Welcome to the World of Standards

ETSI World Class Standards

Final Review Workshop. CSC phase 2, WP 3

Bernd Becker, Emmanuel Darmois, Anders Kingstedt, Olivier Le Grand,
Peter Schmitting, Wolfgang Ziegler

Brussels, October 1st, 2015

ETSI

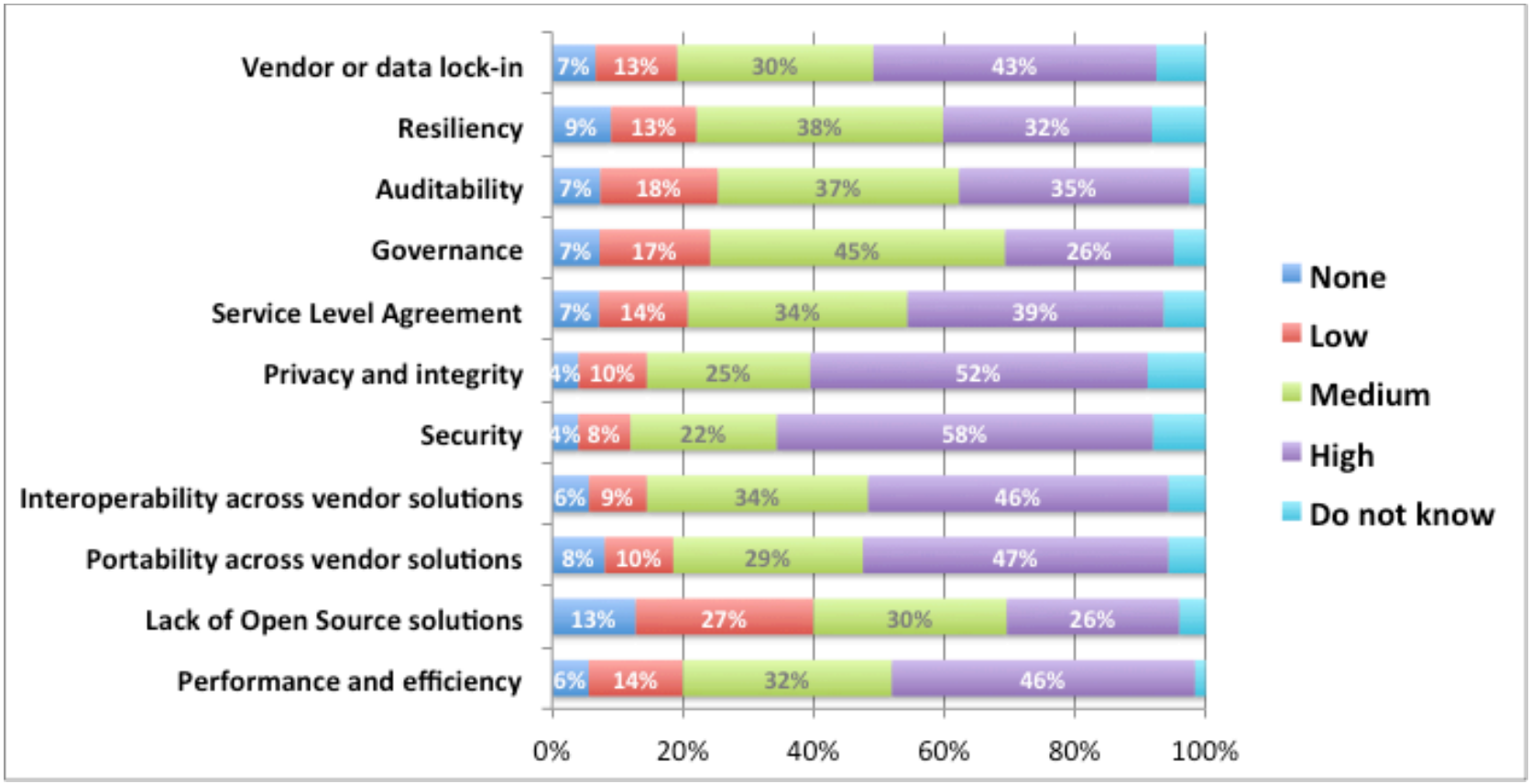
World Class Standards

CSC phase 2 – WP 3
Interoperability & Security in Cloud Computing

- **Presentation outline:**
  - **Report rationale and objectives**
  - **Background and backdrop**
  - **WP 3 – content**
  - **WP 3 – comments, overview**
  - **Conclusions and recommendations**
  - **Retro perspective**

WP 3- Report rationale and objectives

WP 3 backdrop



CSC Phase 2:
Interoperability and Security in Cloud Computing

Report objectives /are to/:

- Identify and present high-level user scenarios to explain and illustrate the relationship between interop and security;
- Identify and present “core concepts”;
- Present existing standards for interop and security;
- Make high level conclusions and recommendations;

Report rationale

- **Security** is listed as a top concern in the web survey report (re WP1)
- **Interoperability** is listed as top concern in the web survey report (re WP1)
- CSC phase 1 identified that security standards were becoming mature but “areas of concern” remained
- Security is a vast area with many different individuals elements and sub-domains to explore and potentially address in terms of availability of standards
- Interoperability exists at several levels and the applicability of interoperability might differ depending on scenario at hand

CSC Phase 2: Interoperability and Security in Cloud Computing

In scope for WP3

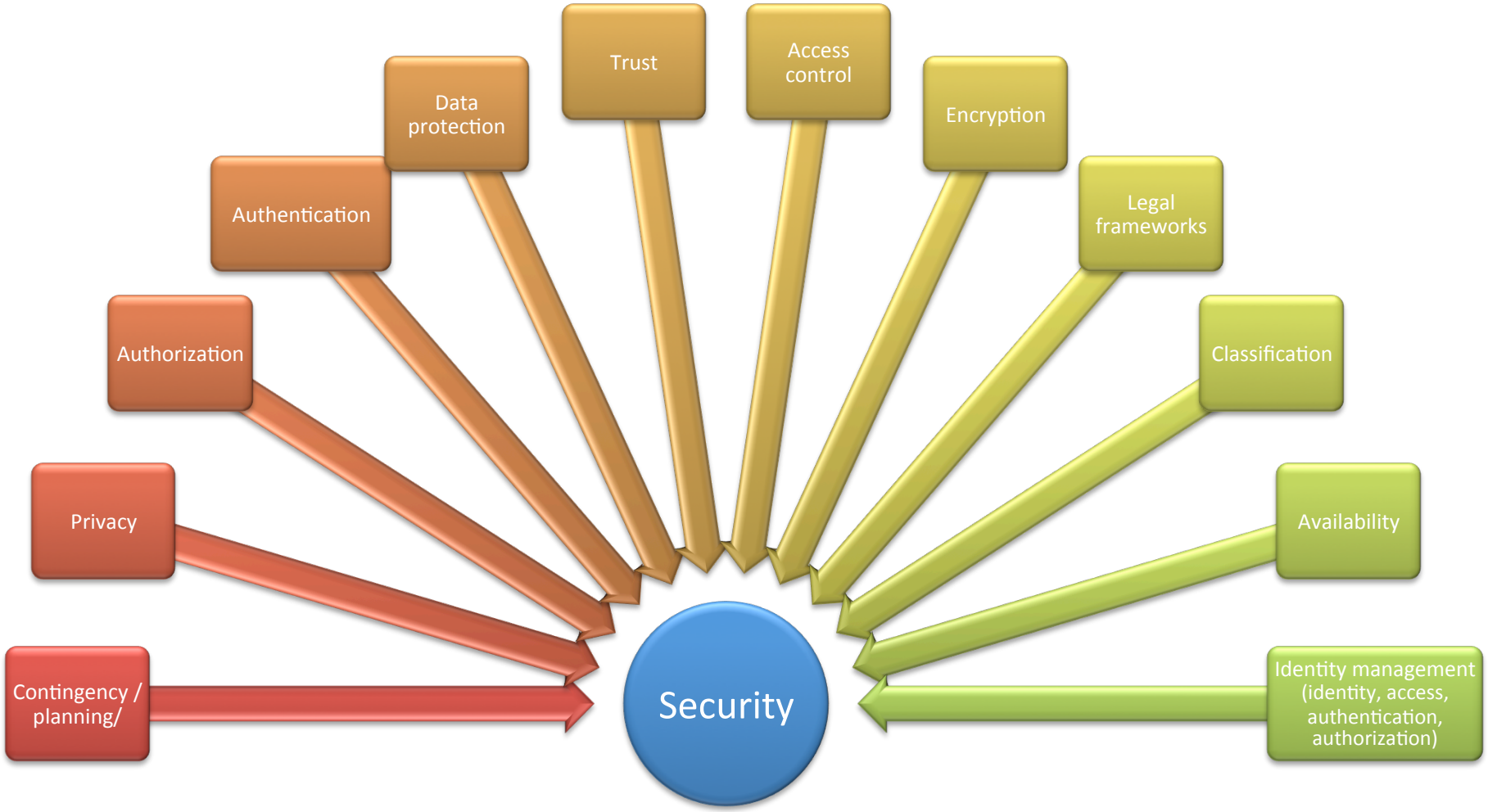
- To analyze the availability of Cloud Computing standards for security
- To analyze the availability of Cloud Computing standards for interoperability
- To identify gaps
- To describe individual areas / sub-domains within the security and interop domains
- To process and add approved suggestions received during the public consultation period (submitted as comments)

Out-of-scope for WP3

- In-depth analysis
- In-depth descriptions of elements / sub-domains of security and interop
- Exhaustive listing of technologies and standards
- Definition of security /aspects/ and interoperability

WP 3 - Background and backdrop

Backdrop:
Security – many aspects to consider



Backdrop:
Interoperability – many levels to consider

- **Levels of interoperability**
  - Different ways to express and tier interoperability exist
  - Commonly, more that one level is recognized
  - Typically, technical interoperability exist at the lowest level

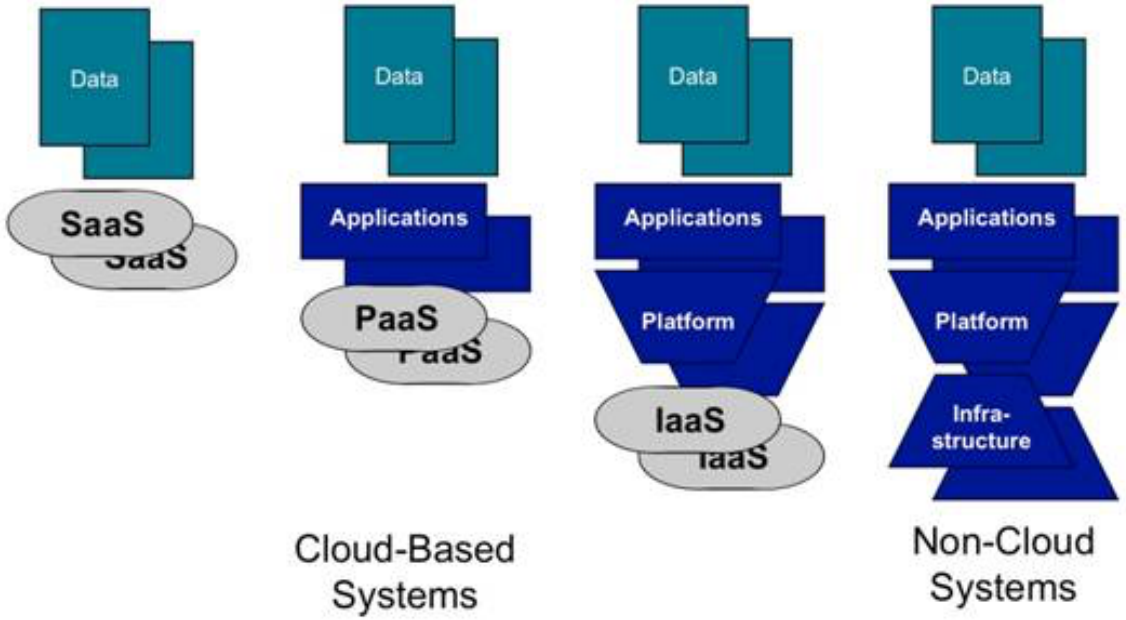
- **Example of interoperability frameworks**
  - EIF (European Interoperability Framework)
  - LISI
  - Open Group
  - …

WP 3 – Interoperability, backdrop

- **Example of models for interoperability**
- **Open Group:**

The cloud computing portability and interoperability categories to consider are:

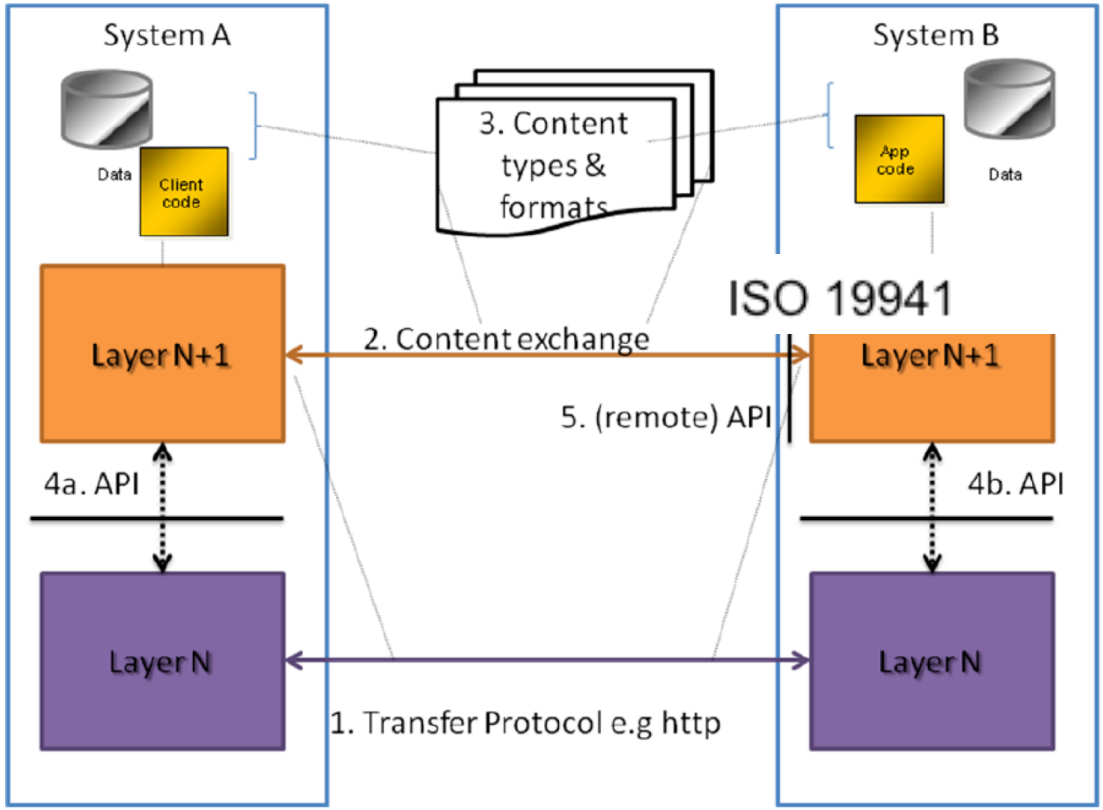
- Data Portability
- Application Portability
- Platform Portability
- Application Interoperability
- Platform Interoperability
- Management Interoperability
- Publication and Acquisition Interoperability



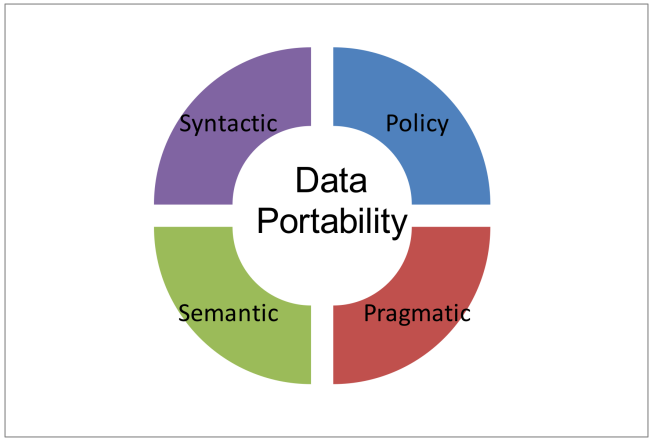
Open Group

WP 3 – Interoperability, backdrop

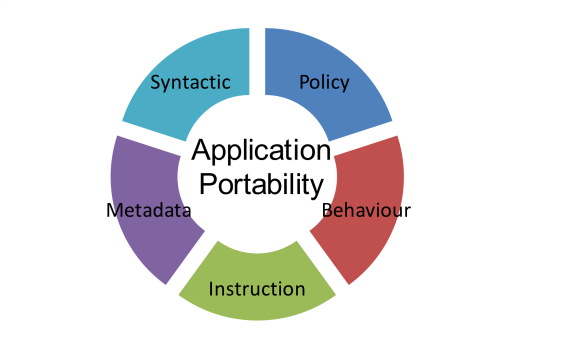
- Example of models for interoperability



ISO 19941



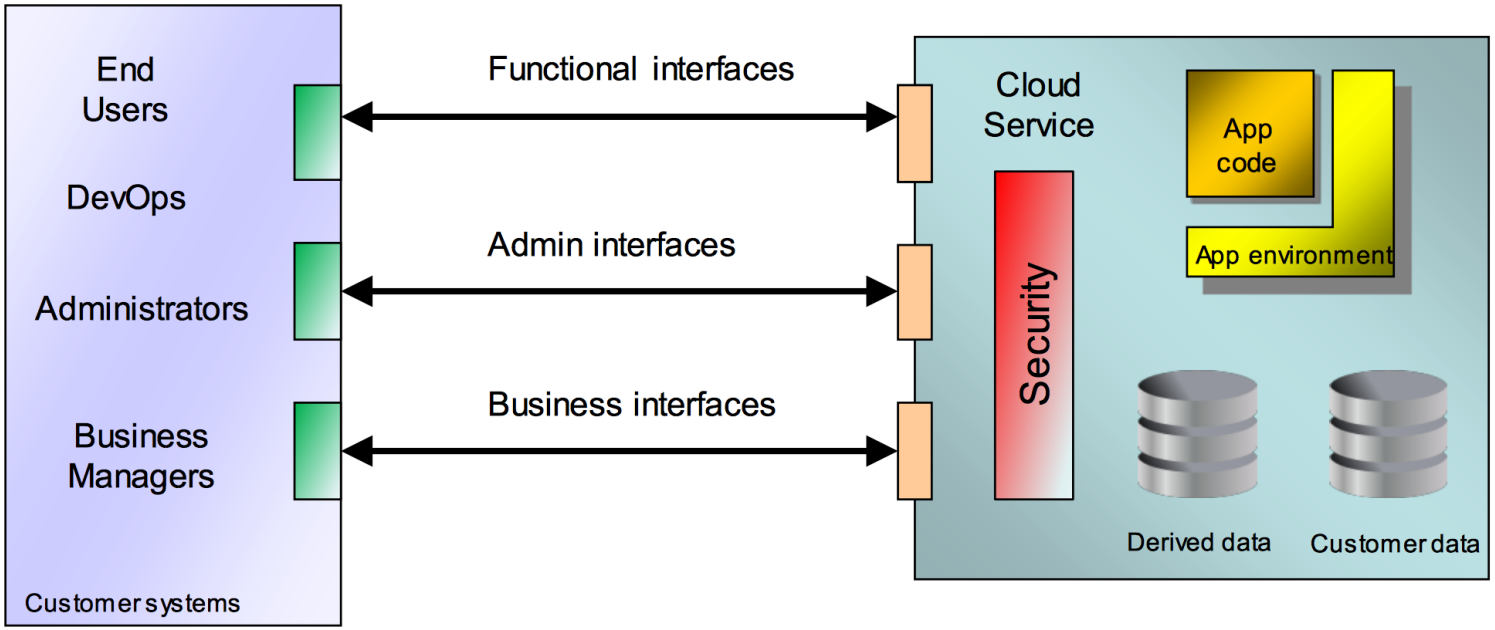
Four facets of data portability



Five facets of application portability

WP 3 – Interoperability, backdrop

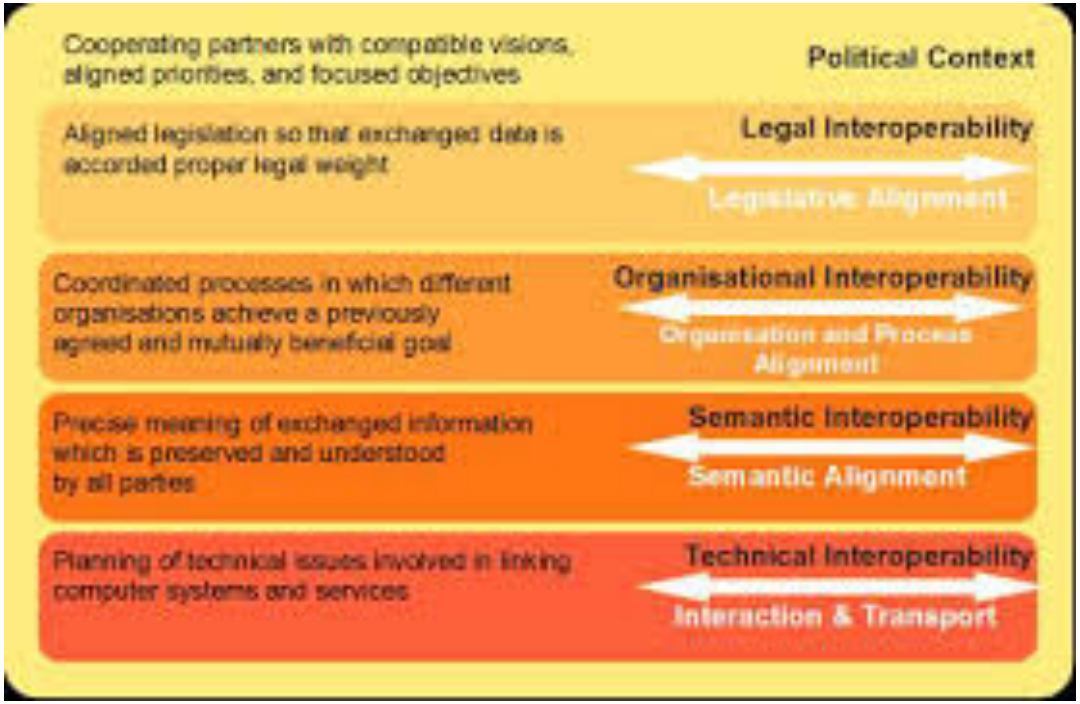
- Example of models for interoperability



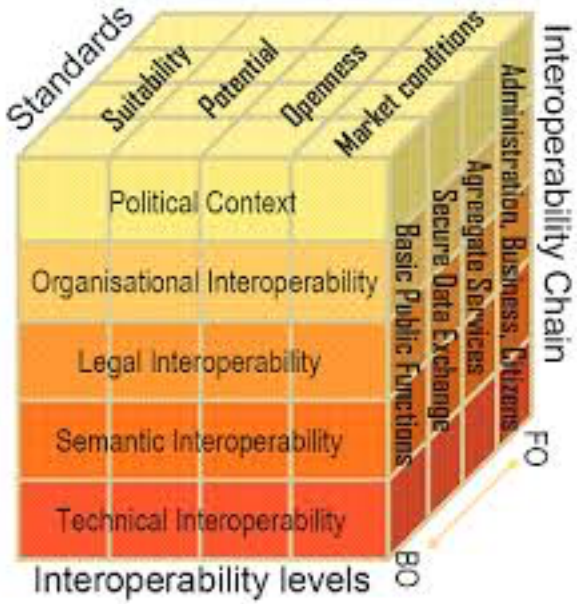
Cloud Standards Customer Council *

WP 3 – Interoperability, backdrop

- **Example of models for interoperability**



EIF



WP 3 – Content

WP 3 – Report content

- **Section 5 – High-level user scenarios interoperability and security**
  - Presented to illustrated some scenarios including use cases where interop and security are critical aspects to understand and consider
  - Places “core concepts”, i.e. cross-cutting aspect, in context
  - Might be used to understand how standards apply to the presented scenarios and the applicability of standards in the presented context

- **Disclaimer**
  - The presented scenarios do NOT represent a exhaustive list of scenarios and use cases where Cloud Computing interoperability and security come into play
  - The list of presented ”core concepts” might NOT be complete
  - Further detailed analysis and in-depth descriptions are probably needed

WP 3 – Report content

- **Scenario 1: Moving data from and between Cloud Computing Service providers**
- **Content**
  - The two uses cases included in the scenario involve the retrieval (CSP → CSC) and moving (CSP → CSP) of data belonging to a CSC
- **High level requirements**
  - CSLA in place, control of data (taxonomy, categories, classification), data protection schemes in place, well defined access and security policies.
- **Core concepts**
  - Data Integrity, Data Protection, Data Accessibility, Conformance, Interoperability (at several levels), Portability, Certification, CSLA.
- **Conclusions**
  - The scenarios exposes the complexity of interoperability and security. It also underlines the importance of strict policies, contracts and the governance of the CSLA.

WP 3 – Report content

- **Scenario 2: Retrieving Customer data in case of Service Provider failure**
- **Content**
  - The scenario looks at the emergency retrieval of a CSC's data in case of a contingency (such as major natural disaster, pressing financial difficulties, legal obligations or due to bankruptcy of the CSC).
- **High level requirements**
  - CSLA in place, control of data (taxonomy, categories, classification), data protection schemes in place, well defined access and security policies, well defined certification schemes (addressing contingency planning in particular).
- **Core concepts**
  - Data Integrity, Data Accessibility, Certification, CSLA.
- **Conclusions**
  - The contingency plan and a full understanding of legal the impliciations for CSP service delivery failure are key factors.

WP 3 – Report content

- **Scenario 3: Using on-premises identity management in the Cloud**
- **Content**
  - The CSC want to incorporate the access to cloud services using the current Single-sign-on (SSO) solution and wants to understand how IM related data is handled (on-premise or in the cloud).
- **High level requirements**
  - User data isolation, access control; CSLA incl. the required metrics (to be included in ISO/IEC 19086-2); data protection, access and security policies defined and enforced.
- **Core concepts**
  - Data Integrity, Data Protection, Conformance, Interoperability (at several levels), Portability, Certification, CSLA.
- **Conclusions**
  - To create reliable IM solutions that combine on-premise and cloud based solutions, isolation of CSC data, security and access control polices, data protection and data transfer protection mechanisms must exist and be continuously enforced (governed).

WP 3 – Report content

- **Scenario 4: Ensuring security in Hybrid Cloud environments**
- **Content**
  - This scenario relying on a “Hybrid Cloud” deployment model describes a very typical situation within companies of all size when Cloud Services get combined next to existing, own operated IT.
- **High level requirements**
  - Data categorization, classification, protection req’s considered, physical location in relation to legal frameworks, well defined access control and security policies, relevant certification(s) in place.
- **Core concepts**
  - Authorization, Authentication, Trust, Data Integrity, Data privacy, Conformance, Identity and Access Management, Interoperability, Certification.
- **Conclusions**
  - Moving to the cloud will affect and change the role of the IT department (from provider to “broker”).

WP 3 – Report content

- **Scenario 5: Ensuring portability and interoperability when migrating from a PaaS Cloud Service Provider to another**
- **Content**
  - The Cloud Service Customer (CSC) develops, tests and runs an innovative application using the PaaS services provided by a Cloud Service Provider (CSP). The CSC wants that the application can be deployed and run in other "target PaaS CSPs".
- **High level requirements**
  - Interoperability (at the required levels), application portability, certification
- **Core concepts**
  - Interoperability, Application Portability, Certification.
- **Conclusions**
  - The availability and use of standards for interop and portability will increase the probability of apps being portable between different PaaS. Conformance policies will assist in the verification of portability, but is also challenging to create and maintain.

WP 3 – Report content

- **Scenario 6: The Cloud as an hybrid innovation platform**
- **Content**
  - The cloud offers new and innovative ways to do R&D. The scenario describes how to tap into the power of the cloud and the need to be able to use the resources in a safe and reliable way, combining on-premise solutions with cloud services for R&D.
- **High level requirements**
  - Interoperability, confidentiality, data protection, security policy.
- **Core concepts**
  - Data integrity, Data privacy, Interoperability, Authentication, Certification, CSLA.
- **Conclusions**
  - The scenario underlines the importance of Trust (CSC → CSP). The protection of sensitive data is a key criterion for the set-up of a successful solution. Support for interoperability and a large range of protocols and data models is also necessary in a hybrid deployment model

WP 3 – Report content

- **Scenario 7: Conformance of Cloud Service Providers to Data Protection regulation**
- **Content**
  - The scenario illustrates the significant differences between the current data protection directive and the upcoming data protection regulation, highlighting some important aspects.
- **High level requirements**
  - Existing SLA's must be analyzed and most likely updated / replaced to reflect the new terms laid out in the regulation (such as PII requirements, data breach processing / mgmt. and more)
- **Core concepts**
  - Data protection, Data privacy, Trust, CSLA
- **Conclusions**
  - Certification schemes that address and ensure compliance with the regulation will probably assist both CSP's and CSC's. The goals of a strengthen data protection for citizens will create the need to amend contracts and SLA's.

WP 3 – Report content

- **Scenario 8: CSLA in brokered, multi CSP use cases**
- **Content**
  - A CSC has procured a cloud service offered by a CSP that in turn comprises and uses cloud services provisioned by several other CSP's.
- **High level requirements**
  - Understanding the role and responsibilities / requirements of the CSC and the CSP sub role "cloud service broker" (CSB) and how these map to and impact the composition of the CSLA is key.
- **Core concepts**
  - Data Integrity, Data Protection, Data Accessibility, Conformance, Interoperability (at several levels), Portability, Certification, CSLA.
- **Conclusions**
  - The inherent nature of cloud computing where cloud services are combined in various ways underscores the need for understanding, defining and ensuring the contract related obligations of several cloud actors.

WP 3 - Content

- **Section 6 – Core concepts**
  - This section elaborates on the core concepts that were introduced in section 5.
  - The core concepts presented are:
    - Interoperability
    - Portability
    - Security (with sub topics)
    - Cloud Service Level Agreement (CSLA)
  - The relationship and dependencies between core concepts is highlighted
- **Disclaimer**
  - The presented core concepts are most likely neither complete, nor is the definitions offered exact or in some cases even not entirely accurate (as seen in some of the comments received)
  - Further alignment, detailed analysis and in-depth descriptions are probably needed

WP 3 - Content

- **Section 7 – Standards, certifications and frameworks for interoperability and security**
  - This section lists the applicable security and interoperability standards and certification schemes
  - The listing presents general and Cloud Computing specific standards
    - Available
    - Under development
- **Disclaimer**
  - The list probably needs further work to make it complete

WP 3 - Content

- **Section 8 – Conclusions and recommendations**
  - This section presents some conclusions made during the development of the report, based on previous conclusions (in CSC phase 1) and the result of the web survey (re WP 1)
  - The conclusions highlight concerns divided into “risks”, “outstanding gaps” and “awareness, dissemination and marketing”.
- **Disclaimer**
  - The recommendations made are highlevel in nature and further work to establish concrete action plans is most likely required.

WP 3 – Comments overview

WP 3 – Comments overview

- **A large number of comments received**
- **Different classes of comments exist**
- **Comments categories - initial observations:**
  - Alignment of the terms and concepts is needed
    - Some concepts are not consistently used and different definitions exist in the report
  - Many submitters are asking for more in depth information
  - Some commenters have not understood the intention of the report

WP 3 – Comments overview

- **A large number of comments received**
- **Different classes of comments exist**
- **Comments categories - initial observations:**
  - Alignment of the terms and concepts is needed
    - Some concepts are not consistently used and different definitions exist in the report
  - Many submitters are asking for more in depth information
  - Some commenters have not understood the intention of the report

WP 3 – Comments overview

- **More that 200 comments received (tentatively 240)**
- **Individual comments (examples):**
  - Gaps are not clearly identified and described (OFE)
  - The goal of the report is not clearly understood (OFE)
  - The use cases presented should be elaborated (SICS Swedish ICT)
  - Expand the data protection section and elaborate on data encryption use cases (CAS Software AG)
  - Provide technical recommendations on how to avoid data exposure (SixSq)
  - Expand on data aspects (data taxonomy, classification, categorization etc.) and use the terms consistently when discussing data protection (CAS Software AG).
  - Several suggestions related to inconsistent use of terms (e.g. “access management” instead of “identity management” (TECNALIA)
  - The report doesn’t offer any conclusions on the impact of the upcoming EU Data Protection Regulation and should focus on existing national legislation (Cloud Security Alliance, CSA)
  - The Federation of CSPs warrants a separate scenario entry (FP7 EUBrazil Cloud Connect project)
  - The issue of “data portability” is not mentioned in the report (OFE)
  - Some important security areas are not covered by the report, such as “incident management, business continuity / disaster recovery, mobile security” (CSA)
  - The concept of “accountability” needs to be further explained (A4Cloud Project)
  - The concept of “context awareness” is not included (CAS Software AG)
  - The classification of standards is not logical and should be changed (CSA)
    - note: proposal included
  - Security standards are missing (CSA)
    - note: missing standards are included in the comment

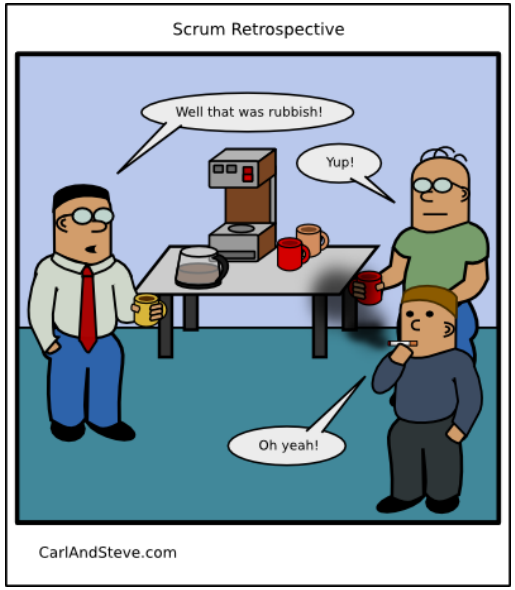
WP 3 – Conclusions

WP3 Report
Interoperability and Security

Conclusions

- **Risks**: Unless the main stakeholders of Cloud Computing can continue the efforts needed to develop and map existing standards to Cloud Computing, the overarching risk is that the potential Cloud Computing users will hold back.
- **Outstanding gaps**: Gaps still exist in many areas, like interoperability and portability standards that will allow CSCs to effortless move their data and applications between different CSPs' services offered on various Cloud platforms. The significance of national, regional and global legislations that restrict and govern the use of personal and/or corporate data must also be fully understood and addressed.
- **Awareness, dissemination and marketing**: Awareness, dissemination and marketing of Cloud Computing standards, certification schemes and available solutions is probably one of the key efforts necessary to propagate and encourage the use of Cloud Computing. Existing and already available solutions that address the concerns should be communicated to Cloud Computing stakeholders.

WP 3 – Retrospective



WP 3 – Retrospective

- **Great interest in the report!**
- **Insufficient time spent on the report**
- **The security terms (in particular) used and referenced are not fully aligned and are sometimes not correctly used / applied in the context they're shown**
- **The goal of disclosing existing gaps is not fulfilled in the report**
- **"Pandoras box" syndrome – is the topic too complex?**
  - Both Interoperability as well as Security are complex and difficult topics. It would probably be worth to consider a follow-up, in-depth analysis of both topics, separately or in relation to each other.
- **The "disclaimer" in the report (section 9) stands; areas to be considered for improvement are:**
  - "*Clarification of the scenarios used for identification of core concepts;*
  - *Expansion of the discussion on the relationship between core concepts;*
  - *More precisions on the list of Standards, Certifications and Frameworks in section 7;*
  - *More (scoped) recommendations.*"