NAV – SaaS IGA rollout

Lessons learned (part 2)

Identity day light 26.09.2024

Eivind Staff – Eivind.Staff@nav.no

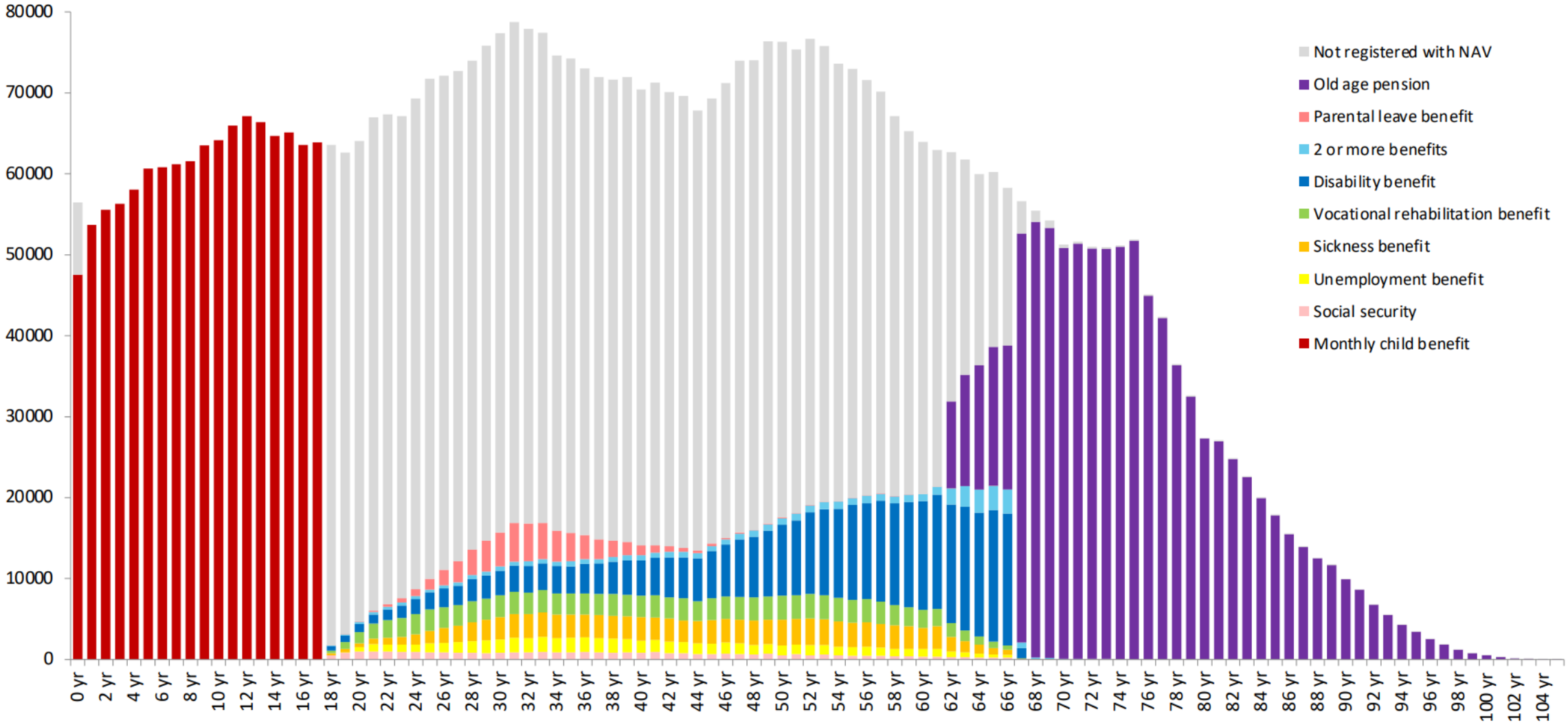
Agenda

- What is NAV?
- Timeline SaaS IGA
- Impediments (why does it takes so long time)
- Lessons learned

What is NAV?

- NAV: = Norwegian Labour and Welfare Administration
- 1/3 of Norways state budget
- NAV, the state and municipalities cooperate in providing a single gateway into public labour and welfare services.
- Develop application for both employees and citizens
- 22000 employees
  - 15500 state employees
  - 6500 municipalities employees
  - + 2000 external

What is NAV?



All numbers are status for citizens residing in Norway as of December 2017. Social security, unemployment benefit, sickness benefit, vocational rehabilitation benefit and disability benefit are controlled for double-counting, and therefore counts citizens with only this benefit. Citizens with 2 or more of these benefits are shown as «2 or more benefits». Source: NAV.
Population numbers per annum are as of 1. January 2022. Source: SSB

Timeline SaaS IGA

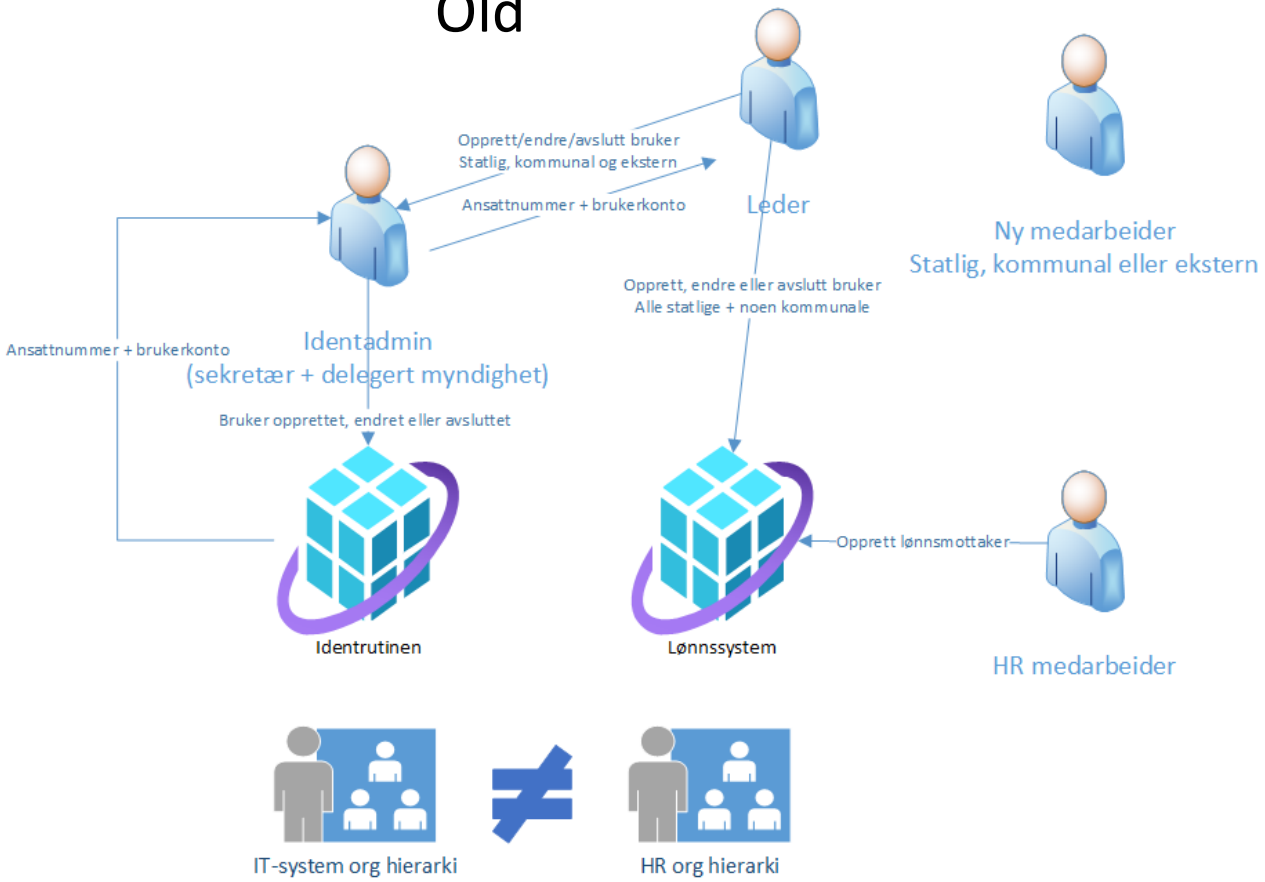
- Autumn 2022 procurement
- December 2022 product selected: Omada Identity Cloud
- Start rollout from January 2023
- In read only production August 2023
  - Bad data quality from HR feed
  - Fixing data quality issues
- Pilot provisioning April 2024 (admin users)
- Pilot recertification June 2024 (admin users)
- Pilot provisioning August 2024 (HR applications - normal users)

Impediments (why does it takes so long time)

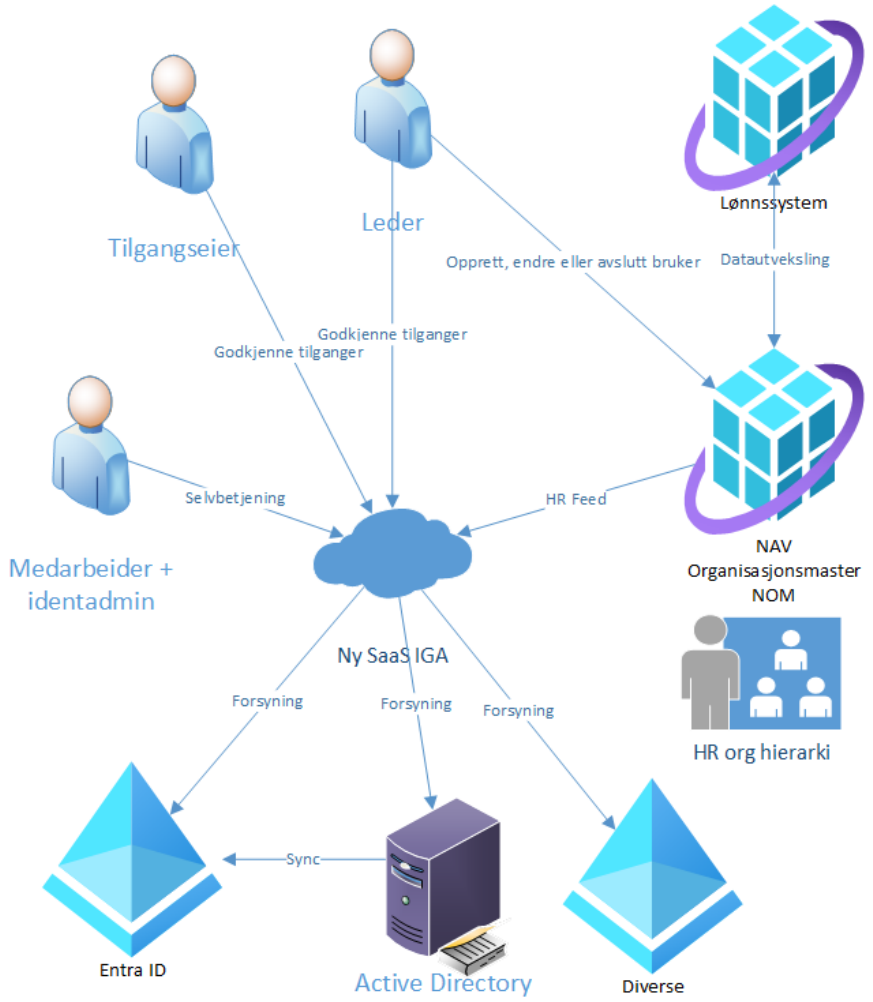
- Data quality from HR feed still lacking
  - Must still run provisioning in review mode to catch data glitches
- Joining HR and Identity process takes time
- Still missing functionality for filtering access request (allowed only by selected organizational units)
  - Incoming in the next 2 releases (we hope…)
- Must finished the pilots
- SaaS still breaks sometimes…
- Still needs to improve deployments processes
- Manual process for deployments breaks way too many times (we really need more automation…)

Joining business processes
HR + Identity

Old



New



Joining business processes

- Separate process we try to join in common process
  - HR process for state employees
  - Identity process for all that need IT access
- HR people not used to update this process before scheduled payroll run
- Identity people not used to handle contract dates and so on
- Another team rolls out the new organization master (NOM)
  - We have to wait for them to finish
- How to make people behave differently due to new requirements?
  - Training and communication
  - “Fail fast” in the process, so they learn?

Try to enforce a policy for the first time

Written policy (that few reads and/or comply with) and no enforcement vs hard policy enforcement

- It is hard to be the first enforcer of a policy few reads
  - Do we want to be the bad guy?
  - Do we break things?
  - Are the business needs to break the policy?
- Hard policy enforcement need very detailed policy (all the egde cases)
  - Policy people are not used to this handle edge cases
- Hard policies are slow to change
- Are there **no** exceptions? Are you **sure**?

SaaS still breaks sometimes

- Updates nearly every month (11 times a year) + patches
- We control when the update is applied to our environments
- No possible to “roll back” (maybe support can do it) without restore with data loss
- The update in July broke the access request process for us
- Had only updated a sandbox environment in August, and we found the bug by accident
- Need to test more with vendor updates
- Bug found and fix is underway, but will not be rolled out before October update

The benefit with a “local” medium size vendor

- They listen
- They improve
- Small bug fixed to the next release
- Even an annoying “why can’t I press enter in the MFA field in the Portal to continue?”
- And usability concerns like “the popup block the information below, can’t see what you have selected”
- Listen to the “we need to be able to allow only selected organization units to request some accesses” and set in on the roadmap and due in October + November

The vendor architecture sometimes creates trouble

- The vendor loves the use of the build in data warehouse
- Every load of data take a minimum of 40 minutes, even 1 change
- Bundles loads (HR + AD + Entra ID) takes even more time (1,5 hours)
- Data load without delta load takes a long time (up to 3 hours)
- And if data are loaded directly into the IGA solution (by API), then the data warehouse do not know this information and data import fails
- Need to replicate data from IGA to the data warehouse or else the import matching will fail
  - Support must set this up
- Major change incoming from vendor, but we need it now

Still need code outside

- Needed to sync from a custom user repository to AD/Entra ID
- Tried both old IGA and new IGA
- Too hard and costly both places
- So are now creating a custom sync application

- And the HR feed data enrichment + data join is still there

No DevOps support – deployments breaks

- Omada have a concept of Changeset
  - Delta of objects (object change from old value to new value)
  - Recorded in dedicated environment with no data
  - No tracking of imported changesets
  - Can break if you change things directly in an environment
- Runbooks are manual steps to perform
  - Environment specific values needs to in the runbook
  - Secrets must be manually entered
  - Secrets must be entered every time you change anything with the object
- Runbooks/manual steps breaks (all the time…)
- Four-eyes principle helps, but are expensive and still breaks sometimes

It is expensive to test

- Manual test is expensive and time consuming
- Test automation are hard to implement
- Have not started with test automation
- Need developers to create test automation

It is expensive to manage environments

- Manual delete&create are expensive and time consuming
- Environments automation are hard to implement
- Have not started with environments automation
- Need developers to create environments automation

- Due to the changeset, environments diverge over time
- Need a reset from time to time
- Production are in practice not possible to reset (too much down time)

Access review process is hard to get right

- Access review is equal to all the access approve, but:
  - No or little context from why the access has needed
  - Massive data volume (typically 1000-5000 question per manager)
  - The access description are not good enough
- Filter review for the most important accesses?
- Smarter review selection? Based on “this is not normal for the employee peers” or something like that?
- QA on access description?
- Better description format? May need context and assumed user group
- Divide the review so smaller and more often review?
- Track the result and adjust approach?
- Enterprise role to the rescue (again…)?