Deloitte.

Online/Cloud Services Trust challenges & eIdentity-aspects

Erik R. van Zuuren,
Director Deloitte AERS Belgium

Global Forum
Brussels Nov 07/08, 2011

Agenda

Weather Forecast…

Trust & Sustainability

eIdentity & eAuthentication

Reliability & Certainty

Online & Cloud Services - Weather Forecast

- Key operational and governance issues to consider as online & cloud services are deployed…

Data controls and ownership	Who will own the data when subscribing to a cloud computing service.? Is the data you create, use, and store within a cloud yours? Could your data be viewed, accessed, or used without your knowledge; sold to third parties; used for unknown purposes?
Backup, retention, and disposal	Is data retention meeting your policy requirements? Is deleted data "really" gone or still preserved somewhere within the cloud? How are data backups and restores handled?
Availability and reliability	How is reliability, access, and availability "guaranteed" by cloud services providers? Is it through service level agreements?
Business Continuity & Disaster recovery	Is your data protected in the event of a disaster? What are the recovery time objectives and service level agreements?
Legal compliance	Is your cloud provider adhering to laws/regulations for your industry and in every jurisdiction which applies?
Assurance	How will you provide your customers with a level of comfort and assurance on the protection and controls in the cloud environment, especially when involving third parties?
Scalability	Can your service provider support growing demand from all clients and provide reliable services at high scalability? Are there vendors with mature offerings?
Security and encryption	Is data secure within the cloud environment? How is security enforced and confirmed? What level of encryption is required to enhance security, and how will this impact operational service levels?
User management & Access Controls	How can the user (corporate users, partners, clients) gaining access to the platform be uniquely identified. How should an organization's IAM-system integrate /federate with that of one or more service providers?
Auditing and monitoring	Are you ready to apply enterprise risk management and controls, and auditing and monitoring practices to applications and data residing in cloud environments?

Deloitte.

Online & Cloud Services - Trust & Sustainability

- Online & Cloud Services need to be sustainable and can / will only be accepted if they can be fully trusted by all parties:

  - Sustainability / Reliable for all parties involved:
    - "Information Service" Providers (Government, Private Sector, …)
    - "Trust Service" Providers (Government, Private Sector, …)
    - Relying Parties (Enterprizes, Citizens, ….)

  - Sustainability:
    - Truly Value Adding Services – Clear Benefits (Time, Quality, …)
    - User Friendliness – Usability anywhere / anytime / any device
    - Reliability / Solidity – Trust / Governance / Architecture & Standards / Operations

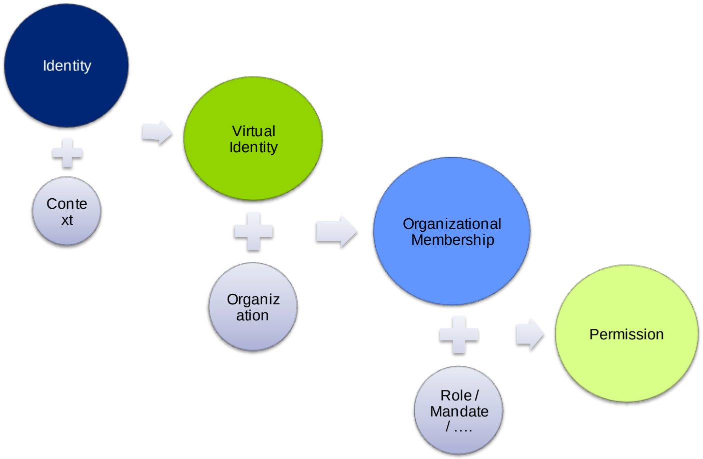
  - Trust:
    - Perception of Security ?
    - Some sort of Privacy ?
    - Presence of Quality Seals ?
    - Existence of Assurance Levels?
    - Presence of Legal Certainty ?

Deloitte.

Online & Cloud Services - eIdentity & eAuthentication

- Any access should be subject to the principles of "need-to-know", "need-to-have" in combination with a sufficiently strong proof of "identity" and relevant "characteristics" or "mandate".

  - What is a Trusted Identity?
  - What is a validated Quality? Characteristic?
  - What are the requirements wrt "Mandates"?
  - What determines the strength of a Credential?
  - Is a Credential linked to virtual/digital identity or to identity + quality or ….?
  - What about cross-border "recognition" of identities / characteristics / mandates ?
  - What about (secured) usability of a credential anytime / anywhere?
  - Virtual / Mobile digital identities acceptable?

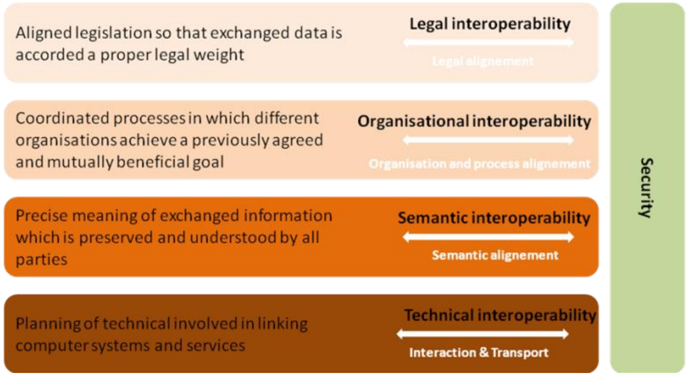


Deloitte.

Online & Cloud Services - Reliability & Certainty

- Relying Parties must have sufficient guarantees that the information they rely on is trustworthy and can be used for further processing.

  - Which is the authentic or an authoritive source of information?
  - How to ensure (cross-border) interoperability / certainty of information?
  - What are the trust / quality / security requirements for any source?
  - Need for quality seals & accreditation schemes?
  - Legal certainty (incl privacy guarantees) with regard to the information given/shared?
  - What about "incident" management & continuity?
  - Liability-settlement in case of "incidents"?



Aligned legislation so that exchanged data is accorded a proper legal weight

Legal interoperability — Legal alignement

Coordinated processes in which different organisations achieve a previously agreed and mutually beneficial goal

Organisational interoperability — Organisation and process alignement

Precise meaning of exchanged information which is preserved and understood by all parties

Semantic interoperability — Semantic alignement

Planning of technical involved in linking computer systems and services

Technical interoperability — Interaction & Transport

Security

Interoperability levels (source: EIF)

Deloitte.

Erik R. van Zuuren
evanzuuren@deloitte.com

Deloitte Enterprise Risk Services
Direct: + 32 2 800 22 99
Main: + 32 2 800 22 57