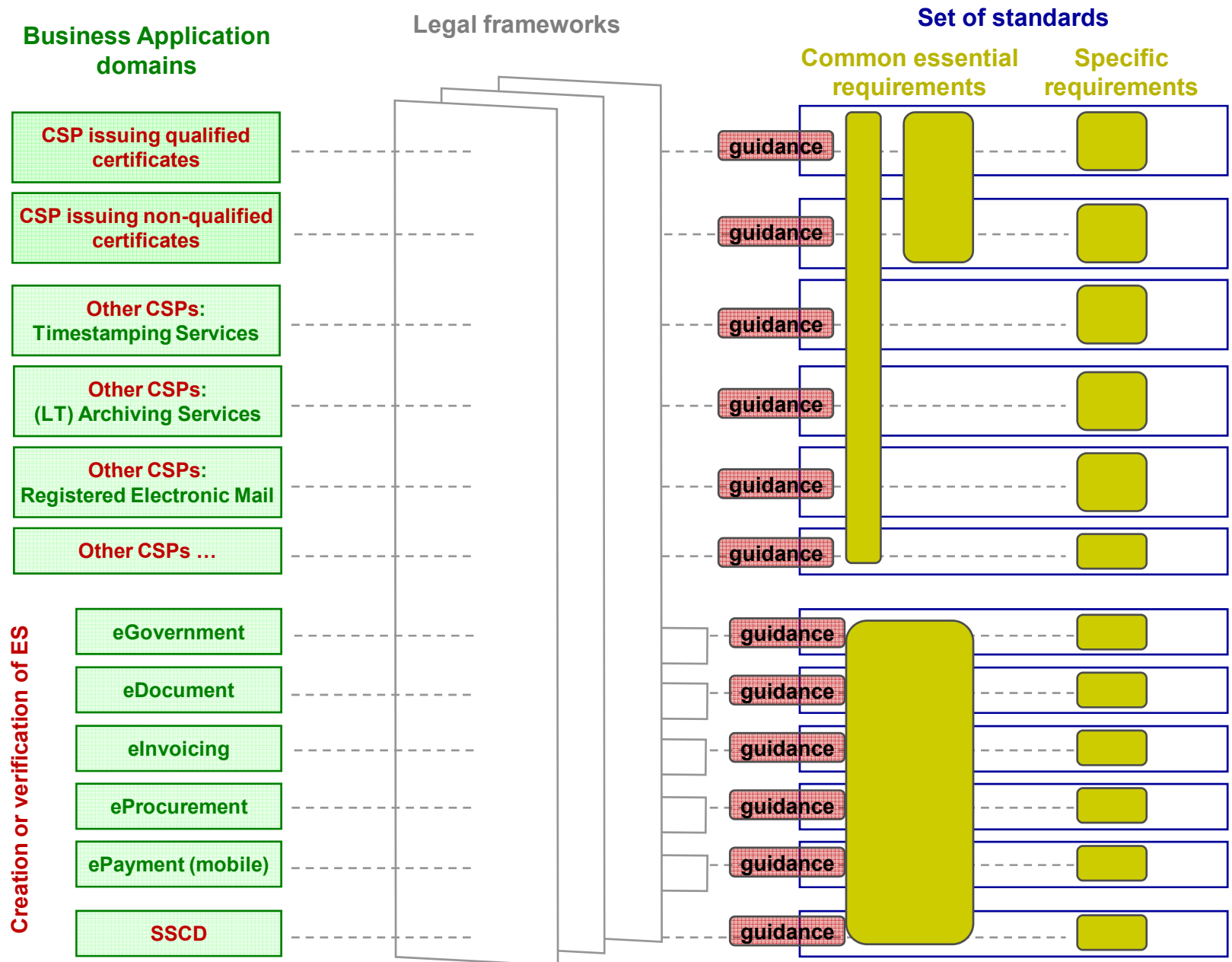
→

Common
essential
requirements

Specific
Requirements

- Organised per ES product category and/or business domain
- Under the form of appropriate quality ESO deliverables:
 - introduced by a straight-talking guide
 - rationalise, assessed and cleaned
 - with straight-talking implementation guidelines & examples

Global re-shaping & reviewing of eSignature standards



Business drive (requirements) → within legal framework(s) → supported by technical specifications (standards)

Marketing recommendations

- The European Commission to undertake the necessary marketing efforts for promoting the use of the European electronic signature standards
 - Within the EU in order to dynamize the full uptake of electronic signatures in the internal market, and
 - Outside of the EU (based on article 7.2), “in order to facilitate the legal recognition of advanced electronic signatures originating in third countries”)
- Considering the following principles:
 - Reduce complexity by focusing on key application areas
 - Economical viability: business case framework
 - Educate audiences to create visibility
 - Applications usability

Conclusions

- Global reshaping of existing standardisation framework:
 - Business needs + legal constraints
= supporting technical specs
 - For all “electronic signatures products” (art 2.12) and covering AES (not only QES)
- Recognition by Commission Decision referencing this new standardisation framework
- Quick wins on QES (to improve currently successful directive approach QCPs)
- Promotion by EC (marketing of ES and ESstandards)

Current next steps

- Facilitating cross-border use of
 - QES and AdES based on QEC for the signature purpose
 - QEC for identification purposes in specific context
- Further work on
 - Creating trust towards CSPs of other Member States and to the validation of signatures originating from other Member States
 - Gathering, publishing and keeping up-to-date some information about the supervised CSPs in Member States In the sense of Article 3.3 of the e-signatures directive (1999/93/EC)
 - Gathering and publishing information on Qualified Certificate Profiles, issued by the supervised QCSPs
 - Gathering information on signature formats used
 - Agreement on minimum requirements regarding ES formats, QEC profiles, use of supervised CSPs list in the context of specific or horizontal applications (e.g., Services Directive, eProcurement, ...)

Questions ? - Contact information



www.sealed.be



- *Sylvie Lacroix*
sylvie.lacroix@sealed.be
- *Olivier Delos*
olivier.delos@sealed.be
- *Patrick van Eecke*
Patrick.VanEecke@dlapiper.com
- *Wim Janin*
wim@one-agency.be