

The quest for the IdM holy grail

Stig Wennevold
University of Tromsø



Disclaimer

- The idea that this project will build a new super campus IdM system is incorrect
- And anyway we were not the project group
- We were not even the pre-project group
- This presentation will not be about interesting results and cool technology
- It will be about lack of results and uncool processes
- It may even be boring – blame Anders, he talked me into giving it



Content

- Background
- Initial problems
- More problems
- Lessons learned and tentative conclusions

Disclaimer (cont.):

This is a work in progress.
The conclusions are mine and not necessarily
those of the neither the group, the report
nor the steering group

Some background

- The Norwegian HE sector
 - 6 (used to be 4) universities
 - 20+ community colleges
 - The NREN: Uninett
- Many common solutions and systems
 - Student registry system
 - HR (incoming)
 - Frida (research doc. System)
 - And lots more..
- FEIDE – the HE id-federation

More background

- There are a lot fewer systems than institutions and some of the common solutions have been very successful
- The (long running) common HR project apparently reached its goal choosing SAP
- Cost effectiveness through cooperation was the mantra of the day
- FEIDE had put IdM on everyones agenda



therefore

UKITEK Proudly presents:

**The quest for the
Norwegian Higher Ed
Common Campus IdM System**

Featuring:

A steering group
A somewhat diffuse mandate
some IT-staff doing IdM stuff today
and
two consultants

Can this possibly go wrong ?

Mandate

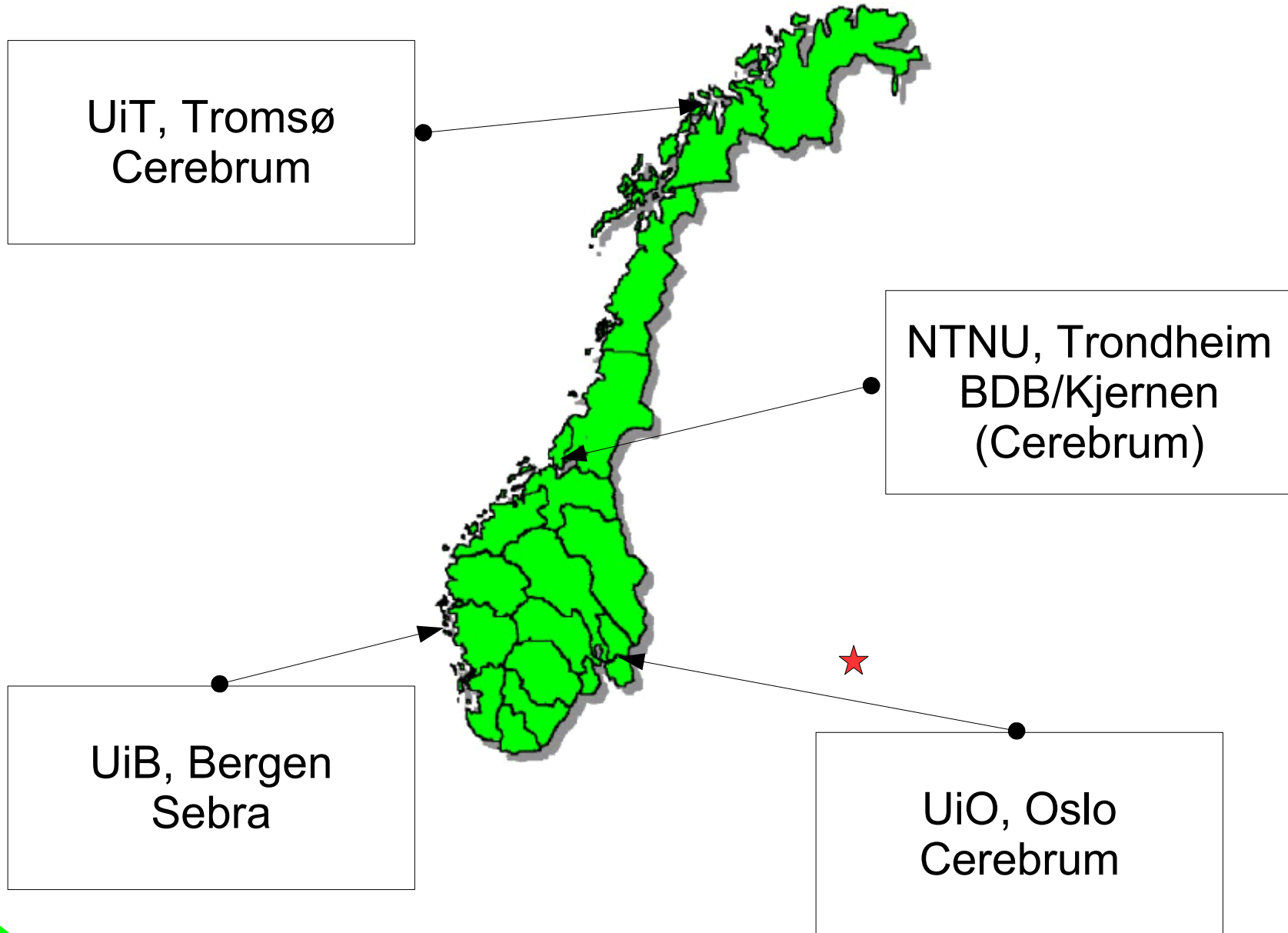
- Specs for common “UserAdministrativeSystem” doing “what our 4 UASs do today”
- Must support today's common source and end systems, including the new HR
- Evaluate commercial vs homegrown
- Plan for interim solution based on Cerebrum
- Please hurry

Note to self: Explain “Cerebrum”

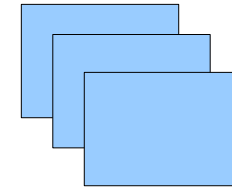
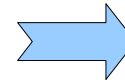
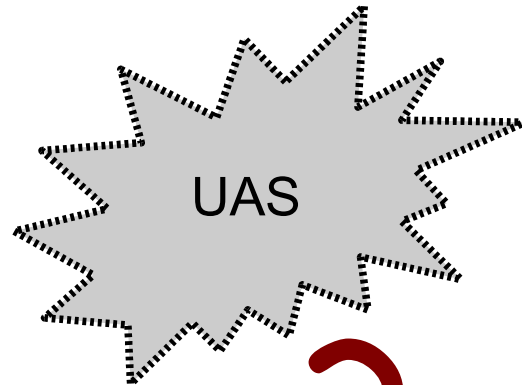
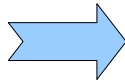
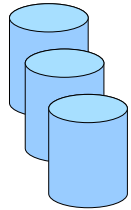
Potential benefits include

- Reduced development cost by sharing code
- Reduced vulnerability by skill and knowledge overlap
- Improved quality by larger brain-pool
- ASP model for the smaller colleges
- Faster adaption of new systems
- More muscle in the marketplace

Where are we



Initial problem – what ?



- HR
- Student Reg
- Others
- Manual sources

- AuthN/Z
- LMS
- Unix / AD acc.
- eMail
- and many more

“UAS” = it seems

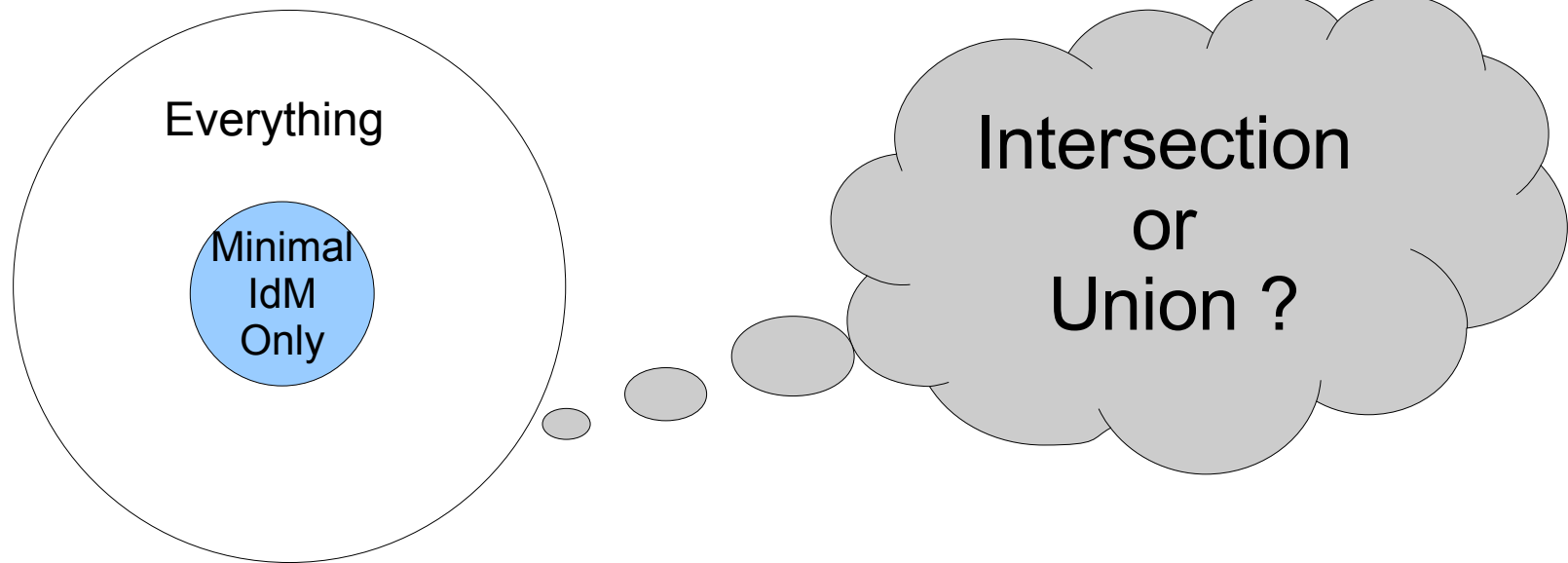
- A Metadirectory modeling large parts of your institution
- Connectors – mappings from systems to model
- Rules – Business intelligence
- Data flow engine
- Provisioning engine
- Monolith covering arbitrary parts of the identity management architecture

UAS today

- Looking at the four universities involved we find four different approaches with overlapping but not identical functionality.
- They are as well documented as most homegrown systems in the sector.
- They work fairly well in their current environment but as a result of evolution rather than intelligent design

-ng ?

UAS-ng scope ?



- Intersection: doable but unsellable
- Union: impossible (but desirable)

Refocus: IMA

Need an IMA that

- Breaks current monolithic UAS into distinct components
- Has a common data model and Interfaces
- Makes mappings, triggers, flow mechanisms etc configurable
- Separates rules (BI), engines and datastores
- Relies heavily on standards

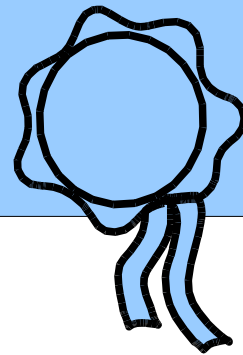
Then start looking for added value by shared components

Challenges

- Defining the architectures scope and components
- Every area that is included => assumptions about the institutions work flow.
- Every area excluded => assumptions about the surrounding information architecture.
- This must involve a lot of people
- and is hard enough for $n=1$.

Postcard from the Quest

We were not really sure where we wanted to go.
We set out in the wrong direction.
We should have brought some other guys along.
We got a bit lost.
But the grail is there and we have a plan.
Send more money.



The Grail

- Really just the inevitable future ?
- The IMA is there and taken for granted
- IdM matures and todays hard issues are resolved
- Yesterdays bleeding edge becomes todays infrastructure
- Infrastructure will no be allowed to continue being hard and ad-hoc
- We find something new to do the hard way :)

The Quest(ion)

- How do we go to the future rather than just being caught up by it and does traveling as a group help or just slow us down ?
- My 2 cents: $n > 1$ is harder but
 - Forces you to things right
 - Adds abstraction and perspective
 - De-localizes the issues
 - Yields benefits even if we end up with $1+1+1+1$

So even if we fail we win :)

Why $n=4$?

*In the long run men hit only what they aim at.
Therefore, though they should fail immediately,
they had better aim at something high.*

David Henry Thoreau
"Walden", 1854



To be continued ...