Context-based identity management: a reality and necessity for online and cloud services

Erik R. van Zuuren,
Director Deloitte AERS Belgium

Trust in the Digital World
18-19 April, Brussels, Belgium
Agenda

Some Vocabulary

Weather Forecast

Reality check

eIdentities

Authorisations

Enforcement

...
Online & Cloud Services – Some Vocabulary

- The “old” world:
  - Certificate Authorities
  - Identity/Attribute certs
  - Relying Parties
  - Subscribers

- The “new” era:
  - “Identity” Providers
  - Identity/Attribute assertions
  - Service Providers
  - “Users”
## Key operational and governance issues to consider going into the cloud...

<table>
<thead>
<tr>
<th><strong>Business Case / Sustainability</strong></th>
<th>Is there a business case? Can we build/establish the targeted environment cost-effectively? Can we establish the targeted environment in such a way which is considered user-friendly for and trusted by the targeted audience?</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data controls &amp; ownership</strong></td>
<td>Who will own the (identity-)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?</td>
</tr>
<tr>
<td><strong>Availability &amp; reliability</strong></td>
<td>How is reliability, access, and availability &quot;guaranteed&quot; by cloud services providers? Is it through service level agreements?</td>
</tr>
<tr>
<td><strong>Business Continuity &amp; Disaster recovery</strong></td>
<td>Is your data protected in the event of a disaster? What are the recovery time objectives and service level agreements?</td>
</tr>
<tr>
<td><strong>Legal Aspects &amp; Privacy</strong></td>
<td>Is your cloud / service / identity provider adhering to laws/regulations for your industry and in every jurisdiction which applies? Both for the “data” and with regard to the Identities?</td>
</tr>
<tr>
<td><strong>Risk Mngt &amp; Assurance</strong></td>
<td>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?</td>
</tr>
<tr>
<td><strong>(Ease of) Scalability</strong></td>
<td>Can your service provider support growing demand from all clients and provide reliable services at high scalability? Are there vendors with mature offerings?</td>
</tr>
<tr>
<td><strong>Security (Mngt &amp; Ops)</strong></td>
<td>Is data secure within the cloud environment? How is security enforced and confirmed?</td>
</tr>
<tr>
<td><strong>User management &amp; Access Controls</strong></td>
<td>How can the user (corporate users, partners, clients) gaining access to the platform be easily and uniquely identified. How should/could an organization’s IAM-system integrate /federate with that of one or more service providers… or identity providers?</td>
</tr>
<tr>
<td><strong>Auditing and monitoring</strong></td>
<td>Are you ready to apply enterprise risk management and controls, and auditing and monitoring practices to applications and data residing in cloud environments?</td>
</tr>
</tbody>
</table>
Online & Cloud Services – A real example

Private Sector Online / Cloud Services > more than one “context”!

Legal Counsel

Compliance Control

End User

Managers

Internal (B2E) Perspective

Local Client Admin

Client End User

Client’s system

External (B2C/B2B) Perspective

Authorities

Privileged Parties

© Deloitte. All rights reserved.
Online & Cloud Services – A real example

Government Online / Cloud Services > more than one “context”!
Online & Cloud Services - eIdentities

For any access a sufficiently strong proof of “identity” needs to be provided and “context” be established.

- What is a Trusted Identity?
- What distinguishes Qualities/Capacities?
- Which are the relevant Characteristics?
- Is a credential linked to virtual/digital identity or to identity or ....?
- What about (cross-border) “recognition” of capacities / qualities?
Online & Cloud Services - Authorisations

Any access should be subject to the principles of “need-to-know” and “need-to-have” and be based on a sufficiently strong proof of “identity” and relevant/trusted “characteristics” or “permissions”.

- Which (types of) permissions can be granted to which context?
- What about cross-border “recognition” of “mandates”?
- Do we need to parametrize roles/authorisations?
Applying context-aware identities in the real world >> need for attribute based policy enforcement?

- **EX1** > When accessing files, authorized officials can see/manage all records, architects can only submit/manage records of their clients and citizens/enterprises can only access their own files.

- **EX2** > Client-records-typeX can only be seen by regional managers of our company linked to this client with a “high” clearance OR by explicitly for this task appointed client-side employees.

- **EX3** > Patient-records-typeX are only available to physicians or nurses working at hospitals in the patients region except in cases of life-threatening situations.
Online & Cloud Services - The journey goes on...

- Legal, Organisational, Semantic, Technical Interoperability...

- Which is the authentic or authoritative source of identity/attribute information?

- How to ensure (cross-border) interoperability / certainty of "claims"?

- Legal certainty (incl privacy guarantees) with regard to the information given/shared?

- What about audit trailing?
- What about incident management & continuity?
- What about liability-settlement in case of "incidents"?

Interoperability levels (source: EIF)