ORGANIZATIONAL ADOPTION OF PRIVACY ENHANCING TECHNOLOGIES (PET)

John Borking
**Vision:** Users can act securely and safely in the Information Society while keeping sovereignty of their private sphere.
CENTRAL QUESTIONS

• WHEN STARTS AN ORGANIZATION BOTHERING ABOUT PRIVACY

• WHAT FACTORS AFFECT AN ORGANIZATION’S DECISION TO INTRODUCE PET

• IS THERE IS AN ORGANIZATIONAL ADOPTION PROBLEM FOR PET?

• DRIVERS AND INHIBITORS FOR ADOPTION BY ORGANIZATIONS OF PET
DEFINITION OF PET

PET IS A SYSTEM OF ICT MEASURES PROTECTING THE INFORMATIONAL PRIVACY BY:

1. ELIMINATING OR
2. MINIMIZING PERSONAL DATA OR
3. PREVENTING UNNECESSARY OR UNWANTED PROCESSING OF PERSONAL DATA, WITHOUT LOSS OF FUNCTIONALITY
For the implementation of PET, certain maturity of the organization is required. It is highly unlikely that immature organizations will implement PET, let alone that these organizations have any awareness of privacy protection. The level of maturity for IAM is a strong indication for the introduction of PET in an organization.
“a staged structure of maturity levels, which defines the extent to which a specific process is defined, managed, measured, controlled and/or effective, assuming the organization develops and adopts new processes and practices, from which it learns, optimizes and moves on to the next level, until the desired level is reached.”

Existing models: CMMi (SE Carnegie Mellon), Nolan Norton, INK (EFQM)....
IAM topology with organization class segments for maturity

<table>
<thead>
<tr>
<th>Top Class</th>
<th>Authentication requirements based on continuous risk analysis and are continuously adjusted</th>
<th>Central real-time controlled authorization sources, automated procedures</th>
<th>Role Based Access Control for all applications and continuous updated authorizations</th>
<th>Automated and reliable for multiple sources</th>
<th>Full responsibility to AO/IC with periodic reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pre-Active</td>
<td>Authentication Requirements based on continuous risk analysis</td>
<td>Central registration, controlled authorization processes, manual procedures</td>
<td>Role Based Access Control used for critical applications</td>
<td>Limited Automated and reliable for multiple sources</td>
<td>Full responsibility to AO/IC</td>
</tr>
<tr>
<td>Active</td>
<td>Authentication Requirements based on one time survey</td>
<td>Central registration, Limited user group, manual procedures</td>
<td>Authorization matrices are updated periodically</td>
<td>Limitd Automated but reliable processes locally</td>
<td>Partial delegation of responsibility to AO/IC</td>
</tr>
<tr>
<td>Starting-up</td>
<td>Arbitrarily formulated authentication requirements (authentication means are provided, adjusted and deleted on user request)</td>
<td>Entries can be double but they are consistent</td>
<td>Authorization matrices defined but are not updated</td>
<td>Limited Automated unreliable processes locally</td>
<td>Sporadically delegated responsibility of AO/IC</td>
</tr>
<tr>
<td>Immature</td>
<td>No authentication means</td>
<td>Double and inconsistent entries because of ad-hoc and ad-hoc processes</td>
<td>No authorization matrices, authorization is defined ad-hoc</td>
<td>Manual process locally</td>
<td>No responsibility delegated into a AO/IC organization</td>
</tr>
<tr>
<td></td>
<td>Authentication Management</td>
<td>User Management</td>
<td>Authorization Management</td>
<td>Provisioning</td>
<td>Monitoring/Audit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Organization
<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
</table>
| Initial    | Activities are ad hoc, with:  
|            |   • No defined policies, rules, or procedures.  
|            |   • Eventually lower-level activities, not coordinated.  
|            |   • Redundancies and lack of teamwork and commitment.  |
| Repeatable | The privacy policy is defined, with:  
|            |   • Some senior management commitment.  
|            |   • General awareness and commitment.  
|            |   • Specific plans in high-risk areas.  |
| Defined    | The privacy policy and organization are in place, with:  
|            |   • Risk assessments performed.  
|            |   • Priorities established and resources allocated accordingly.  
|            |   • Activities to coordinate and deploy effective privacy controls.  |
| Managed    | A consistently effective level of managing privacy, privacy requirements, and considerations is reflected in organization, with:  
|            |   • Early consideration of privacy in systems and process development.  
|            |   • Privacy integrated in functions and performance objectives.  
|            |   • Monitoring on an organizational and functional level.  
|            |   • Periodic risk-based reviews.  |
| Optimizing | Continual improvement of privacy policies, practices, and controls, with:  
|            |   • Changes systematically scrutinized for privacy impact.  
|            |   • Dedicated resources allocated to achieve privacy objectives.  
|            |   • A high level of cross-functional integration and teamwork to meet privacy objectives.  |

— Source: Hargraves et al 2003
S- CURVES MATURITY IAM & PRIVACY

Nolan Norton stages of growth model

Maturity Privacy protection

Maturity IAM Processes

Decision area for further growth
Towards a Typology: Which Organizations?

<table>
<thead>
<tr>
<th>Need</th>
<th>Ability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>Low</td>
</tr>
</tbody>
</table>

PRIME Focus
Organizational Adoption of PET
Results of Interviews and Case Analysis by category

Factor I: Characteristics of PET

Positive:
+ Relative Benefit
+ Role of advisory institutions

Negative:
- Costs
- Compatibility
- Complexity
- PET woven into business processes
Results of Interviews and Case Analysis by category

Factor II: Internal Organizational Characteristics

Positive
+ Perception and level of awareness of privacy regulation
+ Type of Data processed (e.c. risks incurred)
+ Individual Ties with advisory institutes
+ Presence of Key persons

Negative
- Complexity of organizational processes
- Structure and size of the organization
- Diversity in Information Systems
Results of Interviews and Case Analysis by category

Factor III: External Organizational Characteristics

Positive
+ Pressure by privacy legislation
+ Existing offer of PET measures

Negative
- Complexity of privacy law
- Private versus Public organizations
QUESTIONS?

• Thank you