

Brevdato

Afsender Cecilie Marie Jakobsen (Udv. Sagsbehandler,
Digitaliseringsstyrelsen)

Modtagere

Akttitel PITU IT leverandører workshop 2020

Identifikationsnummer 13758779

Versionsnummer 1

Ansvarlig Cecilie Marie Jakobsen

Vedlagte dokumenter Aktdokument
PITU workshop program 27_maj
PITU på Digitalimik.gl_da
PITU Processer
PITU Vejledning - Installation og opsætning - ver. 0.1-1
PITU Præsentation_2020
Invitation til online workshop

**Dokumenter uden PDF-
version (ikke vedlagt)**

Udskrevet 27-05-2020

PROGRAM FOR PITU WORKSHOP FOR IT LEVERANDØRER D. 27/05.

Onsdag d. 27/05:

Kl. 08:30: - Velkomst og introduktion – Styrelseschef Katrine Hjelholt Nathanielsen

Kl. 08:45: - Overordnet præsentation over PITU – Projektleder Cecilie Marie Jakobsen

Kl. 09:15: - Cybernetica præsenterer PITU arkitekturen

Kl. 10:00: - 10 min pause

Kl. 10:15: - Heldin – Lilly fra Færøerne

Kl. 10:45: - Magenta deler konkrete erfaringer:

- Hvordan kom Magenta ind på PITU?
- Et eksempel på planlægning at få en service på PITU
- Eksempler på adgangsstyring i PITU

Kl. 12:15 – Pause

Kl. 13:00 – Afrunding



PITU

Digitaliseringsstyrelsen

2020



INDHOLD

- Hvad er PITU
- Vision
- Rammer
- Fordelene ved medlemskab
- Hvad kræver et medlemskab og prismodel
- Use case
- Vil du vide mere

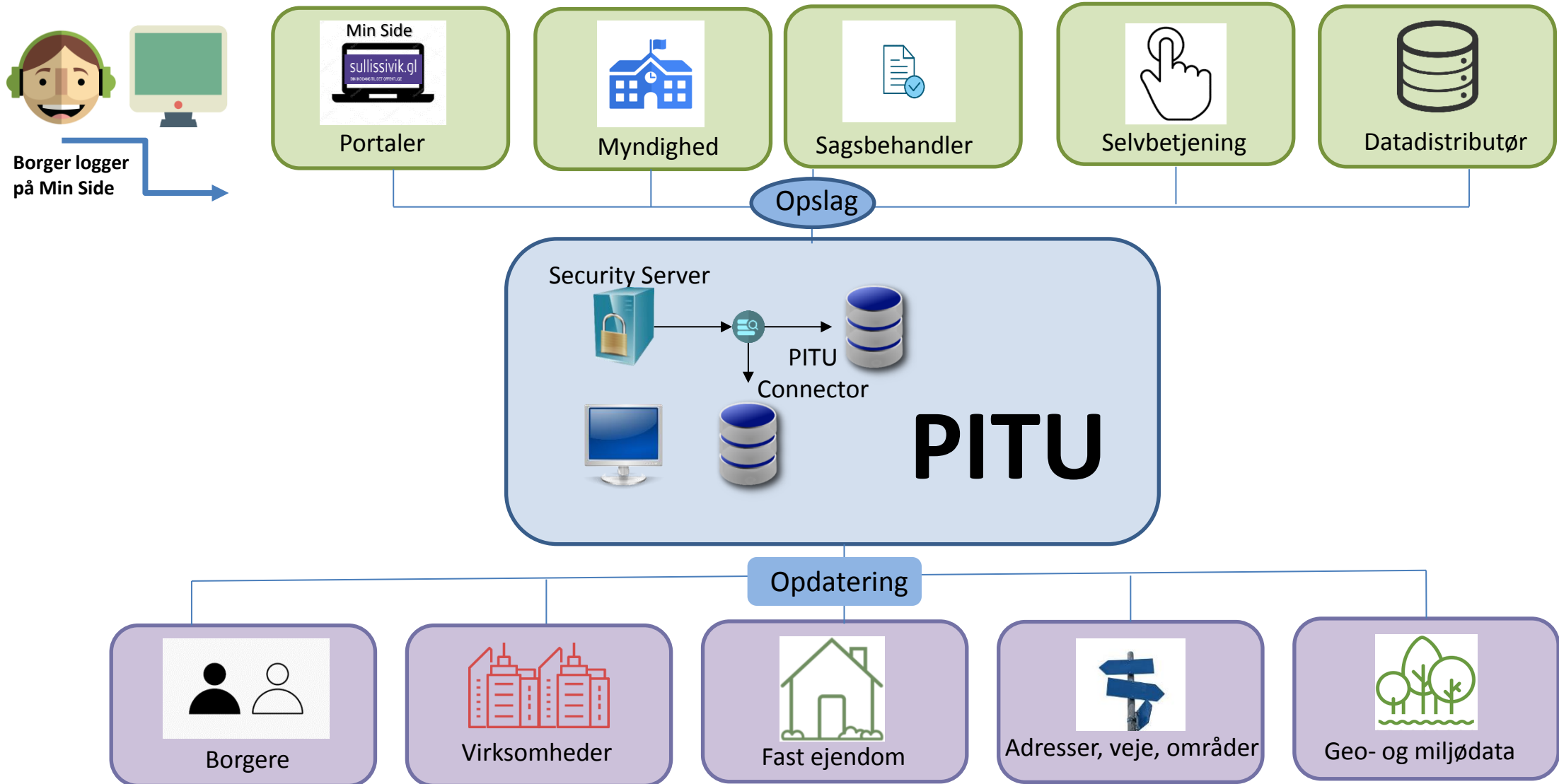


PITU arkitektur

- PITU er en teknisk platform, som gør det muligt for medlemmerne at udveksle data mellem deres IT-systemer via internettet på en sikker, krypteret, systematiseret og beviselig måde.
- Data tilgængelig i PI-TU-arkitekturen udstilles gennem PITU Services og er formuleret som SOAP- eller REST-API'er.
- PITU-arkitekturen består af tre komponenttyper: PITU Kerne, PITU Periferi og Trust Services.



PITU – Tænkt USE CASE



PITU-VISIONEN

- 50% af alle offentlige registre udveksler data via PITU

Digitaliseringsstrategien



Overordnede rammer

Governance

- Forankring i Advisory Board, som består af DIA's styrelseschef, som er formand samt repræsentanter fra andre myndigheder
-

Sikkerhed

- Enkelt kontrolpunkt for alle indgående og udgående tjenester giver ensartet sikkerhedsniveau til alle tjenester og informationsudvekslinger
- Peer-to-peer-krypteret kommunikation
- Digitalt signeret bevisførelse for alle informationsudvekslinger

Jura

- PITU overholder af gældende regler for GDPR
- PITU er infrastruktur – aftaler om udvekslinger sker efter overenskomst mellem PITU-medlemmer
- PITU må ikke forvride markedet med krav eller fordele til enkelte

Økonomi

- DIA drifter PITU med indtægter fra medlemskaberne, dvs. platformen er selvfinansieret og reguleres efter antal medlemmer. Jo flere medlemmer jo billigere medlemskab.
- Årlige udgifter til platformen pr. medlem er pt. 30.000 kr.
- Decentrale udgifter til udvikling af webservices bliver afholdt af den pågældende myndighed.

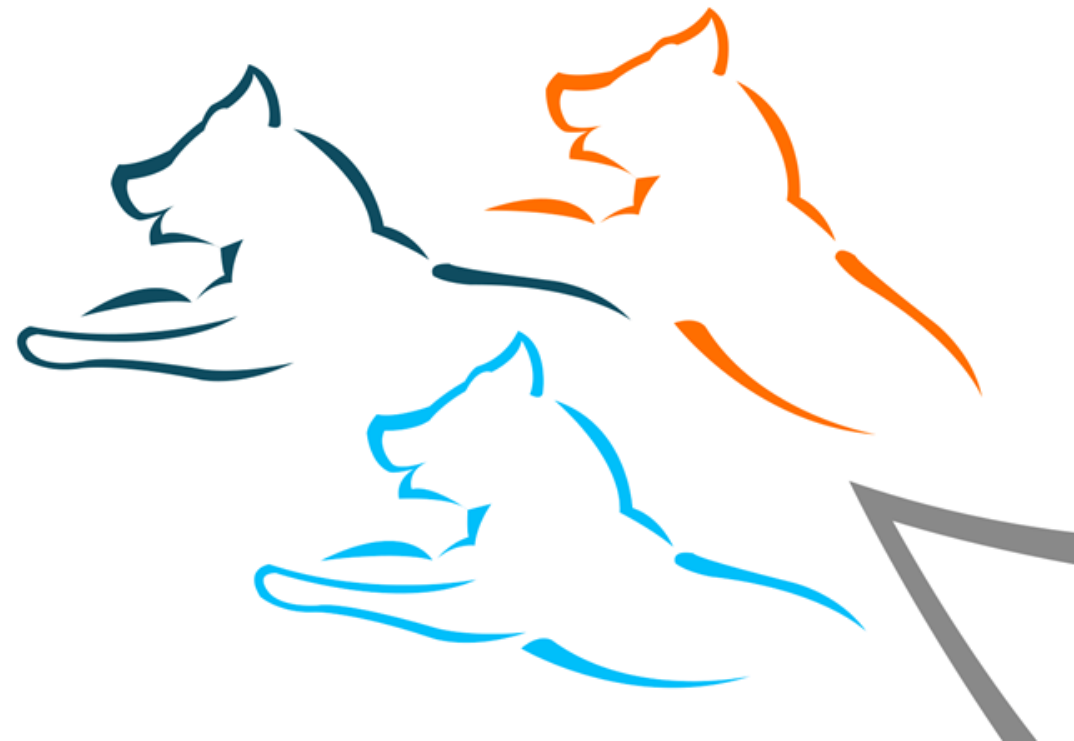
Fordelene ved PITU

- Data er standardiserede, så de kan kombineres og anvendes sammenhængende. Det betyder, at en given information kun kommer fra ét register
- Data kan som udgangspunkt frit anvendes af alle medlemmer.
- Følsomme oplysninger udveksles sikkert gennem PITU, uden at uvedkommende kan se eller påvirke data.
- PITU bygger på simpel og sikker infrastruktur, samt omkostningslav prismodel
- PITU giver bedre grundlag for fællesoffentlige samarbejde i kraft af fælles datadeling
- PITU giver bedre og nye muligheder for at udvikle nye data-baserede services og produkter
- Driftsbesparelser på myndighedernes it-systemer fx. ved at undgå lokal opdatering af data

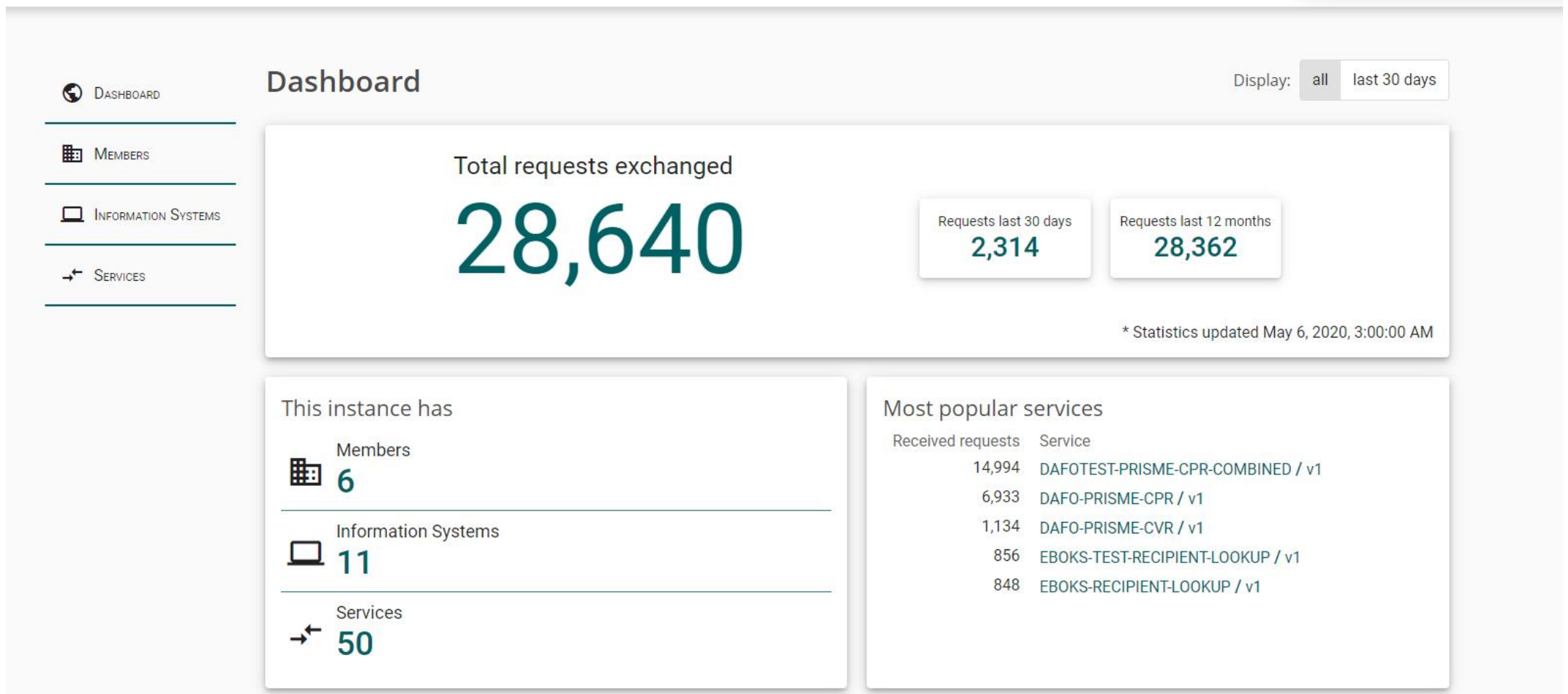


Hvad kræver et medlemskab

- Man skal anmode DIA om medlemskab. DIA vejleder om tilslutningen og det videre forløb
- Medlemmer skal underskrive en SLA og en medlemsaftale.
- PITU medlemskab koster 500 kr. pr. måned og derved 6.000 pr. år. En sikkerhedsserver koster 10.000 i engangsudgift til licens og derefter 2.000 pr. måned og derved. 24.000 pr. år.



Medlemmer og data på PITU



Pitu.data.gl – (fra dato 11/05-2020)

- Antal af udvekslet data: **28.640**
- Antal medlemmer: **6**
- Antal af information systemer: **11**
- Antal data services: **50**



Eksempler på nuværende data fra PITU (fra dato 11/05-2020)

▪ Data

- CPR
- CVR
- Adresser
- Rullende aktuel indkomst (RAI)
- Prisme
- ATP beregningsdata
- Osv.

- Besøg PITU websiden for mere info:
- Pitu.data.gl



Vil du vide mere?

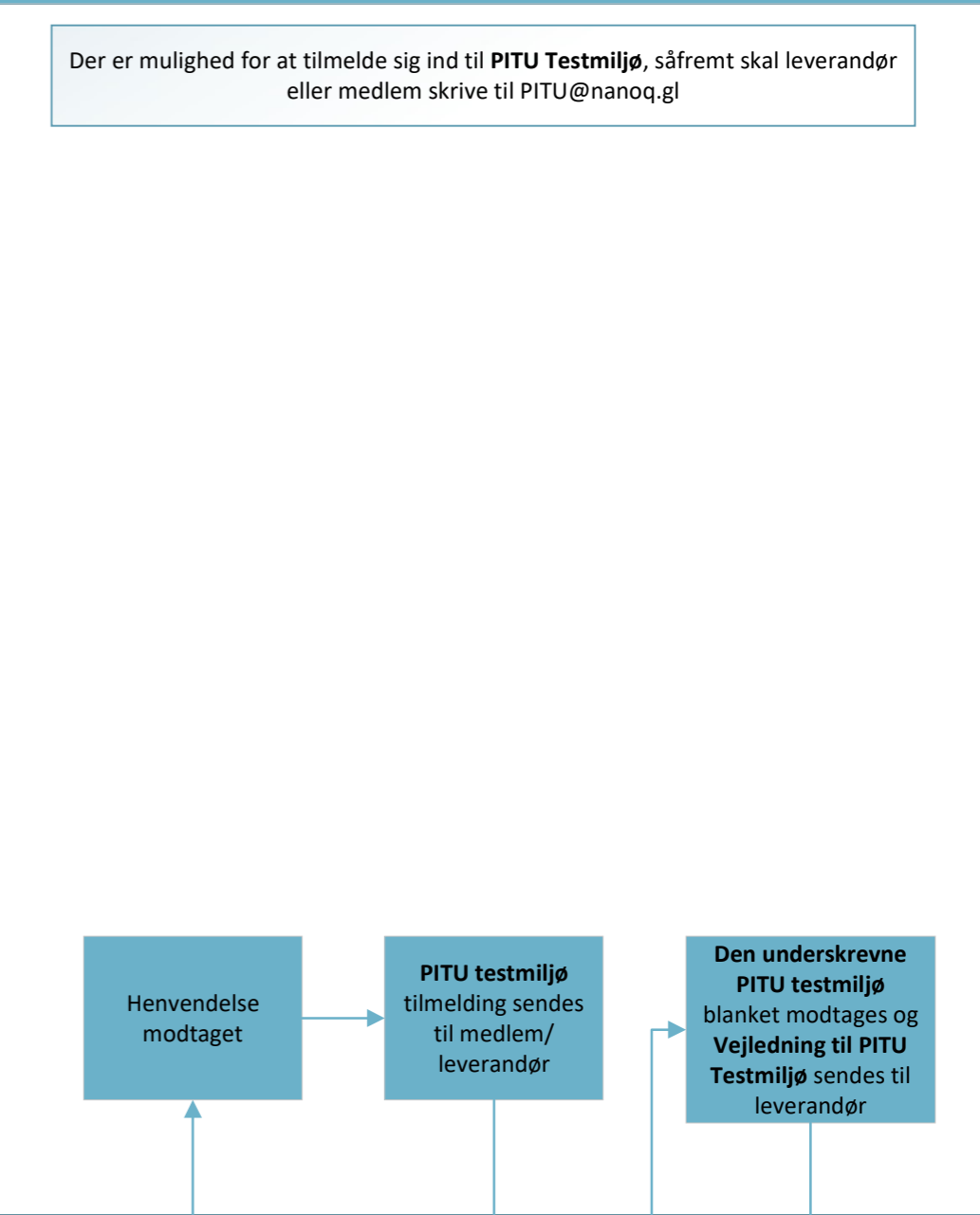
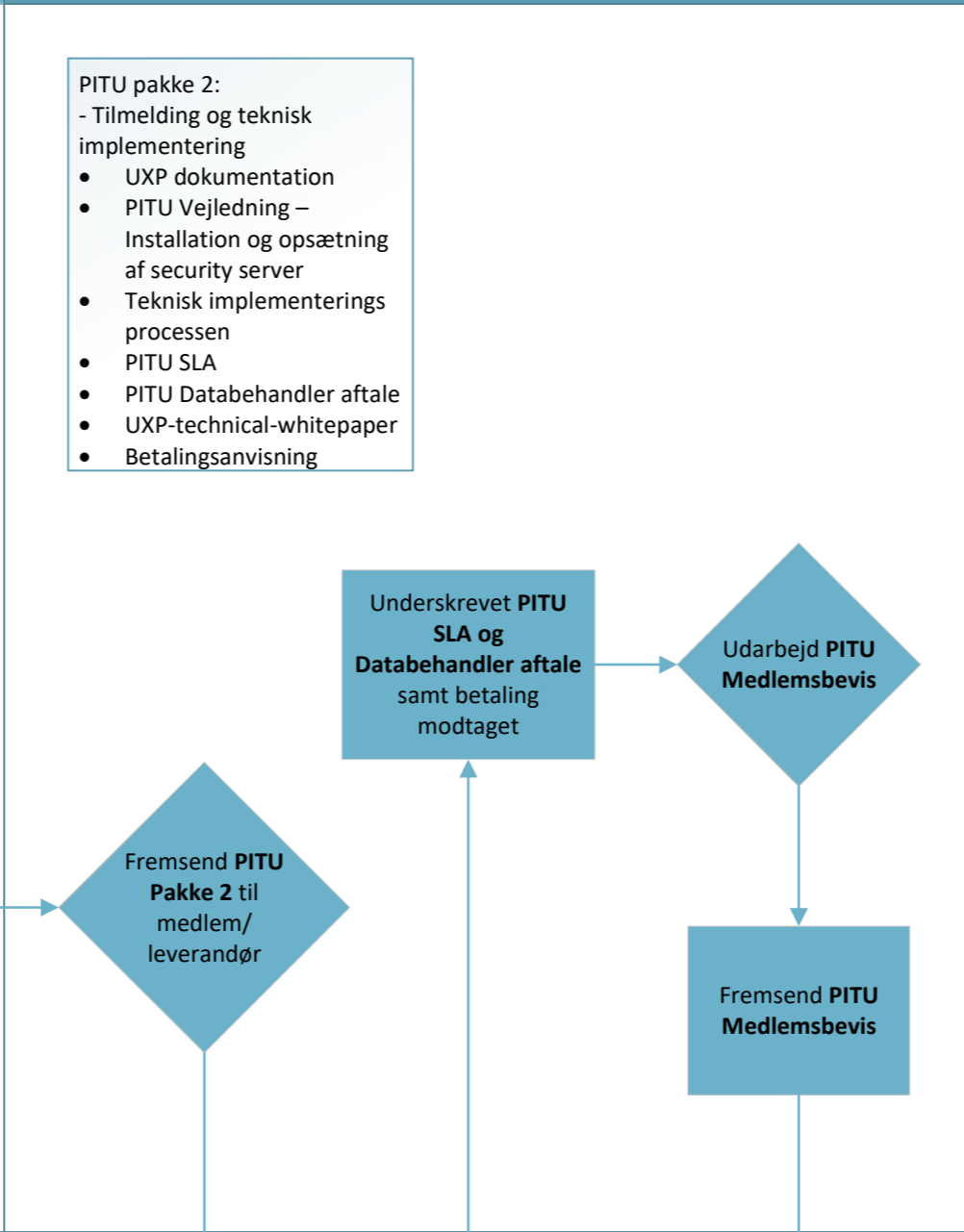
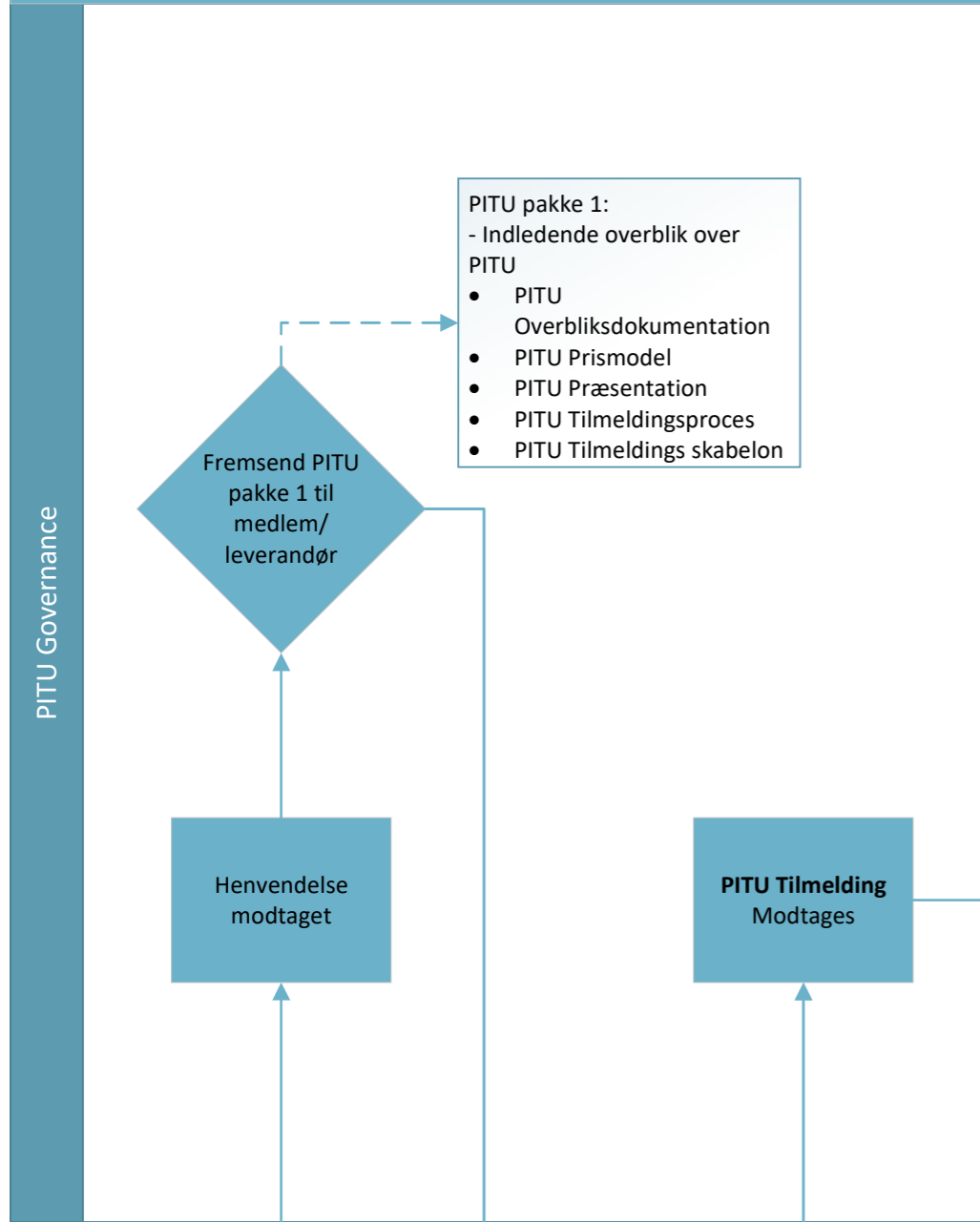
- Besøg vores informationsside på digitalimik.gl:
https://digitalimik.gl/Emner/Digitale%20Loesninger_B/Pitu?sc_lang=da
- Skriv til projektets postkasse: PITU@nanoq.gl



Fase 1. Tilmelding

Fase 2. PITU SLA

PITU Testmiljø



Fase 3. Installer PITU security server

Fase 4. Konfigurer PITU security server

Fase 5. Registrer PITU security server

PITU Governance

IT Leverandør

<UXP-repository-URL> og <UXP-repository-key-URL> afsendes til leverandør fra PITU@nanoq.gl

Bed om <UXP-repository-URL> og <UXP-repository-key-URL> via PITU@nanoq.gl

<UXP-repository-URL> og <UXP-repository-key-URL> modtages

Etabler server med administrator adgang

Installer pakker:

Udfør post-installationstjek

Webservice Pitu.data.gl

Initial konfiguration af security server

Klik på **Please enter Softtoken PIN** og indtast den ny oprettede Software Token PIN

Tilføj tidsstempling

1. Under **Configuration** vælg **System Parameters**.
2. Under **Timestamping Services** vælg **Add**
3. Vælg **UXP TSA Signer #1** i vinduet der popper op og vælg **OK**

Generer nøgler og Certificate Signing Requests

1. Login på Software Token og generer en nøgle
2. Vælg den netop generede nøgle og:
 - A. Vælg Auth for key usage;
 - B. Vælg certificeringsmyndighed
 - C. Download CSR-filen

Importer certifikater i PITU security server

Registrer i PITU arkitekturen/ Registrer under Registry Server

Godkendelse af ny PITU medlem i hjemmesiden

Sørger for at der er en valid certifikat til eget websted.

NOTE: websitet kan tilkøbes hos andre hjemmeside udbydere

1. Opret fil
2. Tilføj URL'en til UXP package repository
3. Tilføj signaturnøglen til UXP repository over listen over godkendte nøgler
4. Installer softwaren med kommandoerne

Browser giver advarsel, lav en undtagelse så serveren er godkendt også skal man klikke på samtlige OK-er

1. Log ind på hjemmesiden og upload licensfilen
2. Verificer og gem licensfilen
3. Gem licensen og upload derpå PITU Global Configuration Anchor
5. Verificer checksummen af PITU Global Configuration Anchor
7. Udfyld oplysningerne ud fra PITU Medlemsbeviset

Opbevar Software Token Pin sikkert.

Se den fulde dokument under **PITU Vejledning – Installation og opsætning ver. 01-1** eller **UXP Security Server 1.10: Installation and Configuration Guide**

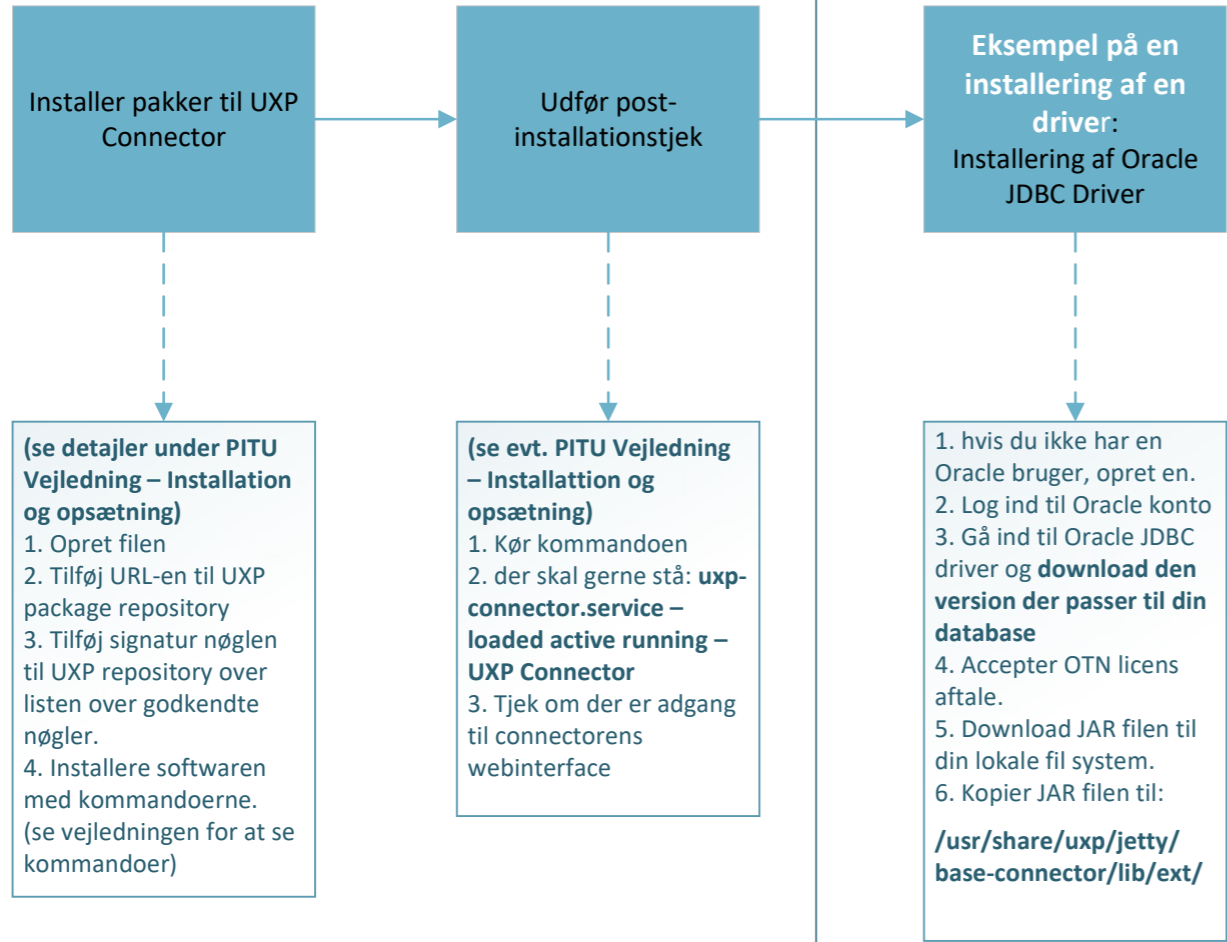


Fase 5. Installation

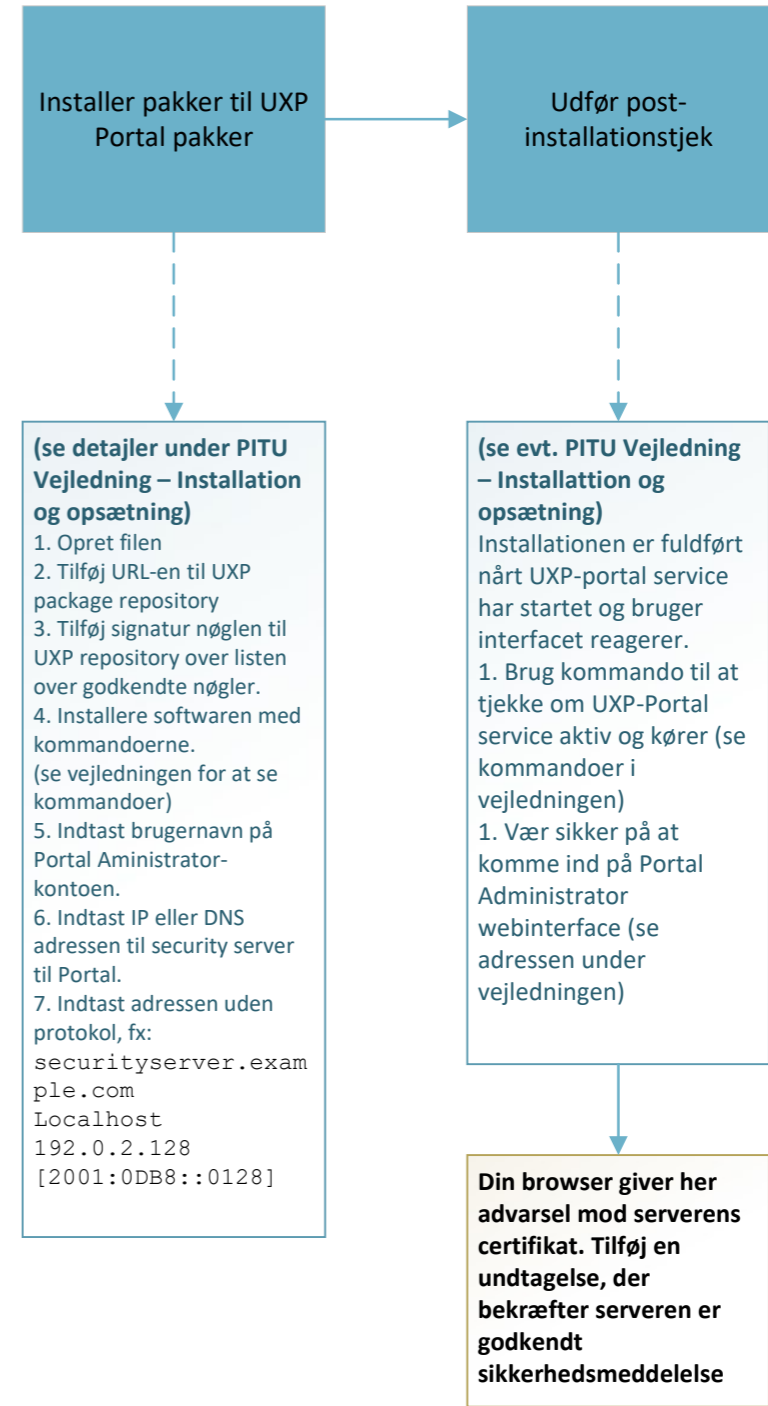
Fase 6. Konfiguration af SQL Database

I tillæg til ovenstående kan det – alt efter opsætning – være nødvendigt at åbne for porte til DNS, NTP og SSH i forbindelse med almindelig serveradministrationen.

Understøttede SQL Databaser:
Understøttede drivers er: HSQLDB, MS SQL, MySQL og PostgreSQL
Inkluderet JDBC Driver er tredje parti software released under forskellige licenser.



I tillæg til ovenstående kan det – alt efter opsætning – være nødvendigt at åbne for porte til DNS, NTP og SSH i forbindelse med almindelig serveradministrationen.



IT Leverandør

IT Leverandør

PITU VEJLEDNING

Installation og opsætning af PITU Security server, PITU Connector og PITU Portal

VERSION 0.1
PITU BETAFASE



INDHOLDSFORTEGNELSE

INDLEDNING	3
BRUGERADMINISTRATION	4
1.1 Brugerroller	4
1.2 Administration af brugere	4
INSTALLATION OG OPSÆTNING AF PITU SECURITY SERVER	5
1. Installer PITU Security server	6
1.1. Etabler server med administratoradgang	6
1.2. Installer pakker	7
1.3. Udfør post-installationstjek	7
2. Konfigurer PITU Security server	8
2.1. Initial konfiguration af Security server	8
2.2. Tilføj tidsstempeling	11
3. Registrer PITU Security server	12
3.1. Generer nøgler og Certificate Signing Requests	12
3.2. Anmod om certifikater	12
3.3. Importer certifikater i PITU Security server	12
3.4. Registrer i PITU arkitekturen	12
INSTALLATION OG OPSÆTNING AF PITU CONNECTOR	13
1. Minimumskrav	13
2. Installation	13
2.1 Installer pakker til UXP Connector	13
2.2 Udfør post-installationstjek	13
3. Konfiguration af SQL Database	14
3.1 Understøttede SQL Databaser	14
3.2 Installering af Oracle JDBC driver	14
INSTALLATION OG OPSÆTNING AF PITU PORTAL	15
1. Minimumskrav	15
2. Installation af UXP Portal pakker	15
2.1 Installer UXP Portal software	15
2.2 Udfør post-installationstjek	16
Opsætning	16
ORDLISTE	16

INDLEDNING

Denne vejledning henvender sig til nye PITU-medlemmer i forbindelse med etablering af opkobling til PITU-netværket. Vejledningen berører emnerne

- Installation og opsætning af PITU Security server
- Installation og opsætning af PITU Connector
- Installation og opsætning af PITU Portal

PITU er funderet på Unified eXchange Platform[®], UXP udviklet af estiske Cybernetica AS. UXP er en videreudvikling af det estiske X-Road. Denne vejledning henviser løbende til UXP-manualerne:

- UXP Security Server 1.10 - Installation and Configuration Guide, Version 1.10.2
- UXP Security Server 1.10 - User Guide, Version 1.10.2
- UXP Connector 1.3 - Installation Guide, Version 1.3.3
- UXP Connector 1.3 - User Guide, Version 1.3.3
- UXP Portal 1.2 - Installation Guide, Version 1.2.3
- UXP Portal 1.2 - User Guide, Version 1.2.3

Vejledningerne må gerne deles med eventuel(le) it-leverandør(er). Der er en ordliste bagerst i vejledningen.

BRUGERADMINISTRATION

1.1 Brugerroller

- **Sikkerhedsofficer** (uxp-security-officer) er ansvarlig for sikkerhedspolitik, sikkerhedskrav og herunder styring af nøgleindstillinger, nøgler og certifikater.
- **Registreringsofficer** (uxp-registration-officer) er ansvarlig for registrering og fjernelse af Security serverklinter.
- **Service administrator** (uxp-service-administrator) styrer data om og adgangsrettigheder til services.
- **System administrator** (uxp-system-administrator) er ansvarlig for installering, konfiguration og vedligeholdelse af Security serveren.

En bruger kan have flere roller og flere brugere kan være i samme rolle. Hver rolle har en tilsvarende systemgruppe, oprettet ved installering af systemet. Dette indikerer at hver bruger har brug for roller til at udføre specifikt aktion.

1.2 Administration af brugere

Brugeradministration bliver udført i kommandolinje i root brugerrettigheder.

Til at tilføje en ny bruger, indtast denne kommando:

```
adduser <username>
```

For at give privilegier til den ny bruger, indtast den følgende kommando som fx:

```
adduser <username> uxp-security-officer  
adduser <username> uxp-registration-officer  
adduser <username> uxp-service-administrator  
adduser <username> uxp-system-administrator
```

For at fjerne privilegier til den bruger som du har oprettet, fjern brugeren fra den systemgruppe som fx:

```
deluser <username> uxp-security-officer
```

Brugerrettigheder bliver anvendt kun efter man har genstartet upx-jetty service.

For at fjerne brugeren, indtast:

```
deluser <username>
```

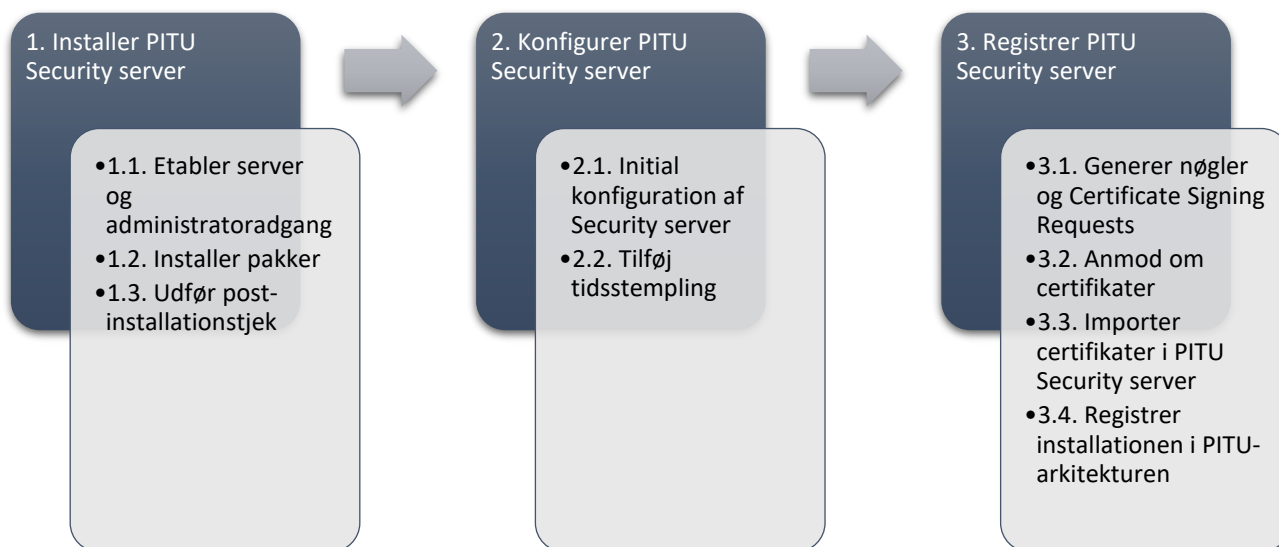
INSTALLATION OG OPSÆTNING AF PITU SECURITY SERVER

Installation og opsætning af PITU Security server følger i store træk beskrivelsen i UXP Security Server 1.10 - Installation and Configuration Guide, Version 1.10.2.

Opsætning af en PITU Security server forudsætter følgende:

-
- UXP repository URL
 - UXP repository key URL
 - Licenser til UXP-komponenterne
 - PITU Global Configuration Anchor
 - PITU Global Configuration Anchor hash
 - Din PITU Medlemsklasse
 - Din PITU Medlemskode
 - Din PITU Security serverkode
-

Opsætning af PITU Security server sker i følgende trin:



1. Installer PITU Security server

1.1. Etabler server med administratoradgang

1. Opsæt en server med følgende specifikationer

PITU Security server		
Minimum hardwarekrav (gerne VM)	CPU 2 core 64bit x86 RAM 4GB HDD 10GB til installation + minimum 50GB til transaktionslogs, mere på Security servere med meget trafik.	
Operativsystem	Ubuntu 18.04 LTS 64bit	
Åbne netværksporte	Porte til indgående forbindelser (TCP)	
	Port	Network scope Formål
	4000	PRIVATE Adgang til webinterface
	80	PRIVATE HTTP forbindelser fra informationssystemer
	443	PRIVATE HTTPS forbindelser fra informationssystemer
	5500	PUBLIC Udveksling mellem Security servere
	5577	PUBLIC Forespørgsler på OCSP-meddelelser mellem Security servere
	5599	PUBLIC Forespørgsler på aktive krypteringscertifikater mellem Security servere
	Porte til udgående forbindelser (TCP)	
	Port	Network scope Formål
	80	PRIVATE HTTP forbindelser fra informationssystemer
	443	PRIVATE HTTPS forbindelser fra informationssystemer
	4400	PRIVATE Serviceanmodninger til PITU Connector
	5500	PUBLIC Udveksling mellem Security servere
	5577	PUBLIC Forespørgsler på OCSP-meddelelser mellem Security servere
	5599	PUBLIC Forespørgsler på aktive krypteringscertifikater mellem Security serverer
	4001	PUBLIC Forespørgsler til PITU Register

I tillæg til ovenstående kan det – alt efter opsætning – være nødvendig at åbne for porte til DNS, NTP og SSH i forbindelse med almindelig serveradministrationen.

2. Tilføj en bruger

```
sudo adduser <username>
```

Denne bruger bliver under installationen af PITU Security server givet administratorrettigheder.

Bemærk at brugernavnet `uxp` er reserveret til interne processer og derfor ikke kan bruges.

1.2. Installer pakker

1. Opret filen

```
/etc/apt/sources.list.d/uxp.list
```

2. Tilføj URL'en til UXP package repository

```
deb <UXP-repository-URL> trusty main
```

3. Tilføj signaturnøglen til UXP repository over listen over godkendte nøgler

```
wget -qO - <UXP-repository-key-URL> | sudo apt-key add -
```

4. Installer softwaren med kommandoerne

```
sudo apt update
```

```
sudo apt install uxp-securityserver
```

Oplysninger om <UXP-repository-URL> og <UXP-repository-key-URL> fås ved henvendelse til PITU@nanog.gl.

1.3. Udfør post-installationstjek

1. Kør kommandoen

```
systemctl list-units -t service "uxp-*
```

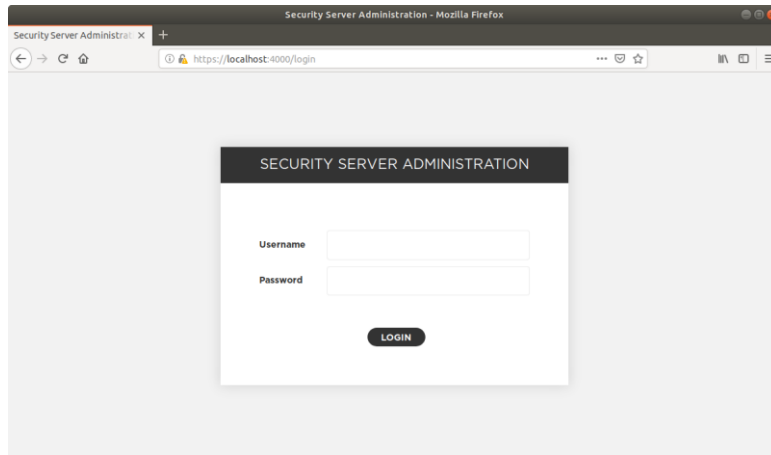
Et skærmbillede lignende dette, skal gerne komme frem

```
pitu@PITU: ~  
Fil Redigér Vis Søg Terminal Hjælp  
pitu@PITU:~$ systemctl list-units -t service "uxp-*"  
UNIT                                LOAD    ACTIVE    SUB    DESCRIPTION  
uxp-confclient.service             loaded active    running    UXP Global Configuration Client  
uxp-jetty.service                  loaded active    running    UXP Proxy UI  
uxp-monitor.service                loaded active    running    UXP Proxy Monitor  
uxp-proxy.service                  loaded activating auto-restart    UXP Message Proxy  
uxp-signer.service                 loaded active    running    UXP Message Signer  
  
LOAD    = Reflects whether the unit definition was properly loaded.  
ACTIVE  = The high-level unit activation state, i.e. generalization of SUB.  
SUB     = The low-level unit activation state, values depend on unit type.  
  
5 loaded units listed. Pass --all to see loaded but inactive units, too.  
To show all installed unit files use 'systemctl list-unit-files'.  
pitu@PITU:~$
```

2. Tjek ligeledes, at der er adgang til Security serverens webinterface via adressen

`https://<security-server>:4000/`

hvor `<security-server>` erstattes af Security serverens adresse. Følgende vindue skal komme frem

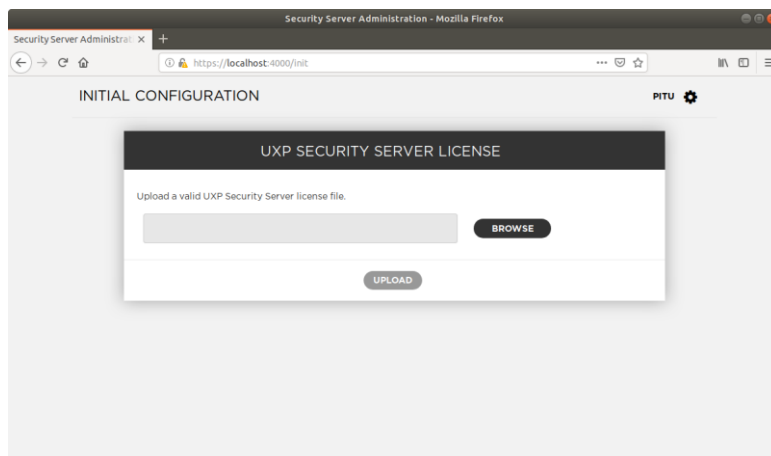


Din browser giver her advarsel mod serverens certifikat. Tilføj en undtagelse, der bekræfter serveren er godkendt sikkerhedsmeddelelse

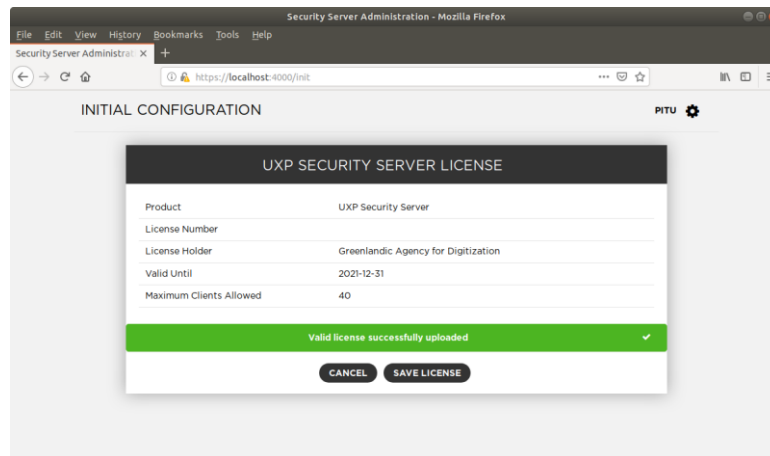
2. Konfigurer PITU Security server

2.1. Initial konfiguration af Security server

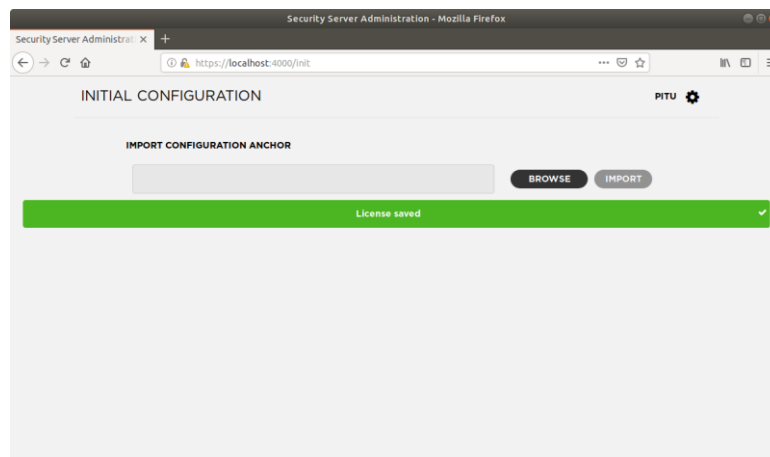
1. Log ind og upload licensfilen:



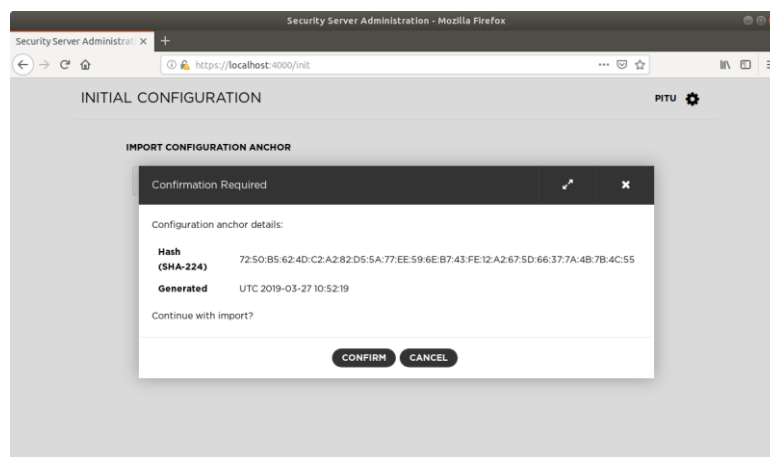
2. Verificer og gem licensfilen:



3. Gem licensen og upload derpå PITU Global Configuration Anchor



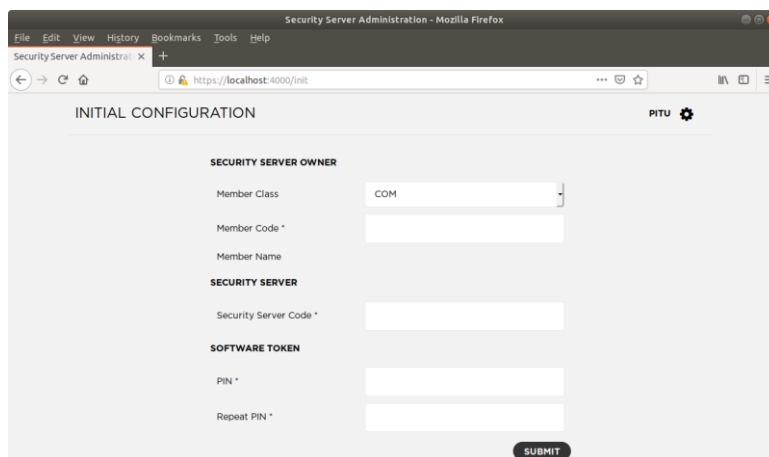
4. Verificer checksummen af PITU Global Configuration Anchor (SHA-224).



Checksummen kan også verificeres via terminalen ved:

```
sha224sum *.xml
```

5. Udfyld oplysningerne ud fra PITU Medlemsbeviset



INITIAL CONFIGURATION

SECURITY SERVER OWNER

Member Class: COM

Member Code *

Member Name

SECURITY SERVER

Security Server Code *

SOFTWARE TOKEN

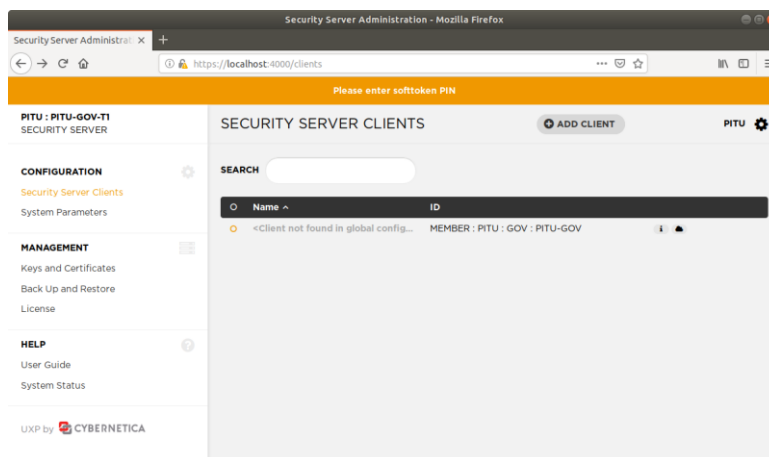
PIN *

Repeat PIN *

SUBMIT

Opbevar Software Token PIN sikkert. Den skal bruges til at tilgå nøgler gemt i Software Token fremadrettet. Software Token PIN skal kan ikke nulstilles eller genskabes.

6. Følg linket i den gule tekst **Please enter softtoken PIN.**



Security Server Administration - Mozilla Firefox

Security Server Administration: X

https://localhost:4000/clients

Please enter softtoken PIN

PITU: PITU-GOV-TI
SECURITY SERVER

CONFIGURATION

Security Server Clients

System Parameters

MANAGEMENT

Keys and Certificates

Back Up and Restore

License

HELP

User Guide

System Status

UXP by CYBERNETICA

SECURITY SERVER CLIENTS

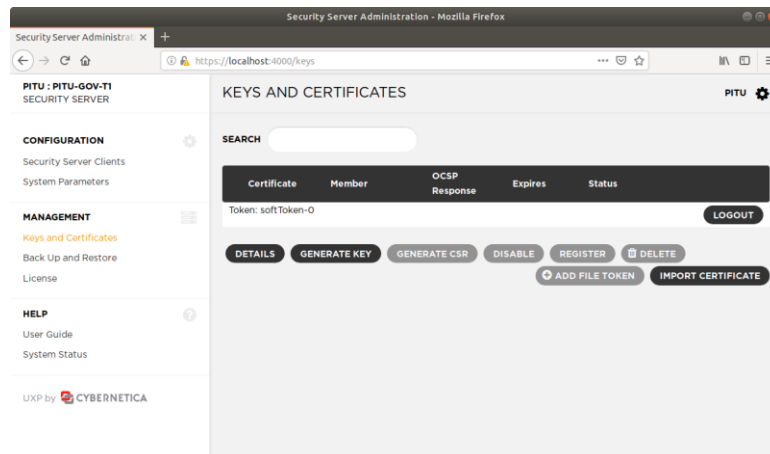
ADD CLIENT

PITU

SEARCH

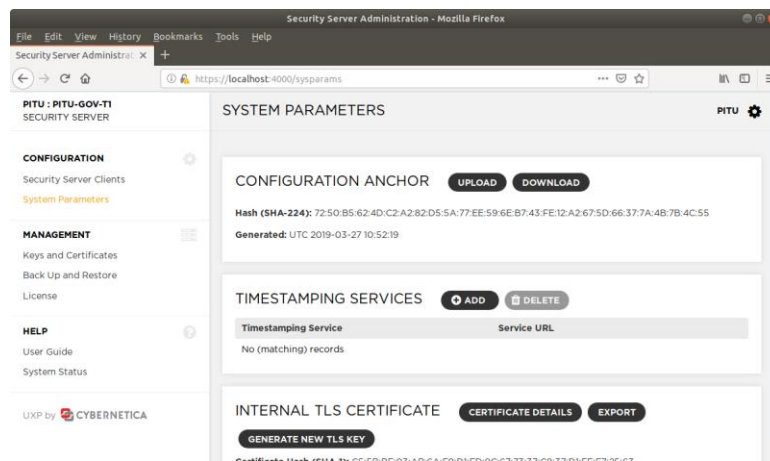
Name ^	ID
<Client not found in global config...	MEMBER: PITU: GOV: PITU-GOV

7. Indtast den netop oprettede Software Token PIN.

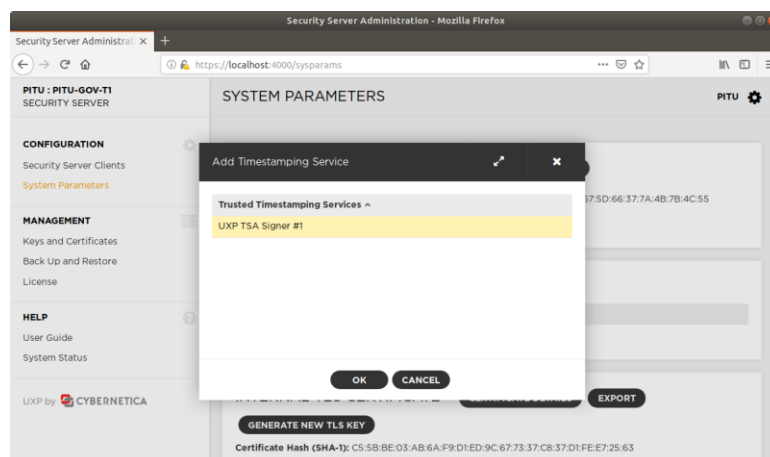


2.2. Tilføj tidsstempeling

1. Under **Configuration** vælg **System Parameters**.
2. Under **Timestamping Services** vælg **Add**.



3. Vælg **UXP TSA Signer #1** i vinduet der popper op og vælg **OK**.



3. Registrer PITU Security server

Sidste trin i installation og opsætning af en PITU Security server er certificering og registrering. PITU opererer med to typer certifikater:

1. Et certifikat til signering
2. Et certifikat til autentificering

Begge certifikater skal erhverves ved en certificeringsmyndighed. I PITU varetages certificering af PITU Governance.

3.1. Generer nøgler og Certificate Signing Requests

CSR til et autentificeringscertifikat:

1. Login på Software Token og generer en nøgle
2. Vælg den netop genererede nøgle og:
 - a. Vælg **Auth** for key usage;
 - b. Vælg certificeringsmyndighed
 - c. Download CSR-filen

3.2. Anmod om certifikater

3.3. Importer certifikater i PITU Security server

3.4. Registrer i PITU arkitekturen

INSTALLATION OG OPSÆTNING AF PITU CONNECTOR

1. Minimumskrav

PITU Connector		
Minimum hardwarekrav (gerne VM)	CPU 2 core 64bit x86 RAM 4GB HDD 10GB til installation + minimum 50GB til transaktionslogs, mere på Security servere med meget trafik.	
Operativsystem	Ubuntu 18.04 LTS 64bit	
Åbne netværksporte	Porte til indgående forbindelse (TCP)	
	Port	Network scope Formål
	4400	PRIVATE Adgang til webinterface

I tillæg til ovenstående kan det – alt efter opsætning – være nødvendig at åbne for porte til DNS, NTP og SSH i forbindelse med almindelig serveradministrationen.

2. Installation

2.1 Installer pakker til UXP Connector

1. Opret filen

```
/etc/apt/sources.list.d/uxp.list
```

2. Tilføj URL'en til UXP package repository

```
deb <UXP-repository-URL> trusty main
```

3. Tilføj signaturnøglen til UXP repository over listen over godkendte nøgler

```
wget -qO - <UXP-repository-key-URL> | sudo apt-key add -
```

4. Installer softwaren med kommandoerne

```
sudo apt update
```

```
sudo apt install uxp-connector
```

2.2 Udfør post-installationstjek

1. Kør kommandoen

```
systemctl list-units -t service "uxp-*
```

Forventet output skal gerne stå som

```
uxp-connector.service    loaded active running    UXP Connector
```


2. Tjek ligeledes, at der er adgang til connectorens webinterface via adressen

<https://<connector-address>:4400/>

hvor <connector-address> erstattes af Security serverens adresse. Følgende vindue skal komme frem

Din browser giver her advarsel mod serverens certifikat. Tilføj en undtagelse, der bekræfter serveren er godkendt sikkerhedsmeddelelse

3. Konfiguration af SQL Database

3.1 Understøttede SQL Databaser

Understøttede drivers er: HSQLDB, MS SQL, MySQL og PostgreSQL

Inkluderet JDBC Driver er tredje-parti software released under forskellige licenser

Database	JDBC Driver	Licens
HSQLDB	HSQLJDBC v.2.3.2	BSD License
MS SQL	jTDS v.1.3.1	GNU LGPL
MySQL	MariaDB Connector/J v.1.5.8	GNU LGPL
PostgreSQL	PostgreSQL JDBC v.9.4.1209	BSD-2-Clause License

3.2 Installering af Oracle JDBC driver

1. Hvis du ikke har en Oracle bruger, opret en.
2. Logge ind til Oracle konto.
3. Går til Oracle JDBC Driver download side og søge for den driver version egnet til dine database.
4. Accepterer den OTN Licens aftale.
5. Download JAR filen til din lokale fil system.
6. Kopierer den downloadet fil til

`/usr/share/uxp/jetty/base-connector/lib/ext/`

INSTALLATION OG OPSÆTNING AF PITU PORTAL

1. Minimumskrav

Minimum hardwarekrav (gerne VM)	CPU 2 core 64bit x86 RAM 4GB HDD 10GB til installation + minimum 50GB til transaktionslogs, mere på Security servere med meget trafik.									
Operativsystem	Ubuntu 18.04 LTS 64bit									
Åbne netværksporte	Porte til indgående forbindelser (TCP)									
	<table><thead><tr><th>Port</th><th>Network scope</th><th>Formål</th></tr></thead><tbody><tr><td>4600</td><td>PRIVATE</td><td>Adgang til webinterface</td></tr></tbody></table>	Port	Network scope	Formål	4600	PRIVATE	Adgang til webinterface			
Port	Network scope	Formål								
4600	PRIVATE	Adgang til webinterface								
	Porte til udgående forbindelser (TCP)									
	<table><thead><tr><th>Port</th><th>Network scope</th><th>Formål</th></tr></thead><tbody><tr><td>80</td><td>PRIVATE</td><td>HTTP forbindelser fra informationssystemer</td></tr><tr><td>443</td><td>PRIVATE</td><td>HTTPS forbindelser fra informationssystemer</td></tr></tbody></table>	Port	Network scope	Formål	80	PRIVATE	HTTP forbindelser fra informationssystemer	443	PRIVATE	HTTPS forbindelser fra informationssystemer
Port	Network scope	Formål								
80	PRIVATE	HTTP forbindelser fra informationssystemer								
443	PRIVATE	HTTPS forbindelser fra informationssystemer								

I tillæg til ovenstående kan det – alt efter opsætning – være nødvendig at åbne for porte til DNS, NTP og SSH i forbindelse med almindelig serveradministrationen.

2. Installation af UXP Portal pakker

2.1 Installer UXP Portal software

1. Opret filen

```
/etc/apt/sources.list.d/uxp.list
```

2. Tilføj URL'en til UXP package repository

```
deb <UXP-repository-URL> trusty main
```

3. Tilføj signaturnøglen til UXP repository over listen over godkendte nøgler

```
wget -qO - <UXP-repository-key-URL> | sudo apt-key add -
```

4. Installer software med kommandoerne

```
sudo apt update
```

```
sudo apt install uxp-portal
```

5. Indtast brugernavn på Portal Administrator-kontoen

6. Indtast IP eller DNS adressen til Security server til Portal

Indtast adressen uden protokol, fx

```
securityserver.example.com  
localhost
```

```
192.0.2.128  
[2001:0DB8::0128]
```

2.2 Udfør post-installationstjek

Installationen er fuldført når UXP-portal service har startet og bruger interfacet reagerer.

1. Brug følgende kommando til at tjekke om UXP-Portal service er aktiv og kører,

```
systemctl list-units | grep -E "^uxp-"  
(forventet output er):
```

```
uxp-portal.service    loaded active running    UXP Portal
```

2. Være sikker på komme ind på Portal Administrator webinterface på <https://<portal-address>:4600/admin>

Din browser giver her advarsel mod serverens certifikat. Tilføj en undtagelse, der bekræfter serveren er godkendt sikkerhedsmeddelelse

Opsætning

ORDLISTE

REST

SOAP

PITU Periferi

PITU Kerne

PITU Medlemsbevis

PITU Medlemsklasse

PITU Medlemskode

PITU Medlemsklasse

PITU Security serverkode

PITU Global Configuration Anchor

PITU Governance

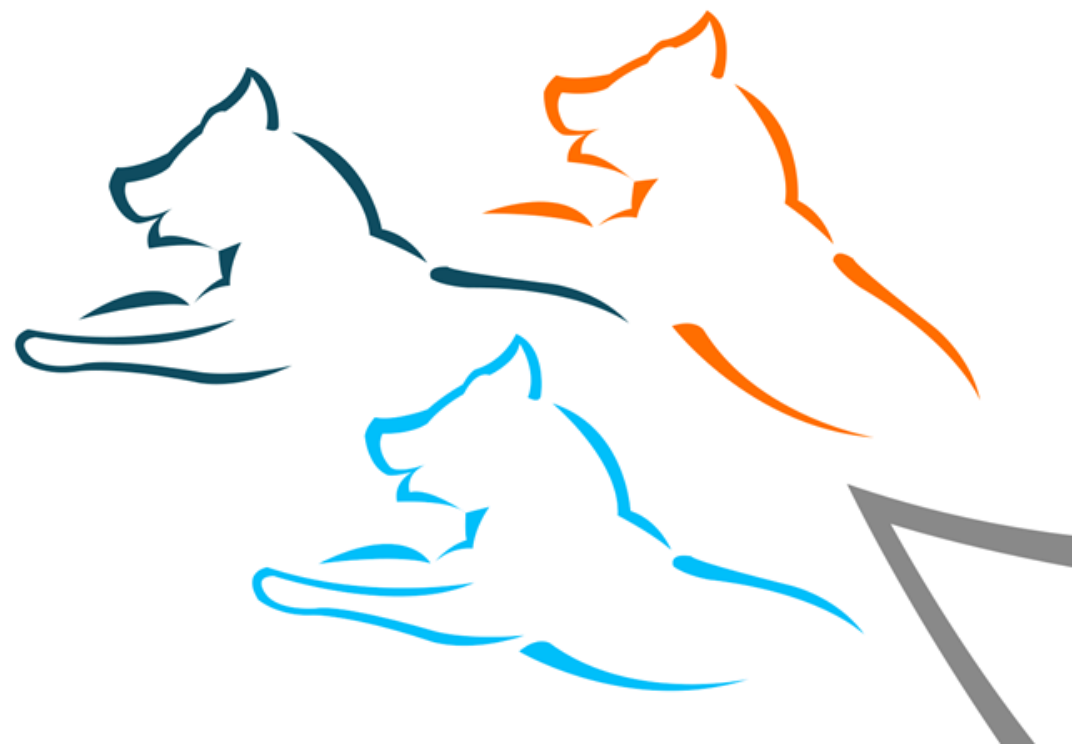
VM

Vejledningen er udarbejdet af Digitaliseringsstyrelsen.

PITU

Digitaliseringsstyrelsen

April 2020



VINKLER PÅ PITU

- PITU-visionen
- PITU/UXP-arkitekturen
- Status på PITU
- Juridiske aspekter af PITU
- IT-branchens rolle i PITU
- Principper for udrulning af PITU
- PITU, Grunddata og Sullissivik
- Governance, drift og finansiering
- Eksempel: En arbejdsgangsskitse



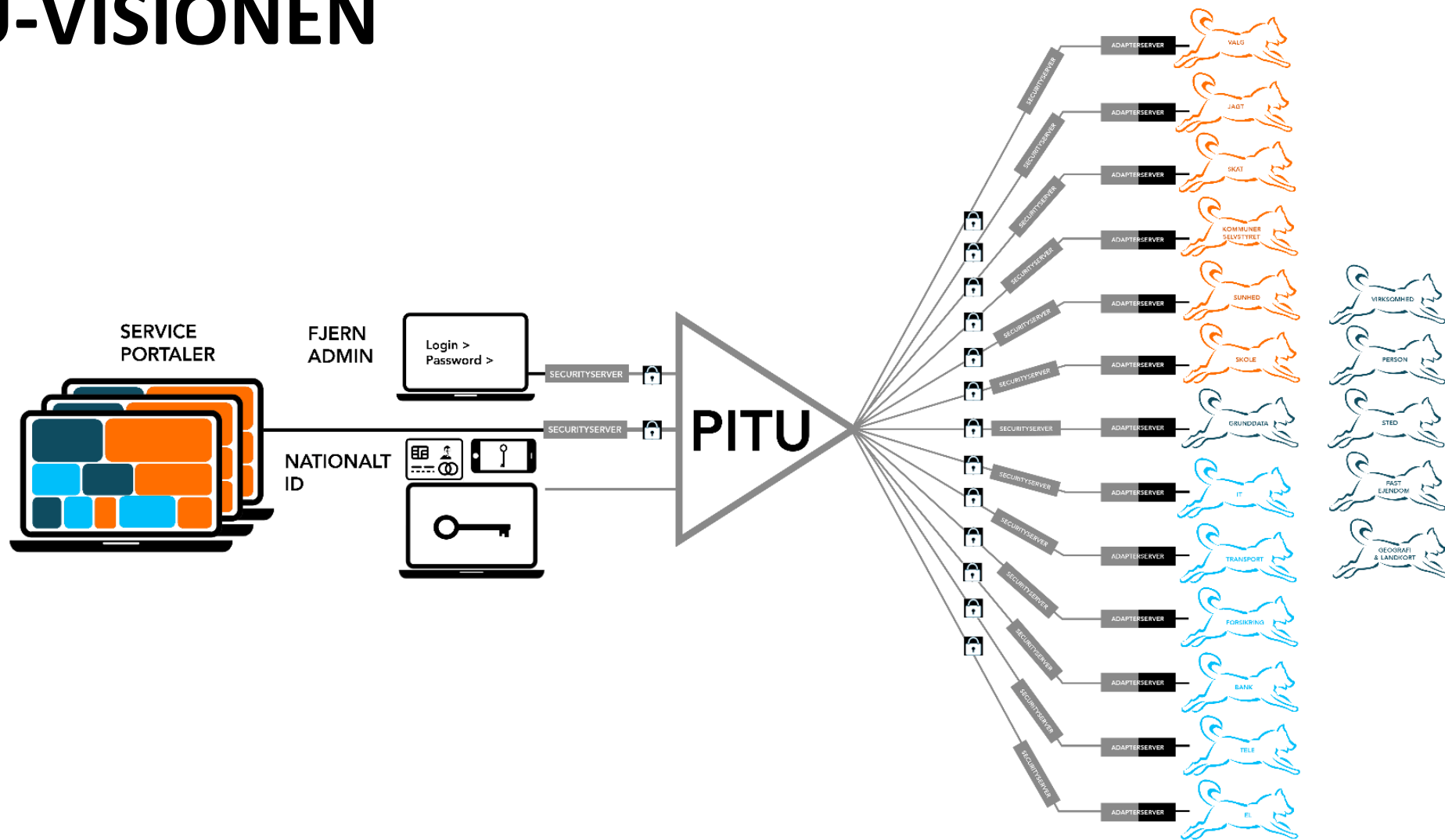
PITU-VISIONEN

Pitu er det grønlandske ord for den forreste rem på en hundeslæde. Remmen skaber bindeled mellem hundeslæden og hundene. En enkel – men helt afgørende – anordning der sikrer, at hundenes skagler samles og fastgøres, så føreren kan styre dem i den rigtige retning. Naalakkersuisut anvender denne metafor og betegnelse for den nye grønlandske platform til dataudveksling.

Digitaliseringsstrategien



PITU-VISIONEN



PITU-VISIONEN

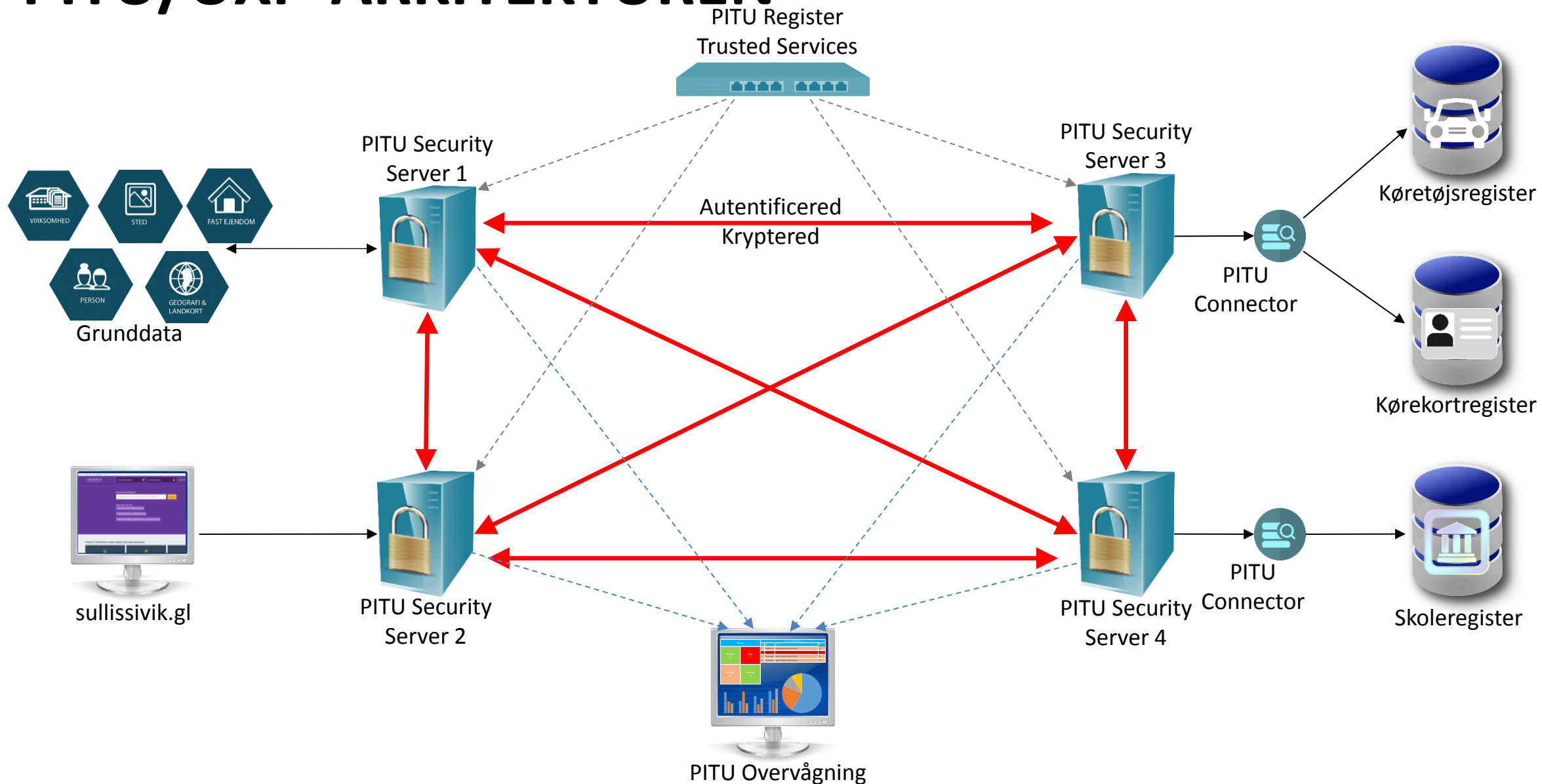
Målsætning 5.a.

50% af alle offentlige registre udveksler data via PITU

Digitaliseringsstrategien



PITU/UXP-ARKITEKTUREN



PITU/UXP-ARKITEKTUREN

PITU Register

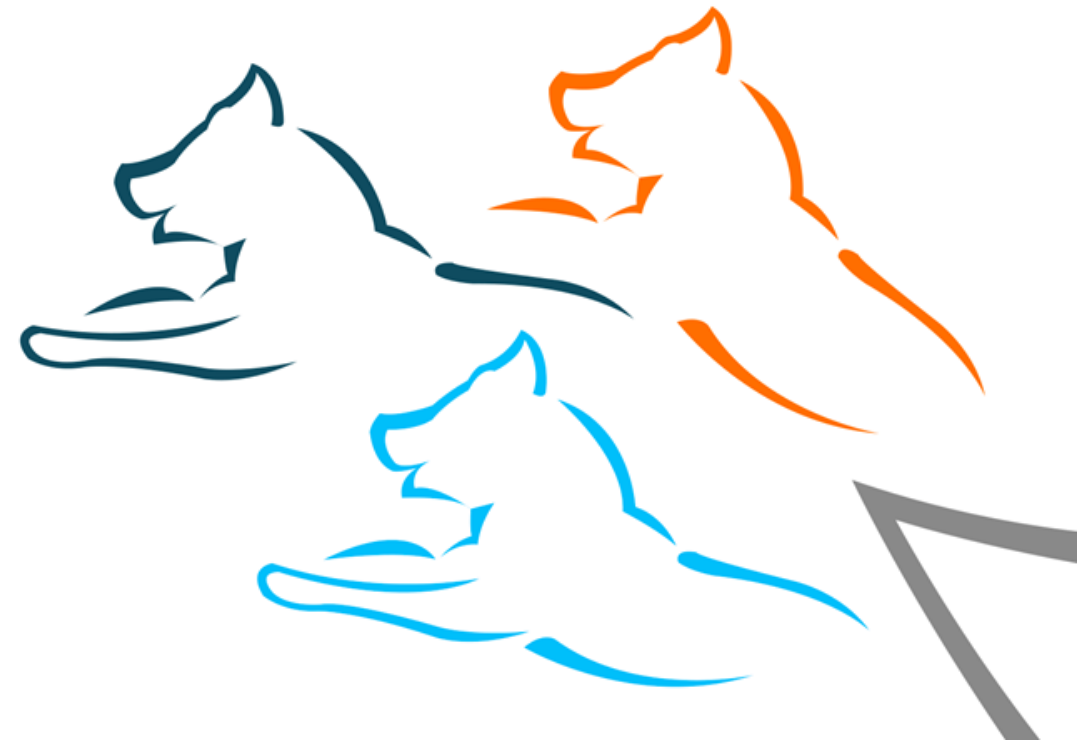
- Administrerer tilsluttede medlemmer og sikkerhedsservere: Navne, IP-adresser, certifikater, kontakter osv.
- Godkendte Trust Service-udbydere: Certificering- og tidsstemplings-myndighed
- PITU registeret gør systemet skalerbart - nye organisationer og
- sikkerhedsservere kan nemt tilføjes, certifikater kan nemt opdateres mv.



PITU/UXP-ARKITEKTUREN

PITU Security Server

- Enkelt kontrolpunkt for alle indgående og udgående tjenester
- Giver ensartet sikkerhedsniveau til alle tjenester og informationsudvekslinger
- Peer-to-peer-krypteret kommunikation
- Digitalt signeret bevisførelse for alle informationsudvekslinger



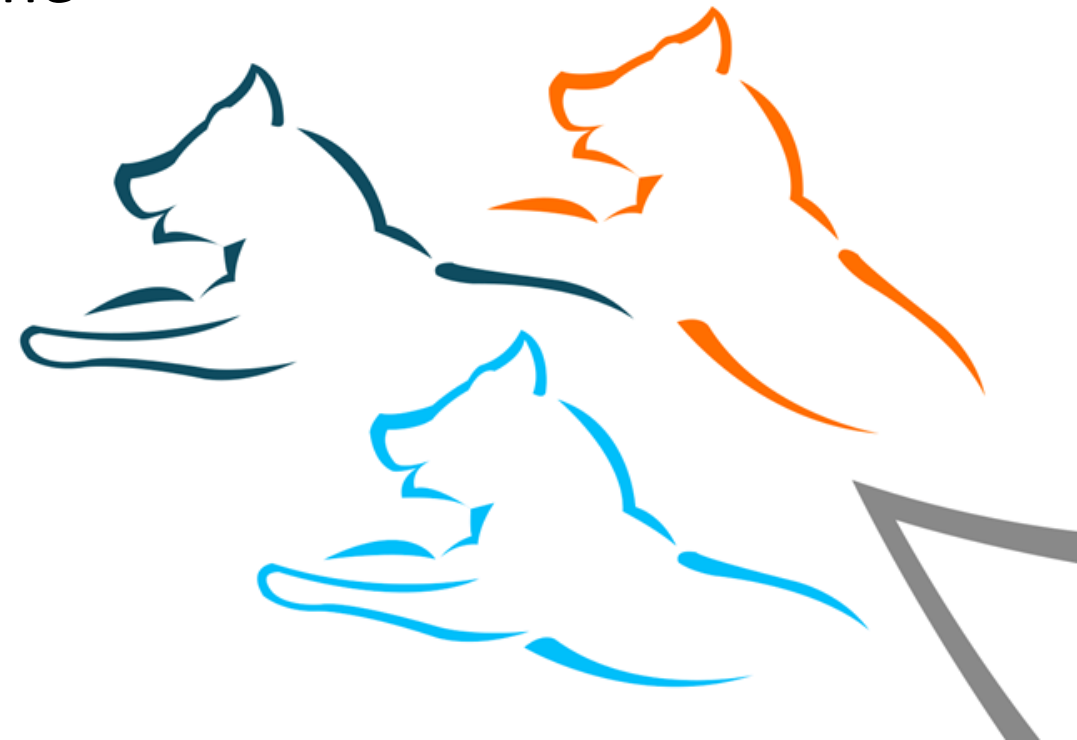
PITU/UXP-ARKITEKTUREN

PITU Connector

- Integreret værktøj til hurtig udvikling af tjenesterne ved at definere database forespørgsler samt til levering af tjenesterne
- Browserbaseret udviklingsmiljø

PITU Portal

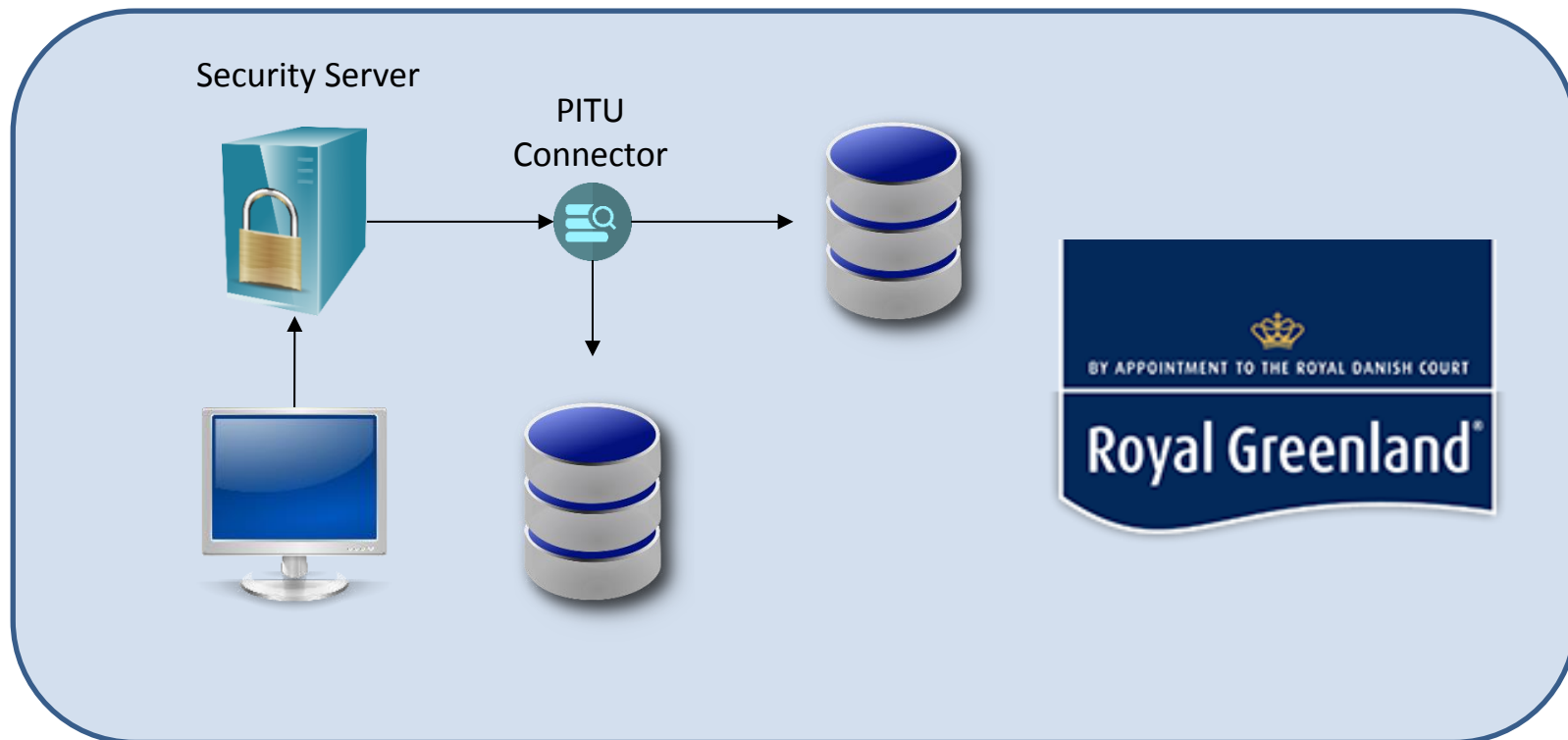
- Webportal, der kan konsumere en service



PITU/UXP-ARKITEKTUREN - TÆNKT USE CASE



AKILERAARTARNERMUT AQUTSISOQARFIK
SKATTESTYRELSEN TAX AGENCY



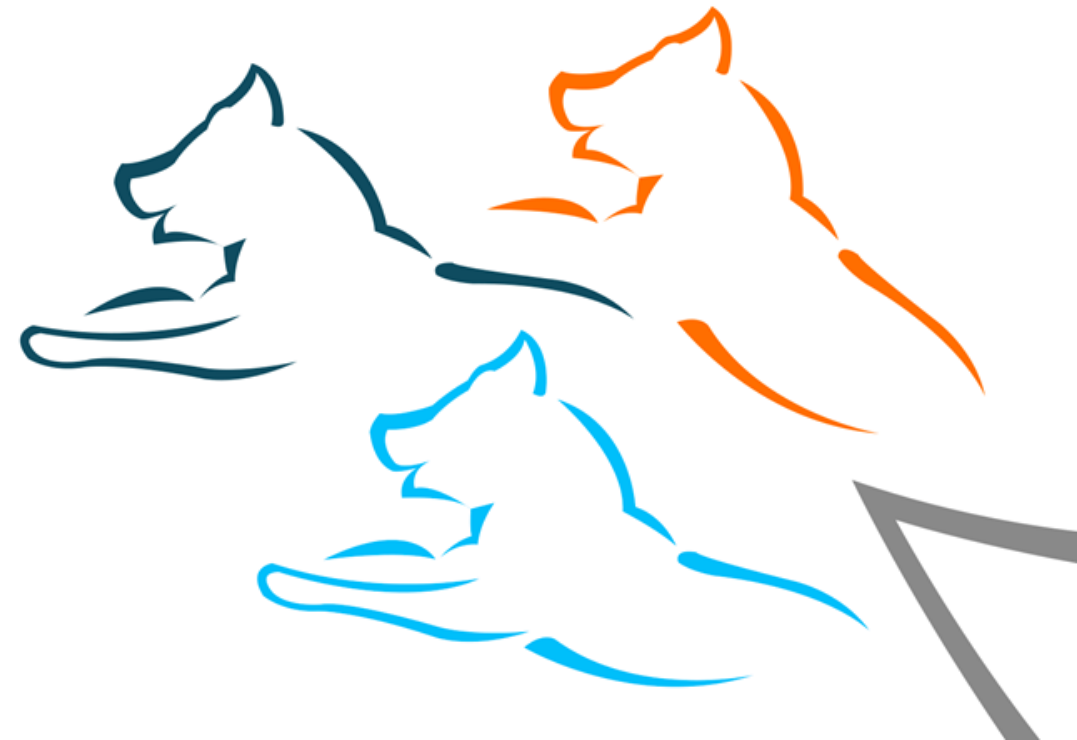
STATUS PÅ PITU

Status

- PITUs kernekomponenter er installeret og i drift
- Et testmiljø er etableret og er i brug
- PITU er i overgang til drift

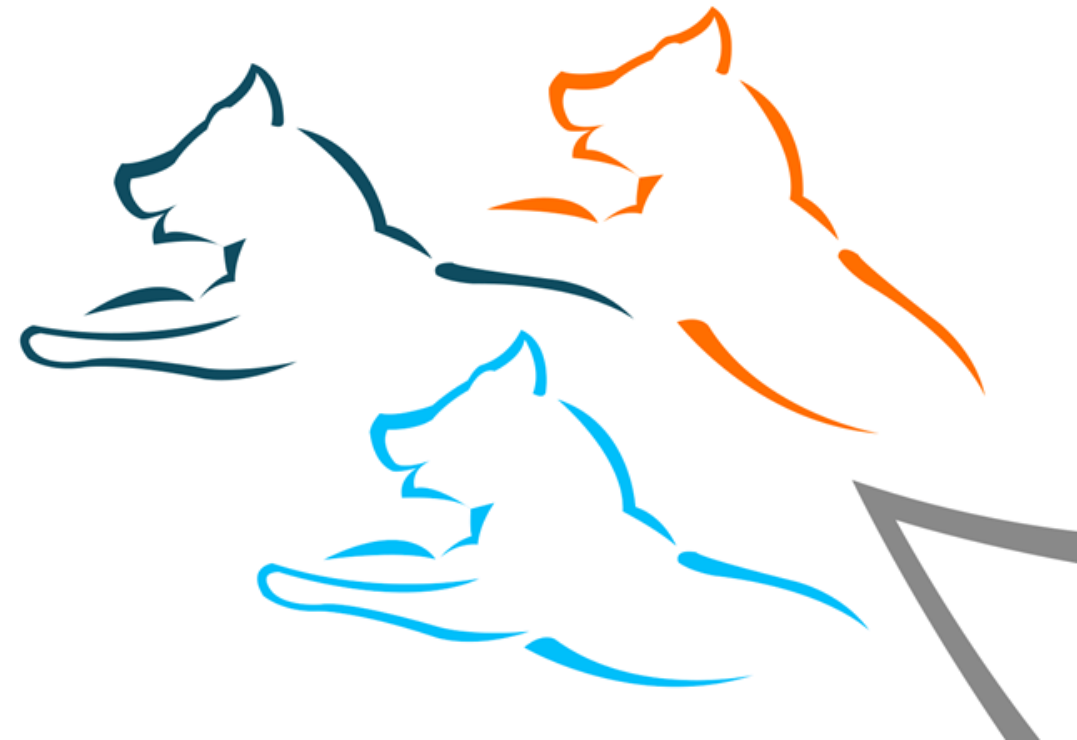
Se oversigt over services og medlemmer

- pitu.data.gl



JURIDISKE ASPEKTER AF PITU

- PITU er infrastruktur
 - ... ikke en datakilde
- En offentlig myndighed, virksomhed eller forening bliver ”medlem” af PITU
- To slags medlemmer:
 - Forbrugere
 - Udbydere
- Et medlem kan både være forbruger og udbyder



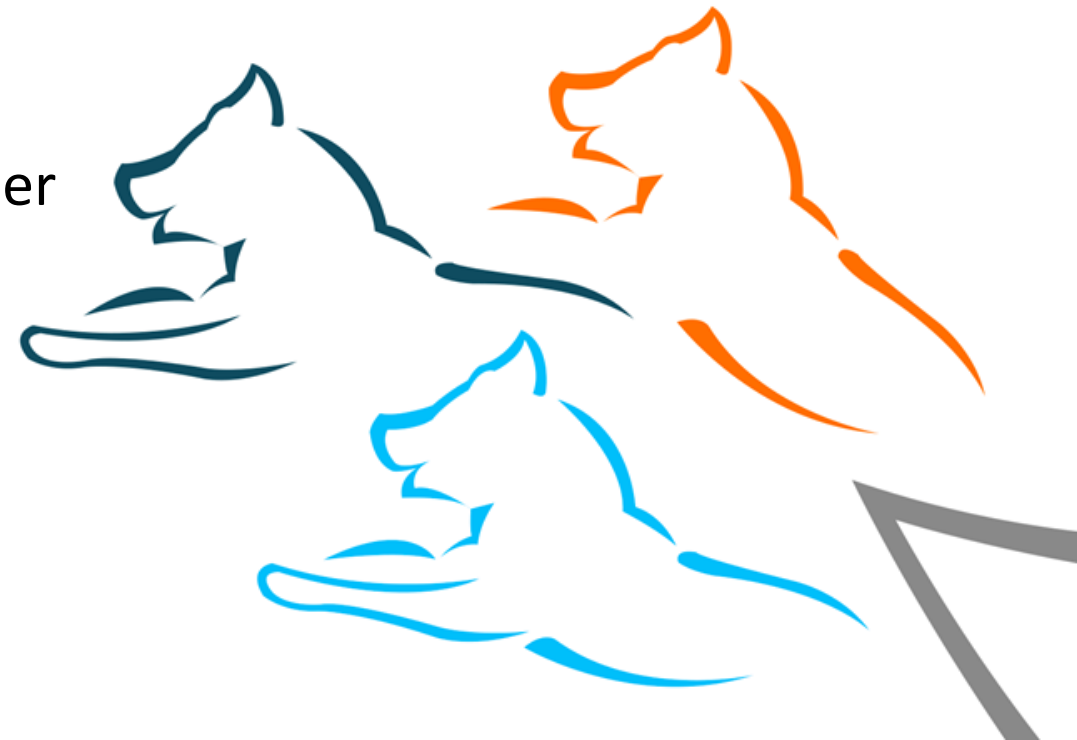
JURIDISKE ASPEKTER AF PITU

- Medlemmer skal underskrive en PITU SLA
- PITU SLA opdateres takt med udrulningen af PITU
- Vejledning til nye medlemmer er lavet
- PITU forudsætter bilaterale aftaler mellem medlemmer om dataudveksling
- PITU erstatter ikke almindelige aftaler mellem en leverandør og et medlem



IT-BRANCHENS MULIGHEDER MED PITU

- PITU standardiserer udvekslingen af data mellem medlemmer
- Let at udvikle nye løsninger
- To typer opgaver i relation til PITU (for nuværende)
 1. Udviklingsopgaver for medlemmer – herunder tilpasning af eksisterende systemer
 2. Hosting/administration af servere



PRINCIPPER FOR UDRULNING AF PITU

Drift

- PITU skal bruges
- Kommunikationsstrategien hviler på gode use cases

Viden

- Sparringskompetence opbygges internt i PITU-gruppen
- PITU-kompetence skal opbygges blandt lokale leverandører
- Ressortansvar, dataejerskab og sikkerhed

Volumen

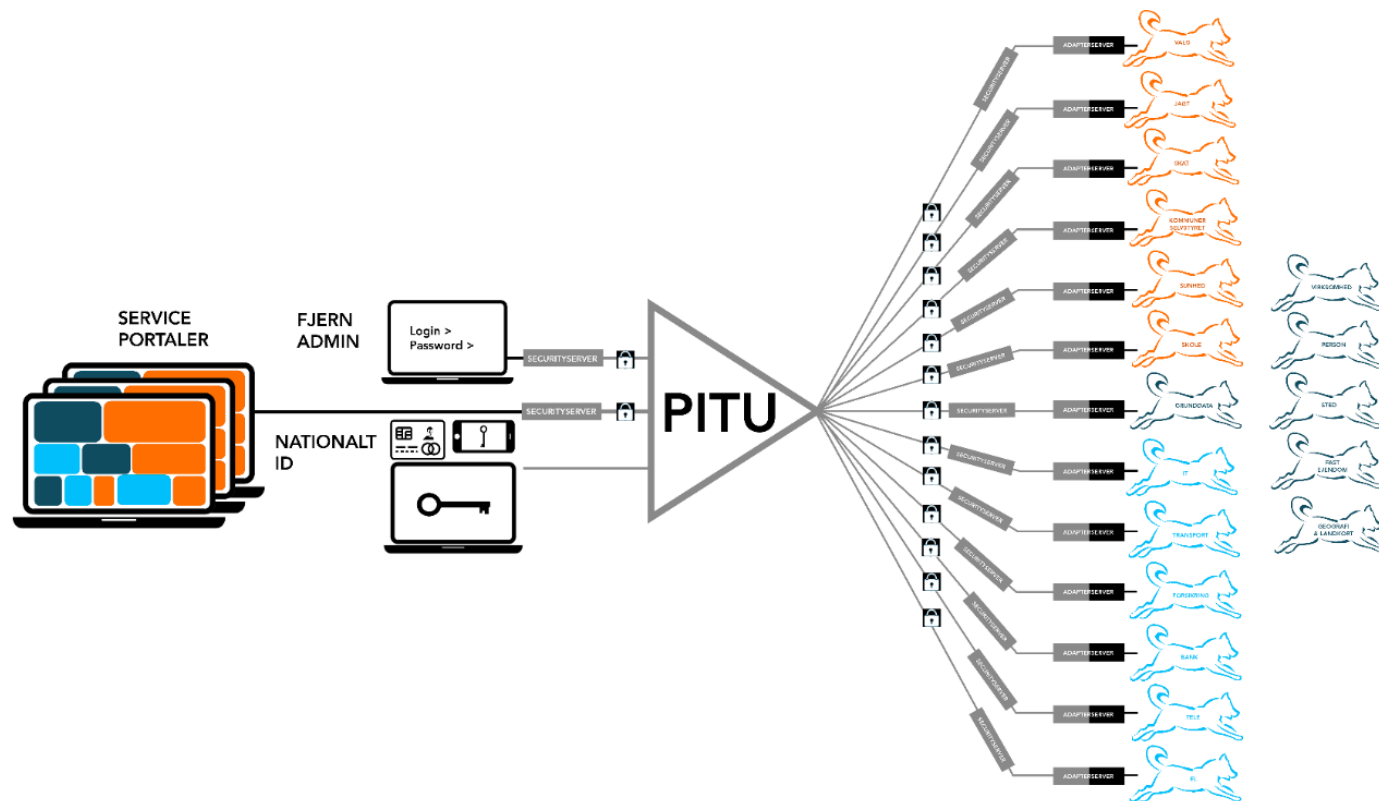
- Fokus på cases med gensidige dataudvekslinger – ”noget-for-noget”
- PITU-lobbyarbejde hos igangværende projekter
- Digitale forudsætningsprojekter

Neutralitet

- PITU er infrastruktur – aftaler om udvekslinger sker efter overenskomst mellem PITU-medlemmer
- PITU må ikke forvride markedet med krav eller fordele til enkelte

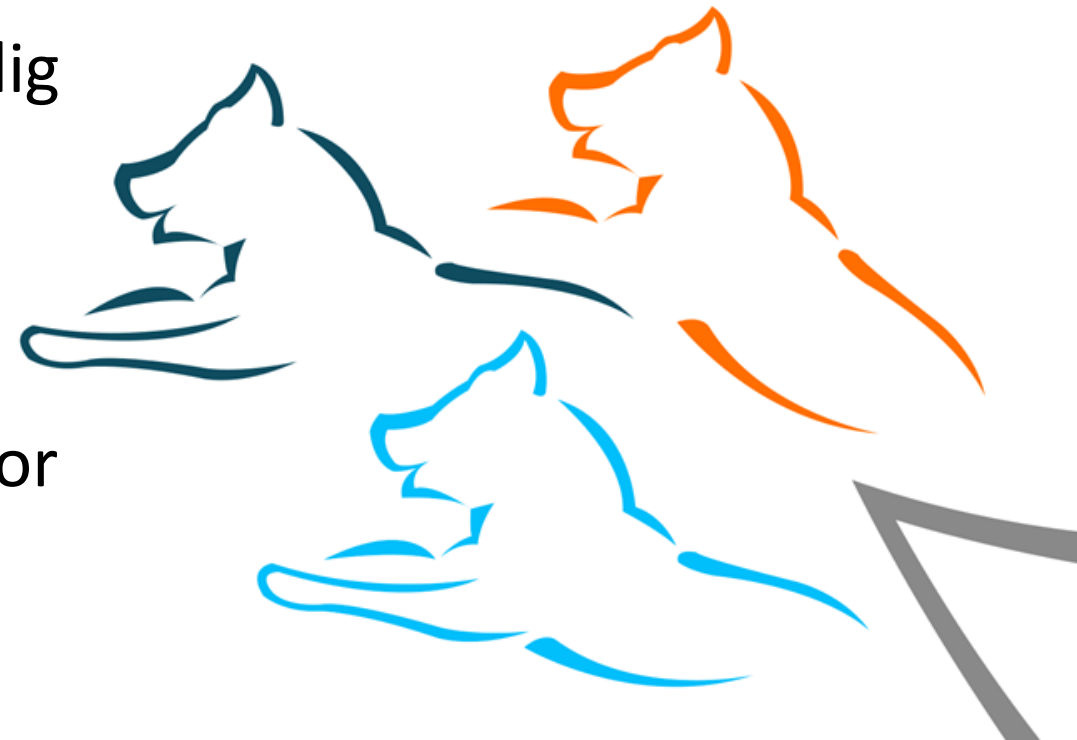
PITU, GRUNDDATA OG SULLISSIVIK

- Digitaliseringsstyrelsen har flere roller
 1. Etablering af PITU
 2. PITU Governance
 3. Sullissivik
 4. Udbyder af Grunddata
 5. Vejledningsforpligtigelse

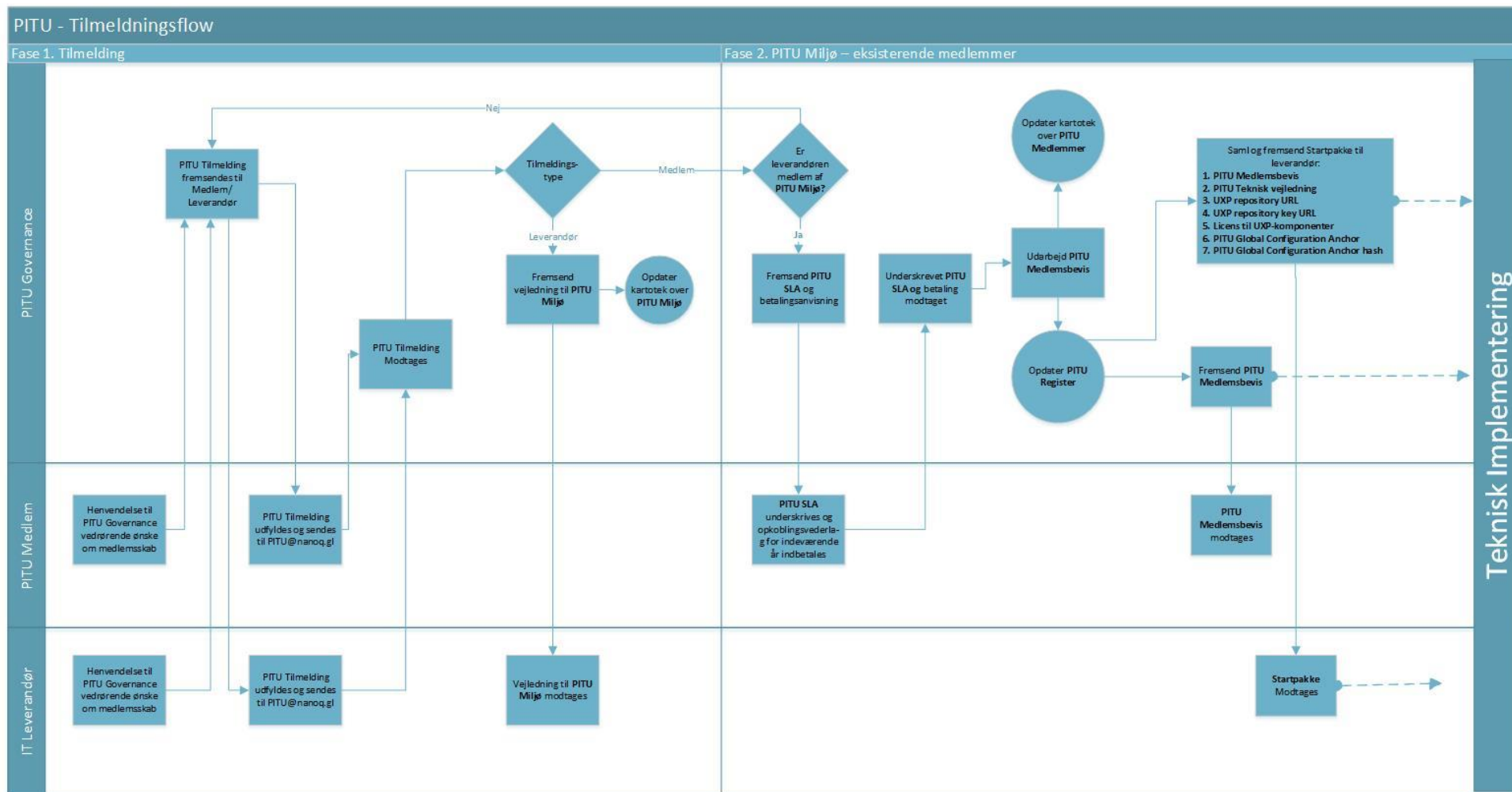


GOVERNANCE, DRIFT OG FINANSIERING

- Færøske erfaringer: Det tekniske kan løses - governance og jura er det virkeligt tidskrævende
- PITU skal – måske – tænkes sammen med det driften af det kommende fællesoffentlig ERP-system
- Den endelige finansieringsmodel for PITU skal på plads
- Jo større PITU-netværk des større behov for tilgængelighed og overvågning



EKSEMPEL: EN ARBEJDSGANGSSKITSE



Hvad er næste skridt?

- PITU kommer i drift
- Nye medlemmer skal kobles på inde i PITU
- Borgerne kommer til at bruge Min Side i Sullissivik, hvor de får adgang til deres data, det vil ske via Pitu.
- PITU har en prismodel, som gør at jo flere medlemmer jo lavere pris.



Naalakkersuisut
Government of Greenland
Digitaliseringsstyrelsen



DIGITALIMIK
SULLISSINERMUT
AQUTSISOQARFIK

Til IT leverandører & IT ansvarlige

PITU IT leverandør online workshop 27. Maj 2020

Program

- Kl. 08:30: - Velkomst og introduktion – Styrelseschef Katrine Hjelholt Nathanielsen
Kl. 08:45: - Overordnet præsentation over PITU – Projektleder Cecilie Marie Jakobsen
Kl. 09:15: - Cybernetica præsenterer PITU arkitekturen
Kl. 10:00: - 10 min pause
Kl. 10:15: - Heldin – Lilly Dam Hanssen fra Færøerne
Kl. 10:45: - Magenta deler konkrete erfaringer:
- Hvordan kom Magenta ind på PITU?
- Et eksempel på planlægning at få en service på PITU
- Eksempler på adgangsstyring i PITU
Kl. 12:15 – Pause
Kl. 13:00 – Afrunding

Fremgangsmåde:

Spørgsmål skal stilles pr. mail eller efter oplæg.
Mail: ceja@nanoq.gl

Inussiamersumik inuulluaqqusillunga

Med venlig hilsen

Projektleder

Cecilie Marie Jakobsen (Digitaliseringsstyrelsen)

Toqq/direkte 563238

ceja@nanoq.gl



Brev dato:

Sags nr. 2017 - 26159
Akt. nr. 13758779

Postboks 1078
3900 Nuuk
Tel. (+299) 34 50 00

E-mail: digitalisering@nanoq.gl
www.naalakkersuisut.gl