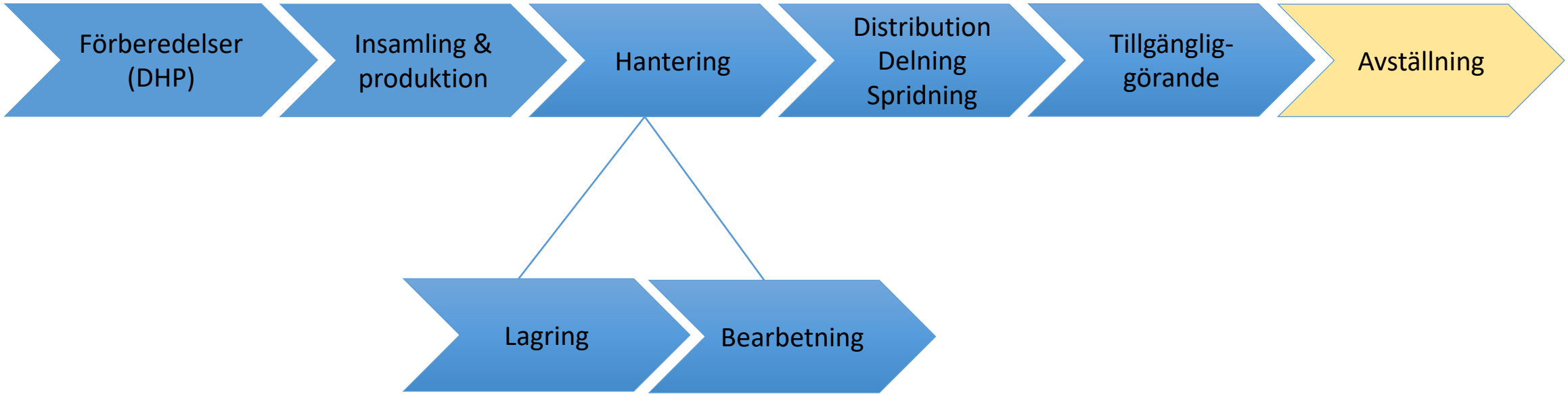
Datadelning och dataöverföring av filer

Fredrik Granström, UmU

Forskningens livscykel



Klassning av data

- Till Klass-0 räknas:
  - Information som kan betraktas som publik
  - Ingen skyddsnivå

- Till Klass-1 räknas:
  - Allmän information till externa användare, e-post
  - Grundläggande skydd krävs.

- Till Klass-2 räknas:
  - Forskningsmaterial, personalärenden
  - Extra skyddsåtgärder krävs.

- Till Klass-3 räknas:
  - Sekretessbelagda uppgifter, rikets säkerhet, kan medföra skada på liv och hälsa.

https://www.msb.se/ och https://klassa-info.skl.se/

Identifierade problem och brister

- Kravproblem, forskare/användare vill ha ”säker lagring” men behöver en säker arbetsplats

- Vi lagrar information på fel sätt
  - ❑ Okrypterad
  - ❑ Vi kan ej garantera vilka som får åtkomst till data, uppnår ej lagstiftningens krav på ”Stark autentisering”
  - ❑ Persondatorerna håller inte måttet säkerhetsmässigt
  - ❑ Lagring sker i molntjänster utanför Sverige/EU.

- Spridning
  - ❑ Delningsmöjligheter saknas så data kopieras mellan olika huvudmän
  - ❑ Inga avtal mellan olika huvudmän
  - ❑ E-post används för ofta med känsliga data, lösenord och engångskoder

- IT-stöd saknas
  - ❑ Säkra enkäter
  - ❑ Identifieringar, få lärosäten har IT stöd för eId hantering
  - ❑ Säkra videomöten och redigeringsverktyg
  - ❑ Bearbetningssystem, en säkrad laptop eller någon form av virtuell desktop

- Personalen vet inte hur de ska göra

De tekniska skyddsåtgärder som behövs genom hela kedjan kan sammanfattas i några principer:

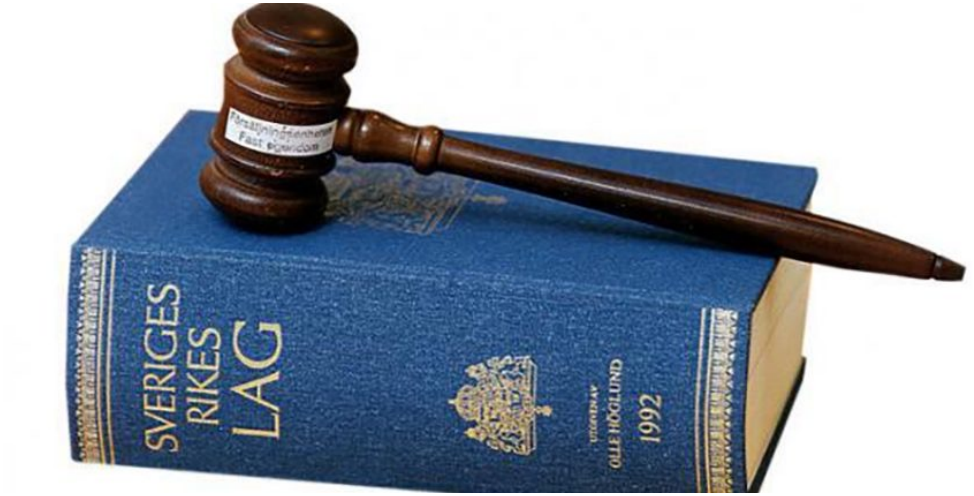
- Hög tillit på identiteter
  - Både på de som hanterar data och de registrerade
- Kryptering vid transport av data
- Kryptering vid lagring av data
- God behörighetshantering
- Loggning och spårbarhet på access på datanivå

Juridik

Råder en väldigt osäkert ute på lärosätena om vad man får och inte får göra. Vi tolkar regler olika mellan lärosäten fast vi har samma regelverk

Några exempel på frågor:

- Pseudonymisering
- Enkäter och video inspelningar
- Persondatorer
- Molntjänster med kryptering
- E-Id, vettingsprocesser

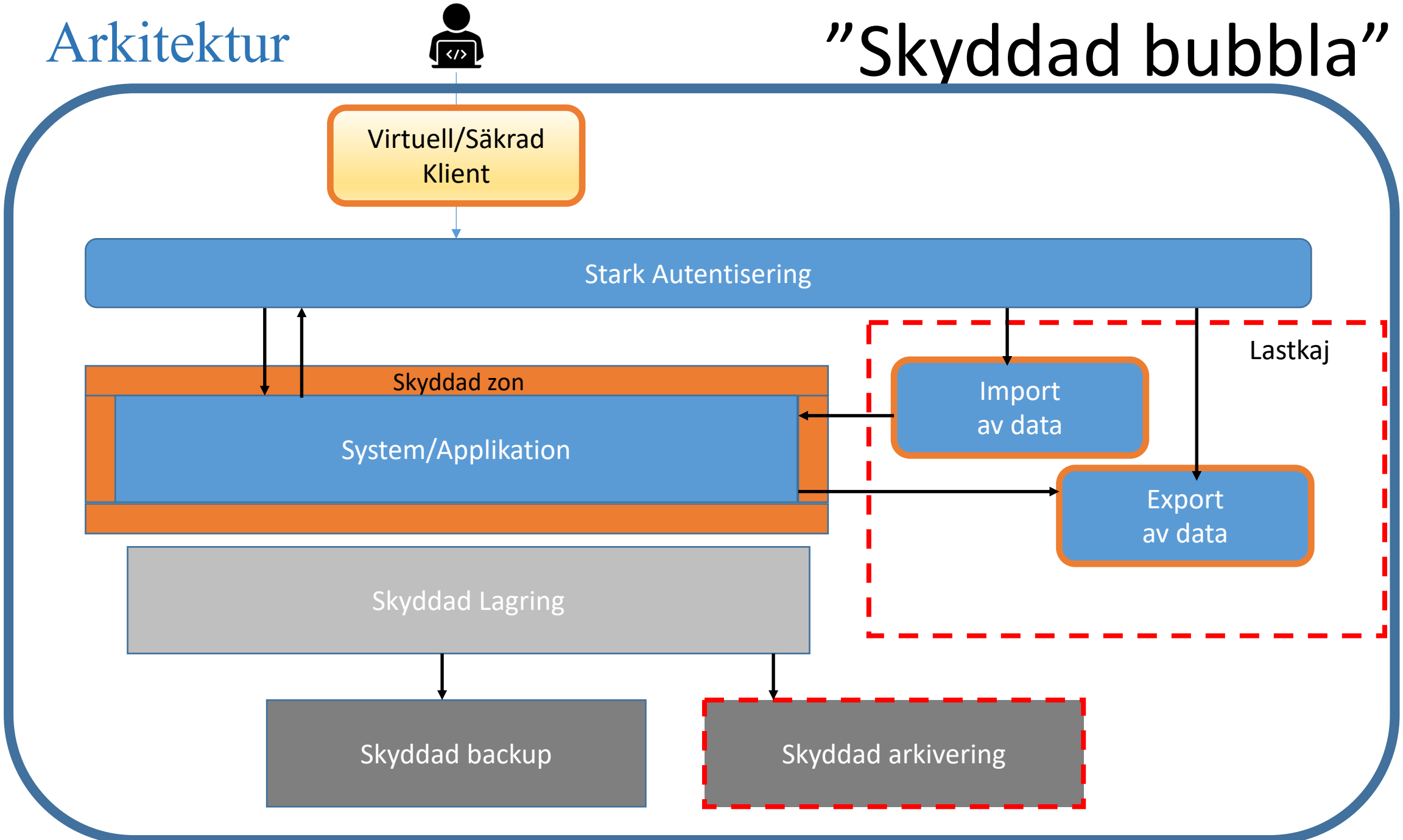


Förbättringar: IT måste lära sig ställa rätt frågor annars blir det alltid NEJ

Förslag: Tillsätt en liknande projekt som detta men där juridiska spörsmål utreds

Arkitektur

”Skyddad bubbla”



Skyddad Miljö och Programvaror

Inom projektet har två varianter diskuterats

- Säkrad dator
  - ❑ En egen ”säker” dator
  - ❑ Beprövad teknik
  - ❑ Managerbart centralt

- VDI
  - ❑ Åtkomst med vilken klient som helst
  - ❑ Hybridvariant, lokalt och i moln
  - ❑ Kan skapa både Windows och Linux VDI-miljöer

Programvaror

- ❑ Program måste säkras och godkännas, RSA ska utföras
- ❑ Paketering
- ❑ Kräver expertkunskaper för olika program
- ❑ Tidskrävande

Förslag: Skapa ett register på program som lärosäten har ”godkänt”. Kanske via Sunet!?!

Lastkaj och Lagring

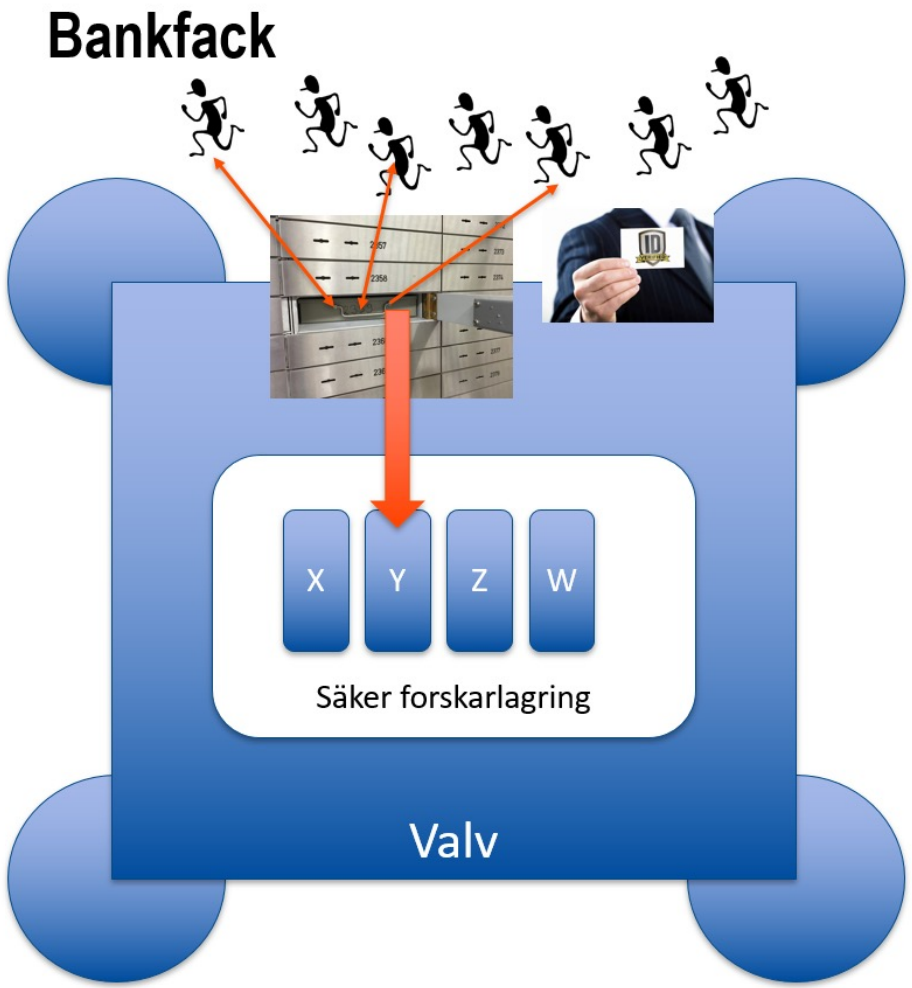
”Lastkaj”

- Import
  - ❑ Data levereras från olika huvudmän på olika sätt
    - Krypterad USB sticka
    - Hämta på websida
    - SFTP
    - Krypterad fil mailas till mottagaren
  - ❑ Stark autentisering på avsändaren
  - ❑ Verifiera att rätt data mottagits (checksumma, antal filer, markeringar)
- ❑ Export
  - ❑ Paketering och märkning
  - ❑ Avtal
  - ❑ Stark autentisering på mottagaren

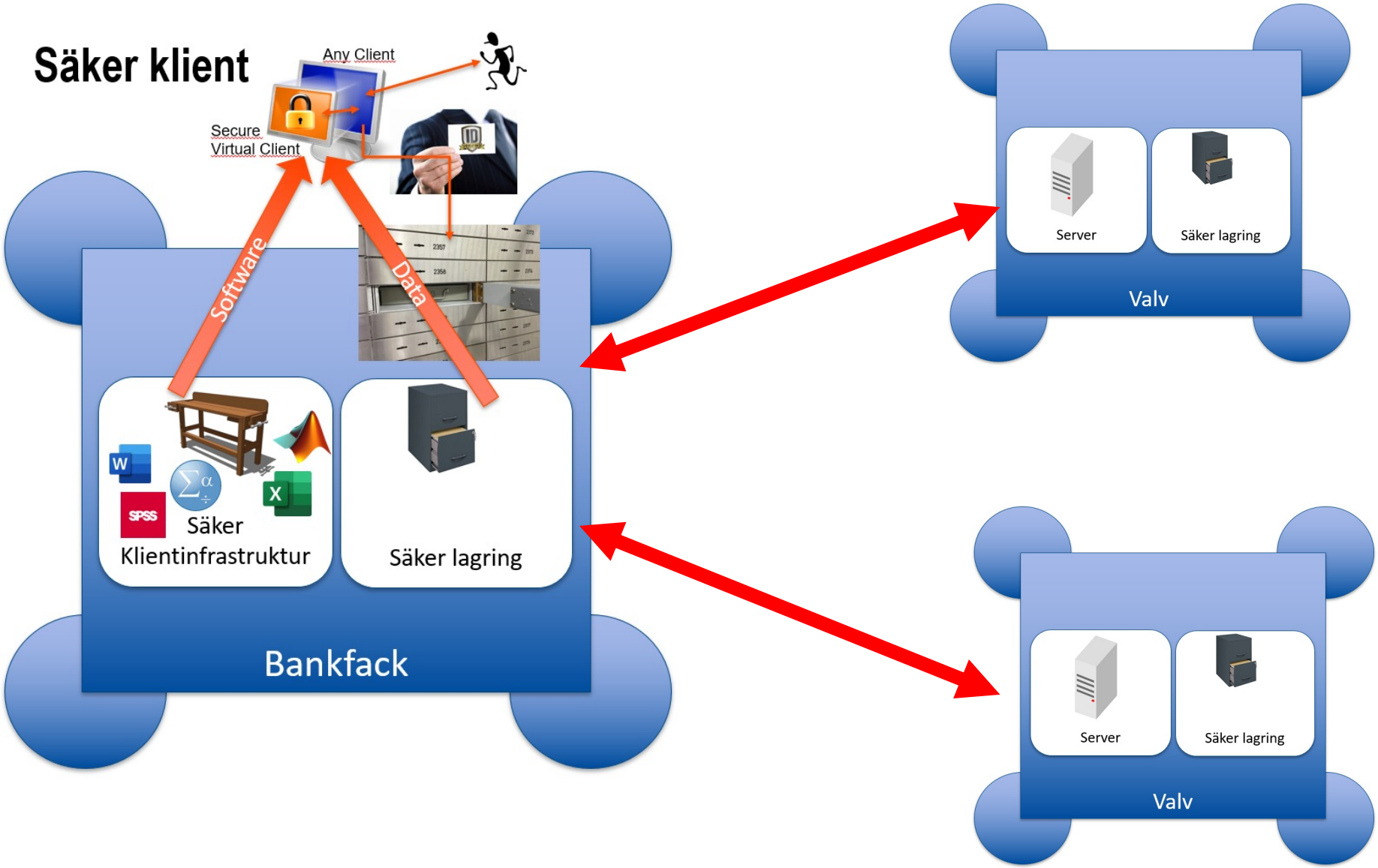
Lagring

- Lokal lagring
- Sunet Drive
- Molnlagring, exempelvis o365. Egen kryptering men då blir det också besvärligt och du tappar fördelarna.

Bankfack istället för Bankvalv



Säkrad klient



Krav genom processen

Det finns inte ett program/system som hanterar hela forskningens livscykel. Många enskilda BRA system finns också ute bland lärosäten men helhetstänket saknas => Säkerhetshål

Förenklad modell:

- Uppstart
  - Säker dokumentlagring med delningsmöjlighet, ex säkrad SharePoint
  - Stark autentisering
- Aktiv forskning/arbete
  - Enkäter, Video, dataset, journaler, analysverktyg
  - Stark autentisering/Behörighetskontroll
  - Loggning
  - Högre krav på prestanda
- Avslut
  - Data blir statiskt
  - Lagring med möjlighet till länkning till publicering, exempelvis SND/SunetDrive
  - Övergår till lärosätets ansvar
  - Arkivering

Positiva trender

- Forskare/Anställda ställer krav
  - Datahanteringsplaner
  - Större medvetande om lagstiftning
- Ledningen på lärosätena har utvecklat insikt och engagemang i detta
  - IT säkerhet i fokus på många lärosäten
  - Juristerna jobbar på högvarv med IT frågor
  - Vi går från punktinsatser till långsiktighet
- Processer kommer på plats mer och mer
  - Informationsklassning
  - RSA
  - Stark autentisering och MFA
  - Guidelines hur skyddsvärd data ska hantera, täpp till brister och hål.

SCOPE

- **Konceptuell Arkitektur**
  - Begrepp
  - Klassning av data
  - Autentisering
  - Loggning
  - Delning
  - Klienter, Client Health Check

- **En best-practice lista gällande:**
  - Autentisering
  - Lagring
  - Kryptering
  - Arkitektur

- **Gemensam kravbild**
  - Utifrån de regler och lagar som finns idag så ska projektet förslå vad som krävs för att nå dessa krav.