Utdanningsdirektoratet

Integrasjon med SAS – nye PAS

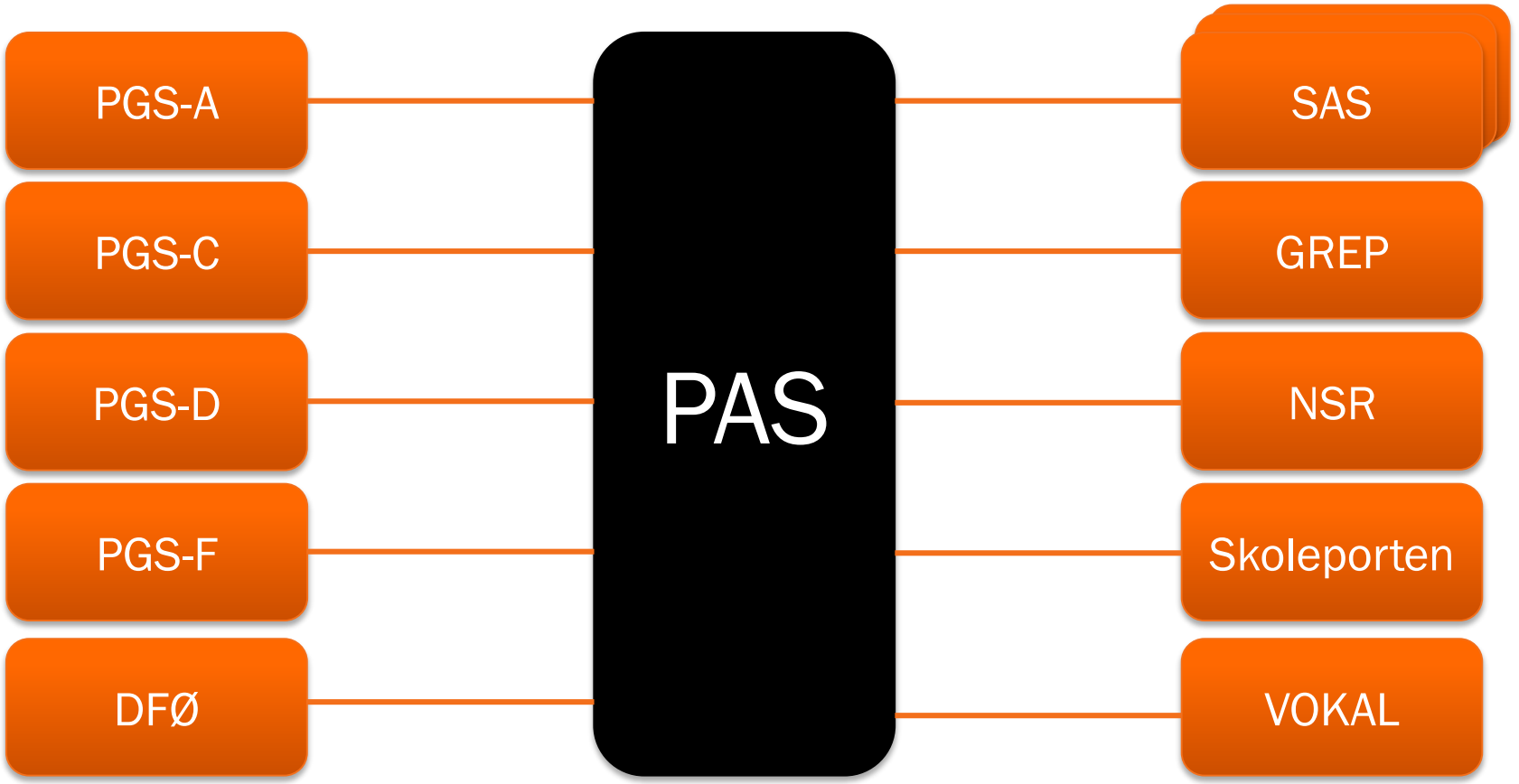
Møte med SAS leverandører 04.02.15

Vidar Kongsli
Espen Ekvang

Agenda

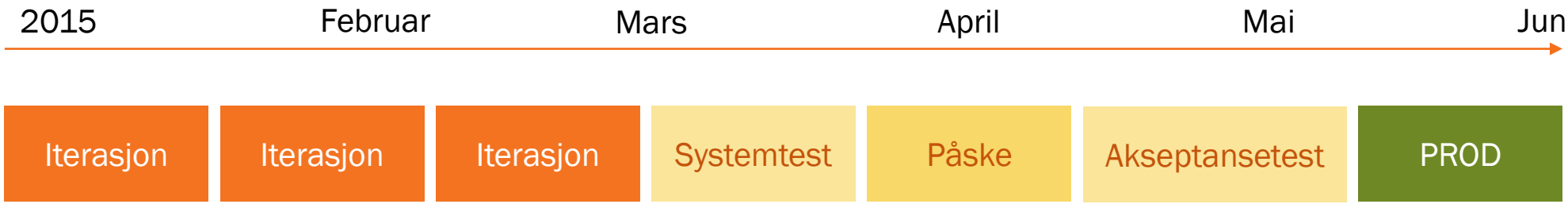
- Overordnet tidsplan
- Funksjonell beskrivelse
- Integrasjonsprinsipper
- Forslag til sikkerhetsmekanisme
- Nye og eksisterende PAS

PAS har integrasjoner med flere systemer



Tidsplan

Tidsplan



- Høsteksamen (sentral) skal gjennomføres i nye PAS

Krav til SAS leverandører

- Integrasjon mot nytt grensesnitt i nye PAS på plass før sommeren 2015

Funksjonalitet

Funksjonell beskrivelse

Hovedmål:

Gjenskape dagens funksjonalitet mellom PAS og SAS

Delmål:

Øke robusthet og datakvalitet i PAS

Dagens funksjonalitet:

- Hente ut eksamensdefinisjoner
- Melde på kandidater
- Etterpåmelding
- Hente ut resultater
- Melde inn fagpersoner

Integrasjonsprinsipper

HTTP-basert API

- Ressursbasert
- Maskin-til-maskin kommunikasjon
- Platformuavhengig
- «Pragmatisk» REST (Representational State Transfer)
  - Level 2 Richardson Maturity Model
- Referanseimplementasjoner tilgjengeliggjøres for hovedplatformer (.NET/JAVA)

Eksempel:

GET http://eksamen.udir.no/api/ekstern/definisjoner

200 Ok XML struktur i payload

Versjonering

- Klienten kan velge hvilken versjon av API-et som benyttes ved å sette dette i en «Accept»-header i forespørselen
  - Klienten må ta høyde for at endepunkter betjener flere versjoner av API-et
  - Hvis klienten ikke spesifiserer versjonsnummer, forutsetter tjeneren til en hver tid siste versjon
- Eksempel på verdi for «Accept»-headeren:
  - application/vnd.pas.sas.v2+json (etterspør versjon 2 og json i retur)
  - application/vnd.pas.sas.v2+xml (etterspør versjon 2 og xml i retur)

Skjemavalidering av innkommende data

- XML Well-formedness
- XML Schema definition (XSD)
- Resurser vil returnere status kode 400 ved valideringsfeil og sende tilbake en JSON/XML med detaljer rundt hva som gjorde at valideringen feilet

Asynkron prosessering

Større oppgaver, eksempelvis kandidatpåmeldinslister, prosseseres asynkront hvor klient kan etterspørre status ved hjelp av oppgavereferanse (task reference).

POST http://eksamen.udir.no/api/ekstern/påmelding (XML påmelding payload)

202 Accepted TaskRef: xyzabc

GET http://eksamen.udir.no/api/ekstern/påmelding/status/xyzabc

200 Ok Status: InProgress/Done/Error

Sikkerhet

Autentisering

- All kommunikasjon skjer over TLS.
  - (SSL 3.0 og eldre støttes ikke)
- Autentisering av server (PAS) ved hjelp av TLS
  - Klienten anbefales å bruke «certificate pinning», p.t. benyttes sertifikater fra «COMODO High-assurance Secure Server CA»
- Klienten autentiserer seg ved et X509-sertifikat
  - Virksomhetssertifikat utstedt av én av de godkjente utstederne (p.t. Buypass, BankID, Commfides)
  - Se «sesjonshåndtering» for hvordan klienten autentiserer seg
  - Tjenesten vil validere sertifikatet mot sertifikatkjede og CRL.

Sesjonshåndtering

- For tilgang til API-ene opprettes en sesjon
  - Sesjonen kommuniseres mellom klient og tjener via en informasjonskapsel (cookie)
- Sesjon opprettes ved at klienten sender en POST-forespørsel til http://eksamen.udir.no/api/ekstern/innlogging, som inneholder:
  - En XML-formattert melding bestående av
    - Organisasjonsnummer for klienten
    - Sluttbruker i klientsystemet hvis dette er relevant for logging / sporbarhet
    - Påloggingstidspunkt (format som definert i kapittel 5.6 i RFC3339)
    - Tilfeldig tall (32-bit nonce)
  - XML-signatur av meldingen signert med klientens virksomhetssertifikat
- Hvis sesjonen er utløpt vil server sende
  - Status: 419 Authentication Timeout
  - Location: /api/ekstern/innlogging

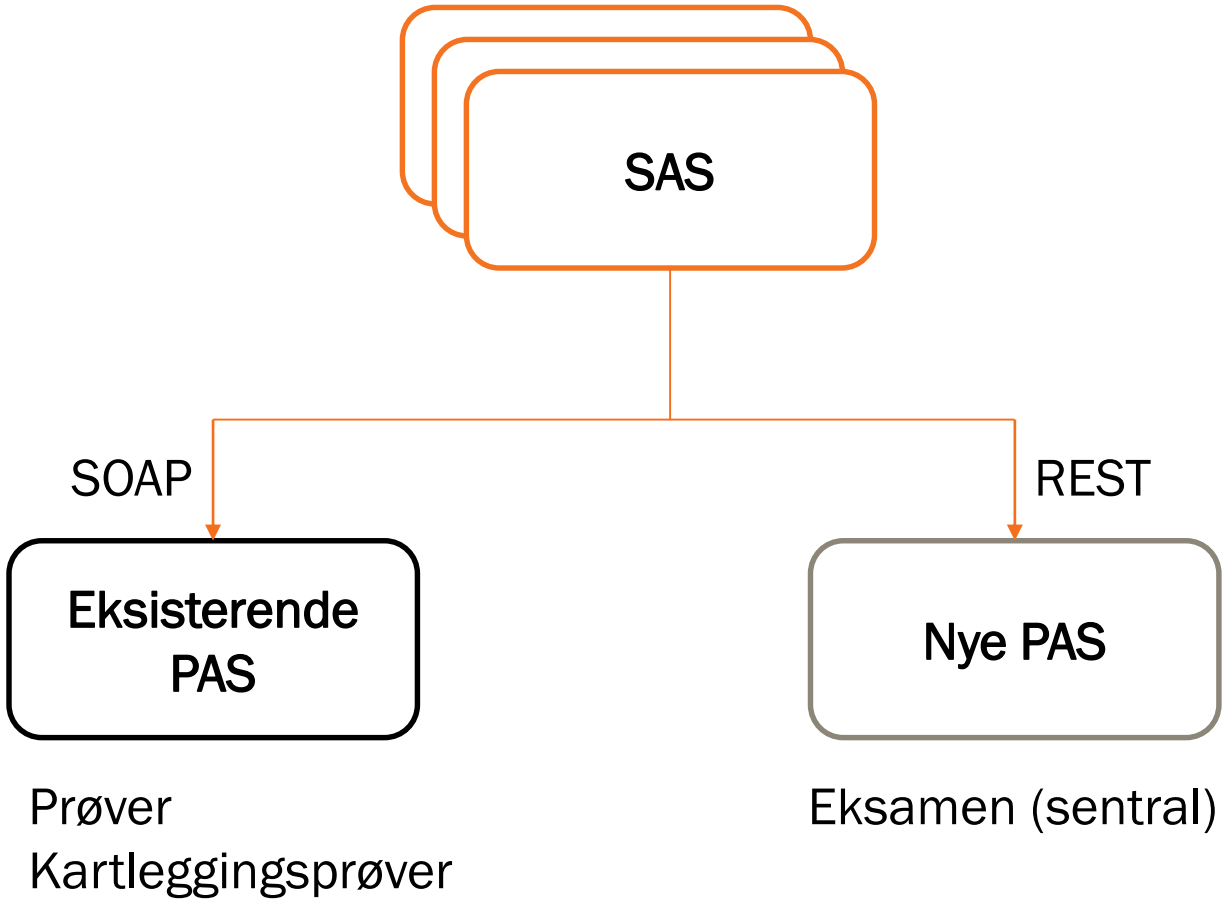
Krav til organisasjonsnummer

- Klientens organisasjonsnummer (og tilhørende virksomhetssertifikat) må tilhøre en enhet som er ett av følgende:
  1. En enhet som fins i Nasjonalt skoleregister (typisk for skoler, kommuner og fylkeskommuner)
  2. En enhet som er meldt inn på forhånd til Utdanningsdirektoratet (typisk SAS-leverandører)

http://musicianguide.cn/wp-content/uploads/2012/01/cooperate.jpg

Nye og eksisterende PAS

Nye og eksisterende PAS ved lansering av nye PAS høsten 2015



Veien videre

Oppstart

- Velge ut pilotleverandør(er)
- Definere grensesnittet
- Implementasjon
- Testing
- Resterende leverandører inkluderes
- Implementasjon
- Testing

Hva er klart nå?

Hvor finner jeg mer informasjon?

http://tiny.cc/integreremedpas