Pitu - konkrete erfaringer

Af Jørgen Ulrik B. Krag <jubk@magenta.dk>

Magenta - hvem er vi

- Softwarelevarandør der leverer Open Source software i Danmark, Grønland og norden
- Har løst opgaver i Grønland siden 2012
- Kontor i Grønland siden februar 2019
- Primære nuværende produkter i Grønland
  - Datafordeleren
  - E-boks
  - Selvbetjeningsløsninger til Skattestyrelsen

Magenta på Pitu: Overblik

- Demo-projekt på den første Pitu konference i september 2018
- Datafordeleren (test) på Pitu i april 2019
- Ny datafordeler-service til E-boks februar 2020
- Ny generiske services for CPR, CVR og adresser i april 2020
- Igangværende:
  - Service for rullende aktuel indkomst baseret på UXP Connector
  - Hjælpe med installation og drift af UXP Security Servere

Pitu-demo på konference 2018

- Projekt i samarbejde med Digitaliseringsstyrelsen og landslægen
- Database fra pilotprojekt for sygeplejerskeautorisationer
- Service via UXP Connector: Hent liste af autorisationer
- Service udbudt i Security Server
- Opslag demonstreret via UXP portal
- Alle UXP-produkter installeret og konfigureret af Cybernetica

Pitu-demo på konference 2018 - erfaringer

- God teknisk dokumentation for de enkelte komponenter
  - Dog svær at forstå indtil man får en generel introduktion
- Opsætning af denne type service er mere et spørgsmål om konfiguration end udvikling
- En stor del af den avancerede konfiguration er håndteret centralt
- Sikring af kommunikation via certifikater kan være en udfordring

Første services fra Datafordeleren

- Nyt Pitu-miljø
- Security Server leveret af Digitaliseringsstyrelsen
- Udstilling af eksisterende CPR og CVR services udviklet til Prisme ERP-systemet
- Sikring af kommunikation mellem Datafordeler og Security Server
- Test-services blev udstillet først, efterfulgt af de samme services i produktion

Første services fra Datafordeleren - erfaringer

- Adgangsstyring flyttes fra oprindelig applikation til Security Serveren
  - Adgang er kun på èt niveau: Enten har man adgang eller også har man ikke
- Forbindelse mellem Security Server og applikation skal sikres, to muligheder:
  - Firewalls / netværk
  - HTTPS og klient-certifikater
- Procedurer for aftaler omkring adgang skal fastlægges
- Pitu-klienter der skulle have adgang skulle importeres og godkendes på Security Serveren
  - Dette skyldes muligvis at de ikke var godkendt på deres egen security server

Ny service til E-boks

- Opslag på om borgere og virksomheder hører til i Grønland
  - Troede vi kunne bruge eksisterende services, endte med at specialisere
- Udvikling af både service og klient
- Pitu som sikkerhedslag og til administration af adgang
  - Sikring via HTTPS og klient-certifikat

Ny service til E-boks - erfaringer

- Specifikation af servicen tog noget tid at få på plads
  - Endte med en en-til-en integration mellem to systemer med begrænsede muligheder for generel udbredelse
- God ide at lave et transparent Pitu-klient-bibliotek
  - Rammeværktøj der tager sig af alt Pitu-relateret så klient-softwaren blot kaldes på normal vis
  - Kan genbruges i anden sammenhæng
- Ny “Pitu-bruger” kræver oprettelse og konfiguration af ny Pitu-klient i Security Server
- Tilføjelse af en ekstra service til det eksisterende Datafordeler-setup krævede meget lidt arbejde
  - Registrering af ny service
  - Tildeling af adgang

Nye generiske services for Datafordeleren

- Nye services for CPR, CVR og adresser
- Designet til at være bredt anvendelige
- Fokus på generel anvendelighed
  - Services skal fungere på en måde der gør det let at integrere dem ind i f.eks. kommunal sagsbehandling
- Simplificering af data
  - Data skal være lette at forstå
  - Data skal være lette at anvende
  - Kun nuværende gældende data
- Data samlet i èt opslag
  - Enkelt service for adresse der samler delelementer

Nye generiske services for DAFO - erfaringer

- Design af en service er en stor og vigtig opgave
  - Services der udbydes skal være lette at forstå
  - Services bør målrettes mod anvendelsen
    - Søg på adresser som én service frem for separate services for lokalitet, kommune, veje, husnumre etc.
- Udbydes mange services fra den samme Security Server skal man have en plan for navngivning

Spørgsmål?

Ny service på Pitu - hvordan?

- Analyse og specificering af servicen
- Anskaffelse af Security Server / tilmelding til Pitu netværket
- Udvikling af servicen
- Registrering af servicen i Pitu-server
- Tildeling af adgang til dem der skal bruge servicen

Ny service på Pitu: Analyse

- Hvilke kildedata til servicen?
  - UXP Connector produktet kan måske anvendes hvis data kan hentes direkte fra en database
  - Dokumentér præcis hvilke data det er servicen tilbyder
- Hvem skal bruge servicen?
  - Det er vigtigt at servicen er bredt anvendelig
- Hvem bestemmer hvem der skal have adgang til servicen?
  - Hvem er det aftale om udveksling af data skal indgås med?
- Findes der et standardiseret dataformat der kan anvendes?
  - Brug af standardiserede data gør livet lettere for alle parter

Ny service på Pitu: Security Server

- Genbrug hvis man allerede har en Security Server :)
  - Der skal stadig åbnes i firewalls etc.
- Anskaffelse af maskine
- Installation af operativsystem (Ubuntu Linux)
- Adgang til netværk / åbning af firewalls
  - Skal kunne “snakke” både med de bagvedliggende services og med andre security servere
- Installation af UXP software
- Registrering af serveren i UXP netværket / oprettelse af Pitu member og klient(er)
- Opsætning af overvågning

Udvikling af servicen

- Adgangsstyring / netværksopsætning der gør det muligt for Security Serveren at kalde servicen på en sikker måde
  - Via firewalls og netværk
  - Via HTTPS og klient-certifikater
- Selve servicen udvikles som normalt
  - Dog med adgangssystem der arbejder sammen med Security Serveren
- Ved REST-services
  - Hav en plan for dokumentation, for eksempel Swagger / OpenAPI
  - Eksempler i dokumentationen gør det *meget* lettere at forstå en service

Registrering af service i Security Server

- Kræver at den Pitu klient man vil registrere servicen under er registreret på Security Serveren
- SOAP services tilføjes via URL til WSDL-fil
  - Vær opmærksom på om WSDL-fil indeholder de rigtige adresser / endpoints
- REST services tilføjes via URL
  - Giver adgang til alt under den angivne adresse - vær sikker på at der ikke udstilles for meget
- Service registreres med navn og angivelse af version
  - Disse kan ikke rettes når servicen først er oprettet
  - URL for en rest-service kan rettes efterfølgende
- Hav en plan for navngivning - en service med navnet “Test” siger intet om hvad servicen tilbyder

Demo af administrationsgrænseflade

Adgangstildeling ud fra service

- Aftaler skal være på plads før der åbnes op for adgang
- Data-aftagers Pitu-klient skal være registreret og centralt godkendt
- Adgang tildeles i Security Serverens administrationsgrænseflade
    - Security Server Clients => Rest/SOAP services for den client der har servicen => Access Rights => Add subjects => Søg / klik på ønskede => Add selected

Adgangstildeling ud fra klient

- Aftaler skal være på plads inden adgang tildeles
- Klik på “Service Clients” for den klient der udbyder servicen
- Hvis aftager-klienten er i listen:
  - Klik på klienten og klik på “Access rights” i toppen
  - Klik på “Add services”
- Hvis den ikke er i listen:
  - Klik på “+ Add” i toppen”
  - Vælg aftager-klient i listen og klik på “next”
- Vælg ny services der skal være adgang til og klik på “Add selected”

Adgangsstyring: Fjerne adgang til service

- Ud fra service
  - UXP admin => “Securty Server Clients” => “SOAP/REST services” for den klient der udbyder servicen => klik på service => “Access rights” => vælg klient der skal fjernes => “Remove selected”
- Ud fra klient
  - UXP admin => “Securty Server Clients” => “Service clients” for den klient der udbyder servicen => vælg klient => “Access rights” => Vælg services der skal fjernes => “Remove selected”

Organisering af adgangsstyring

- Opdeling af services:
  - Security Servere (f.eks. en i hvert miljø)
  - Pitu klienter (en klienter for test-services, en for produktion-services etc.)
  - Via navngivning (f.eks. datafordelerens DAFO-<service> og DAFODEMO-<service>)
- Der findes et system hvor man kan gruppere klienter i “Local access right groups” på sin security server
- Magentas erfaringer
  - Hav en plan fra starten
  - Navngivning er ekstremt vigtigt

Generelle erfaringer

- Stort set alt arbejde foregår up-front
  - Størstedelen af arbejdet ligger i planlægning og design
  - De administrative opgaver forbundet med Pitu er forholdsvis små
- Den tekniske dokumentation er god
  - Trin-for-trin instruktioner for både tekniske og administrative opgaver
  - Tilgængelig via link i administrationsgrænsefladen for hurtig opslag
- Overvågning kan være en udfordring
  - Nødt til at teste fire steder:
    - Egen applikation / klient
    - Egen Security Server
    - Fjern Security Server
    - Fjern applikation / service
  - End-to-end overvågning overvåger alle på en gang, men giver “falsk” trafik
  - Security Serveren tilbyder health-check services

Generelle erfaringer II

- Magenta lærer stadig nyt om Pitu
  - Vi troede der var et godkendelses-step på Security Server før man kan give klienter adgang
- Det er vigtigt at få en fælles forståelse og begrebsafklaring
  - Magenta har haft en del forvirring omkring klient vs medlem

Spørgsmål / diskussion?