Some practical experiences with negotiating cloud services

27 January 2015, CoCo Cloud Seminar, Oslo

Jan Meijer, UNINETT

UNINETT

UNINETT AS

- NREN: national research & education network
- Not-for-profit, membership-based. Ca. 140 members
- Education Department's tool for shared ICT-infrastructure

- National network (=physical infrastructure)
- Shared services, procurement, demand aggregation
- National programmes on eCampus and Higher Ed Cloud
- Collaboration with other 4 Nordic NRENs via NORDUnet AS
- Collaboration with other EU NRENs

Box procurement

- “sync ‘n’ share” = “cloud-based file synchronization and sharing”
- Wanted legally compliant enterprise Dropbox
- Shared procurement of framework agreement with other Nordic NRENs via NORDUnet
  - 6 active participants in contract process
  - each NREN is different
  - each has community to answer to
- UNINETT reseller of Box licenses
- Box: USA startup in phase 2; strong growth

Expectation with cloud services

Process

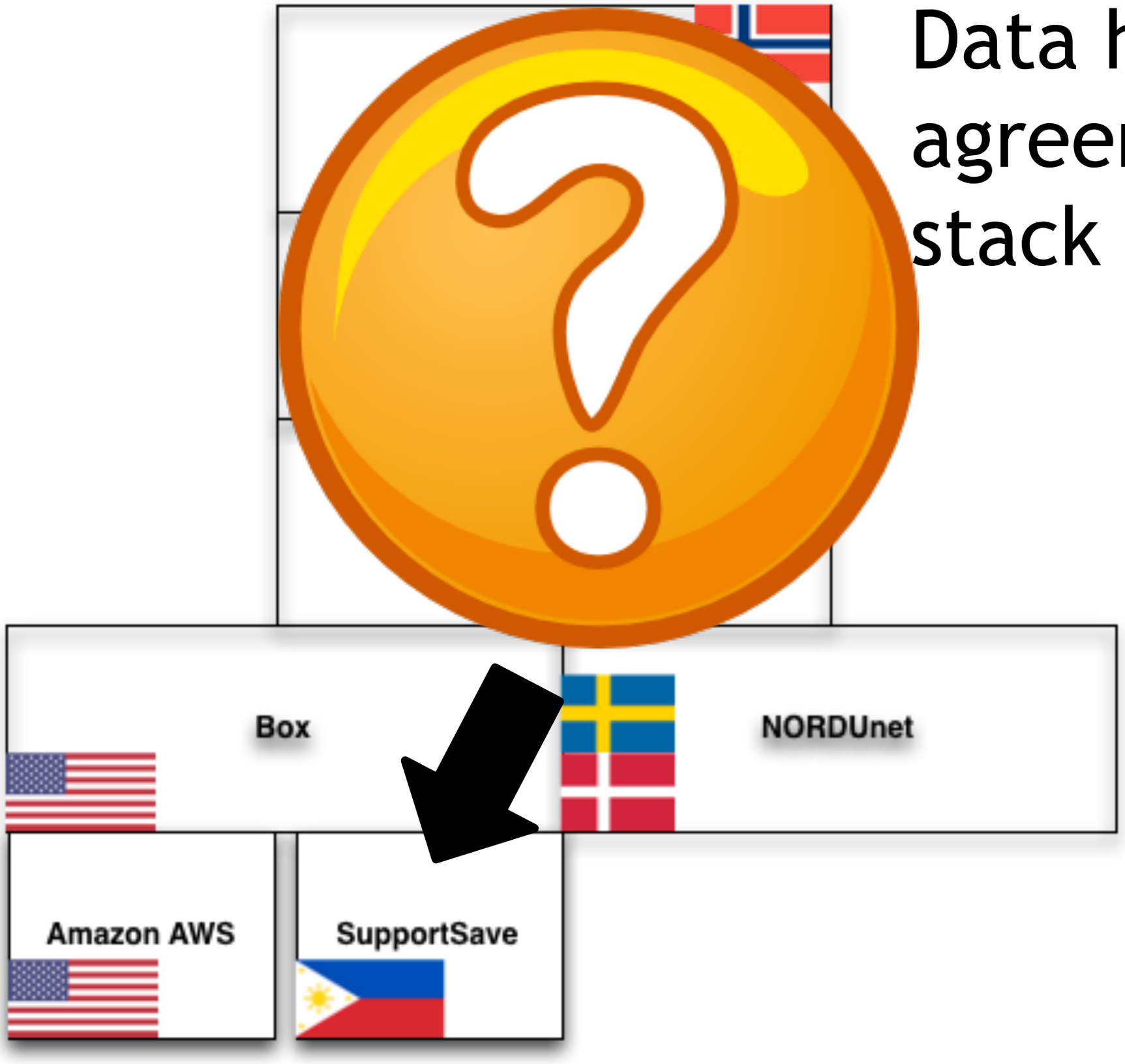
- **Sep 2012**
  - Community consultation
  - Write RfP
- **Dec 2012**
  - EU Tender start
- **Apr 2013**
  - Start Framework contract negotiation
- **Jun 2013**
  - Start Call-off negotiation Norway (DHA)
- **Jul 2013**
  - Framework signed
- **Oct 2013**
  - Call-off contract signed
- **Dec 2013**
  - Service start

- **Apr 2013**
  - Investigation technical integration user provisioning
  - Shared risk assessment process with sector in .no
- **May 2013**
  - Conclusion + test implementation user provisioning and logon integration
  - Shared risk assessment done and published
- **August 2013**
  - Imlementation production user provisioning and logon integration
- **Sep 2013**
  - Investigation technical support for legal compliance

Documents

- Framework agreement Box – NORDUnet AS
  - Includes standard Box service agreement
- Call off contract UNINETT AS - Box
  - Adapted Box service agreement
  - International data processing addendum with modifications
- Risk assessment for use of Box
  - shared for .no higher ed sector
  - risk for institution, UNINETT
- Service agreement UNINETT AS – institution
  - Service contract
  - Data handling agreement

Data handling agreement stack



Data handling agreement Box

- “The data importer agrees and warrants to make avallable a written audit report not older than 18 months by a registered and independent external auditor demonstrating that the data importer’s technical and organizational measures are sufficient (according to ISO 27001:2005, SSAE 16 Il SOC1 and 50C2, HIPAA).
- “At least once per year, Data Processor shall make itself available to discuss with Data Controller the security measures affecting the Customer’s instance of the Box Service.”
- User opt-in via AUP for transfer of name, email to callcenter in .ph

Why the long turnaround time?

- Mapping a “one size fits most” service on a legal and operational reality
- Unfamiliar parties, process and constraints
- Important details come piece-meal
- Many cooks in the kitchen
- Temporal and physical separation
- No clear shared understanding of the challenge

Challenges

- Issues at end-user side, (www.tosdr.org)
- Safe Harbour is ... open for interpretation
- World's call centres in India and Philippines
- Cloud providers do one size fits most, but there is no global one size fits all legal framework
- As organization you can't regulate your responsibilities away

Cost, compliance and context

- Employees in .no higher education: 30.000
- Students in .no higher education: 250.000
- Box license cost: 70 NOK / seat / year (7 EUR)
- Licenses procured: 5000
- 1 UNINETT hour (2015): 1150 NOK
- 1 risk assessment about 20-40 hours
- Estimated hours @ UNINETT needed to provide service: 300/year

Cost of compliance not depending on service size!

Compliance reality 2.0

- Improve service cost / compliance cost ratio
- Remove FUD
- Compliance competence with project & service managers
- Automation: paperwork as a service
- As a community: common understanding and way of dealing with the challenges
- As a community: certification process for cloud providers to enforce standards for compliance

Is compliance enough?

- Spies spy and potential terrorists need to be monitored
- Sovereignty vs. data-sovereignty, in a centralised world?
- Legal compliance vs. what are you comfortable with

Thank you

jan.meijer@uninett.no
skype: janmeijer.no
tel: +47 90177711