

Identity Management at the Danish Authorities

Expert-Talk Vienna 18th October 2007

devoteam
consulting ↑

Expert Talk
@ devoteam consulting

Who am I?



Bjørn Mose

- Age: 49 years
- Education: Master of Science Computer technology, Copenhagen University
- CISA – Certified Information Systems Auditor

Job at Devoteam Consulting A/S, Denmark

- Devoteam Consulting title: Senior Consultant
- Employed in company for more that 13 years
- Working experience, security: 15+ years

Primary working areas:

- Security
 - Identity Management
 - Security Architecture
 - Contingency planning
 - Security Management

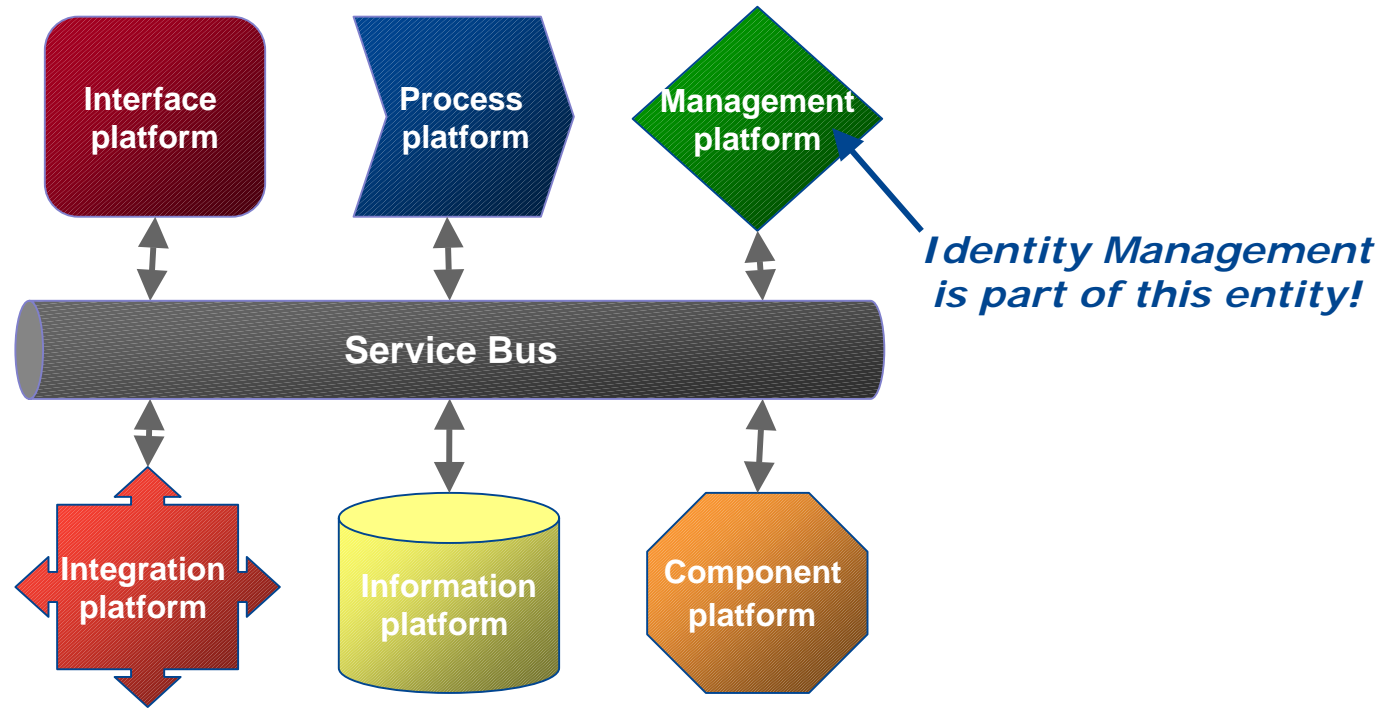
- The Directorate for Food, Fisheries and Agri Business supports development and production in the entire food industry in Denmark and contributes to the formation of policies of The Ministry of Food, Agriculture and Fisheries.
- They support development and production in the food industry in order to:
 - promote the sale of healthy and secure food
 - show consideration to the environment of nature in the production of food
 - boost the competitiveness of the food industry.
- The directorates activities include:
 - metering out subsidies to farmers and fishermen
 - administration of the Law of Land Holdings
 - administration of the law of land consolidation and acquisition of land
 - check the grantees and **the administration of subsidies**
- **The directorate pays out just about 10,5 billion DKK (1.4 billion €) in subsidies to farmers, fishermen, companies in the food business, research institutions, etc. A little more than 9,5 billion DKK (1.3 billion €) are financed by the EU.**
- Staff of approximately 400, directorate with head office in Copenhagen and an office in Tønder in Jutland

Scope

- The Common Agricultural Policy (CAP) reform in 2003 -> New requirements to the administration of the subsidies.
- Denmark adopted the reform in January 2005 -> The Directorate for Food, Fisheries and Agri Business implemented a temporary IT solution in order to support the reform.
- To improve service and efficiency, the Directorate wanted to implement a new solution in 2008-2009.

General requirements

- Customer and employees at the Directorate are all users in the new solution.
- Service Oriented Architecture (SOA)
- Initially 35.000 registered users
- Able to manage up to 100.000 registered users
- Able to handle request from 2.000 concurrent users (peak)



- The Identity Management part of the solution is only one of several sub-components in the Management platform.
- The interface between the Management platform and the rest of the system is primarily the Service Bus.

- Distributes user administration
- Support handling of different kind of actors (>10)
- Support handling of different kind of roles (>10)
- Support the use of authority
- Support SSO to other systems
- Segregation of duties in the workflow system
- Rights limited in time or limited by external conditions or by number of use
- Instantly change of users rights when roles are withdrawn or changed
- Authorisation system with workflow support
- Advice to people in charge when rights related to a role are changed.
- Support of non-repudiation

- The (security) solution should be available as a set of services

- Compliance with standards:
 - Web Single Sign-on - SAML, Liberty Alliance Project, .NET Passport
 - Access control – XACML
 - Provisioning – SPML
 - Web Service Security - WS-Security
 - Directory Services - LDAP, DSML, X.500-series

- User authentication using:
 - Public Certificate (X.509)
 - User-id/password
 - Corporate network sign-on
 - Federation

- Configurable password requirements

- Support of information classification of systems, services and data
- Services and interfaces must have assigned a classification level
- Logging and monitoring:
 - Full traceable handling of all interactions
 - Monitoring of key parameters and security settings
- System should support alerts based upon user defined limits.
- Compliance with national and international (EU) legislation

IBM

- Solution is based upon Websphere Portal, which is an 2EE Enterprise Application, which supports all J2EE standards and the Portlet standard JSR 168. Supports furthermore WSRP and Struts (MVC) software.
- Login and user profile is handled by Tivoli Access Manager. Only standard user profile information is supported by the LDAP solution.

WM-Data

- Solution is based upon Oracle Application Server Portal 10g. Complies to J2EE std. JSR 168, WSRP, JavaScript, WebDAV, SOAP and WS. Oracle DBMS is required.
- Login and user profiles are handled by COREId which support all requirements except e-mail notification. Uses SSO based upon Windows Native Authentication and Kerberos tickets and certificates.

Ementor [selected integrator & vendor]

- Basen upon a pure Microsoft products, with additional Web parts developed by Ementor. Do not support Portlet standard. Difficult to integrate in a non-Microsoft environment. Do not support WSRP 1.0.
- User profile management using Microsoft AD, which has some limitations.

- Do not develop your own IMS.
- In case you do have a pure Microsoft environment – think once again: Do I really need an Identity Management system?
- Do not expect to use SSO on every single system you have.
- Do not go for the “Big Bang” implementation. Take one small step at a time.
- Federation is smart, but local users are much easier to implement.
- Use a centralized log-function in order to be able to overlook your IMS.



Expert Talk @ devoteam consulting



Thank you for your attention!



UNITED ARAB EMIRATES
UNITED KINGDOM

© Devoteam Consulting A/S.
This document is not to be copied or reproduced in any way without the express permission of Devoteam Consulting.

CONTACT

Person:	Bjørn Mose
Phone:	+45 2536 3632
E-mail:	Bjorn.mose@devoteam.dk
Address	Devoteam Consulting A/S Tuborg Parkvej 10 2900 Hellerup + 45 3945 0700 www.devoteam.dk

DOCUMENT

ID:	#63215
Author:	Bjorn Mose
Date:	27/10/2007
