Bankenes utfordringer og tilpasninger knyttet til 3. parters tilgang til konto (XS2A) som følge av PSD 2

Brynjel Johnsen, Bits

Generelle utfordringer

En stor endring

På mange områder der bankene tidligere har hatt ansvaret selv – og har hatt full kontroll, må de overlate mye av ansvar og kontroll til tredjepartsaktører. Dette er vanskelig.

Tidslinjen

PSD2 direktiv – RTS - EU-lovgivning - Norsk lovgivning

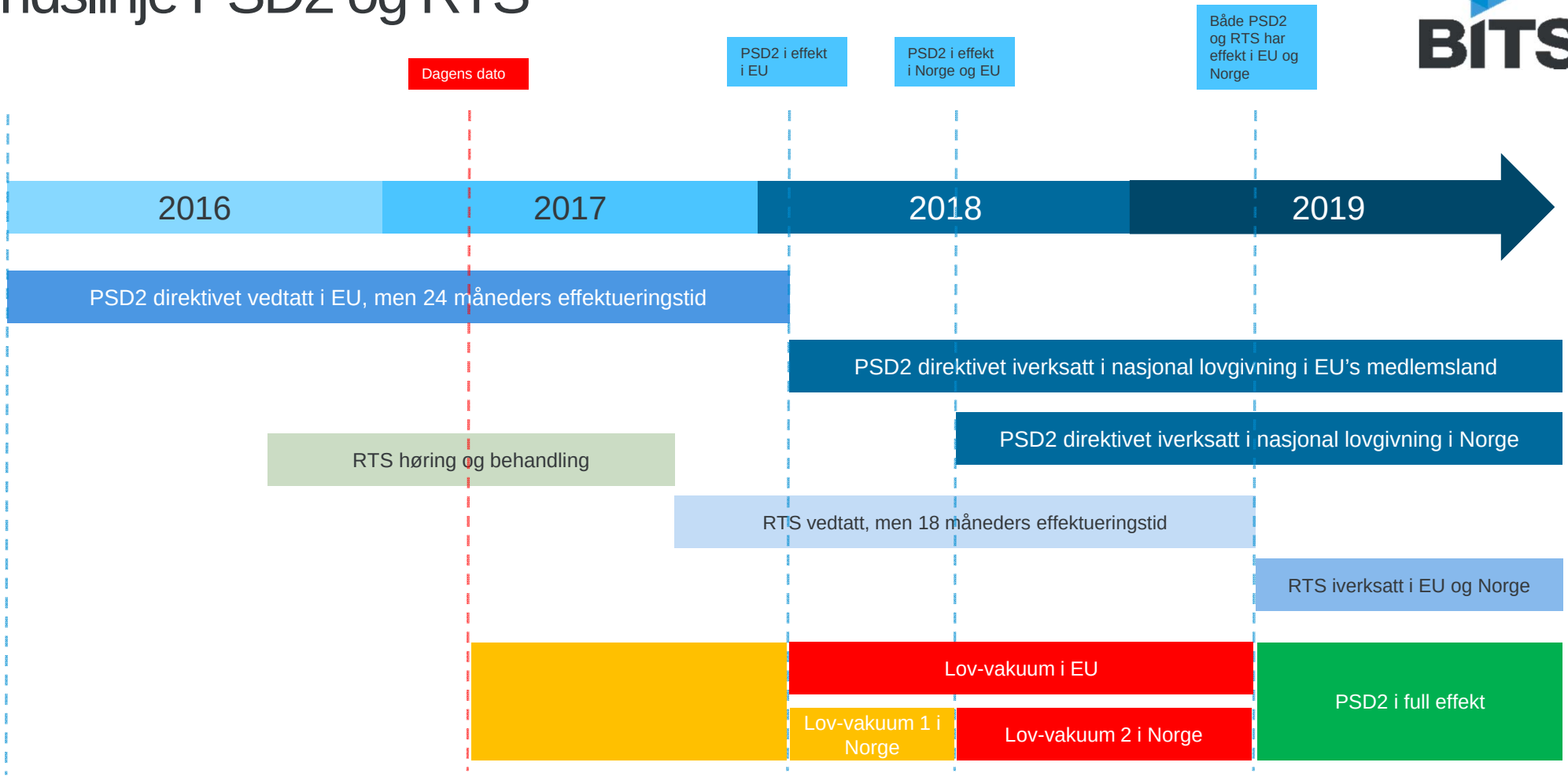
Teknisk implementering

Teknisk implementering – bevegelig mål – omkamper - Er screen scraping tillatt eller ikke?

Uavklarte forhold

Hva er tillatt? Hvor går grensene for bankenes ansvar, og hvordan skal de håndtere samtykke?

Tidslinje PSD2 og RTS



Hvilke nye aktører reguleres av PSD2?

Third Party Providers (TPP)

- *Payment Initiation Service Providers (PISP),*
  … kan levere betalingstjenester basert på bankkundenes konti og bankenes betalingsinfrastruktur, ref artikkel 66 i PSD2
  … eksempler er kontobasert nettbetaling

- *Account Information Service Providers (AISP),*
  … kan levere kontoinformasjonstjenester basert på bankkundenes konti, ref artikkel 67 i PSD2
  … eksempler er tjenester som viser «min økonomi» med aggregering av kontoinformasjon på tvers av ulike banker

- *Payment Instrument Issuing Service Provider (PIISP)*
  … kan utføre dekningskontroll mot en bankkundes konto for et kjøp som skal gjennomføres med et avtalt betalingskort (antatt utstedt av PIISP)
  … her finnes det ikke så mange eksempler, men det har vært nevnt ulike typer lojalitetskort som kan knyttes mot en betalingskonto

Bankene må forholde seg til andre aktører så raskt som mulig!

- **Tredjepartsaktørene er i markedet i dag**
  - Flere aktører er allerede i det norske og europeiske markedet og tilbyr PISP og AISP tjenester.
  - Tilgangen til konto for disse aktørene er imidlertid ikke fullt ut regulert før RTS er på plass i 2019.
- **De norske bankene må etter alt å dømme forholde seg til internasjonale aktører allerede 13. januar 2018 når PSD2 gjelder i EU**
  - Norge er et attraktivt marked, og vi må regne med at europeiske aktører fremover retter sin oppmerksomhet mot Norge.
  - På et tidspunkt i 2018 vil også det norske lovverket være tilpasset PSD2.
- Siste frist for tilpasning for de norske bankene er ved effektuering av RTS en gang våren 2019.

Gitt den uavklarte rettslige situasjonen, og at innholdet i RTS er kjent så er det i alles interesse at løsninger som dekker kravene i PSD2 og RTS kommer på plass så raskt som mulig.

RTS - Regulatory Technical Standards on Strong Customer Authentication and common and secure communication

Bankene må tilby minst ett grensesnitt som tredjepartsaktører kan benytte for tilgang til betalingstjenestene som er omfattet av PSD2

…enten samme grensesnitt som banken tilbyr kunden(!), eller et dedikert grensesnitt for tredjepartstilbydere

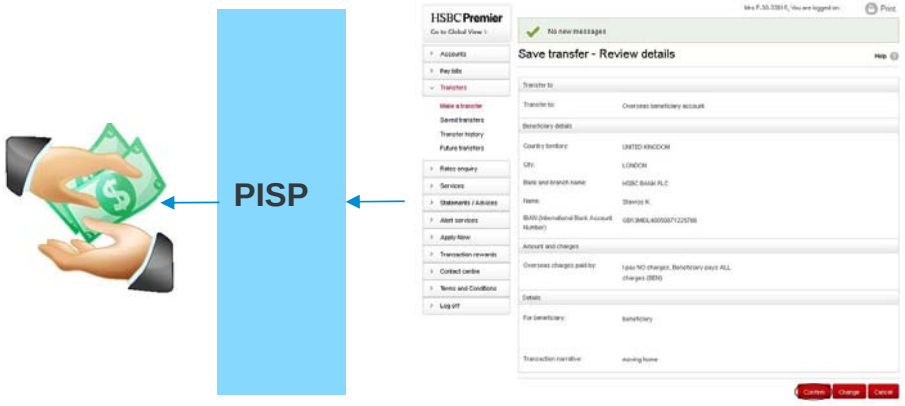
Uavhengig av dette er såkalt «screen scraping», som noen aktører benytter i dag ikke tillatt etter effektueringen av RTS, forventet i april 2019. Men her pågår det en dragkamp…

Byrden er på banken: - hvis en bank ikke tilbyr et dedikert grensesnitt, hva er så alternativet? Kan vi da risikere at en TPP benytter «screen scraping» likevel? Selv om det ikke er tillatt? Og hva kan man gjøre med det?

NB! Kravene i RTS gjelder også bankens egen nettbank. Det er ikke så relevant for grensesnittet, men for innhold og Strong Customer Authentication kan det få betydning.

Hvordan skal banken legge til rette for PISP?

For PISP må banken tilby alle typer betaling som bankene tilbyr sine kunder gjennom det ordinære grensesnittet (nettbank)



En betaling er ikke nødvendigvis bare det man bruker i hverdagen…

- Innenlands betaling
- Innenlands «straksbetalinger»
- Utenlands betalinger av ulike typer
- SEPA betalinger (SCT, SCT Inst, Sepa fast)

For bedriftskunder må man på samme måte støtte ulike typer betalinger:

- Lønnsutbetaling
- Samlebetalinger

Viktig: Kunden skal uavhengig av betalingstype få samme informasjon om betalingen via TPP som kunden får i sin nettbank.

- Gebyrer
- Vekslingskurser
- Status for betalingsutførelse
- Valuteringsdato

Hvordan skal banken legge til rette for AISP?

For AISP må banken levere informasjon om alle typer betalingskonti.

AISP

Banken må levere ut samme informasjon som de tilbyr sine kunder i det ordinære grensesnittet – altså nettbank.

Hva er en betalingskonto i denne sammenhengen?

- Hva er en betalingskonto?
- Hva med sparekonto som man kan betale en regning fra?
- Andre typer konti?

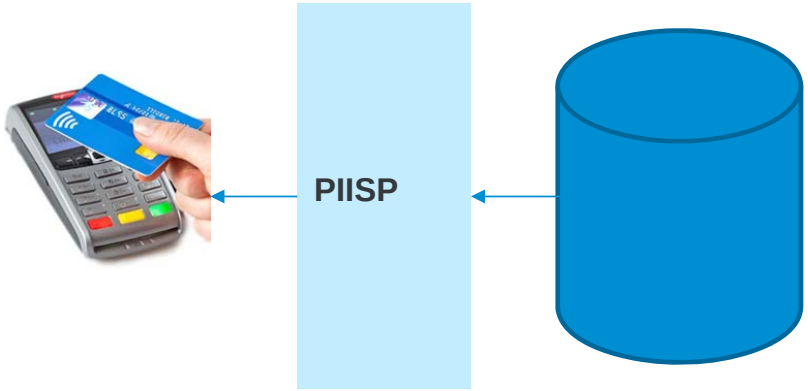
Banken må levere ut samme informasjon om en betalingskonto til en kunde via en AISP som kunde har tilgjengelig i sin nettbank

- Saldo
- Transaksjoner de siste 90 dager

… og all tilhørende informasjon som de ser i nettbanken

Hvordan skal banken legge til rette for PIISP?

For PIISP må banken levere ut et svar «ja» eller «nei» for om det er dekning på konto for et forespurt beløp.



Kunden må tilordne et bestemt kort fra en kortutsteder til en spesifikk, nærmere avtalt betalingskonto før PIISP kan forespørre om saldo.

Hvilke korttyper skal kunne knyttes opp til en konto?

- Kort utstedt av andre enn bank
- Lojalitetskort med betalingsfunksjon
- Andre korttyper?

Hvilke typer konti kan et kort knyttes opp mot?

- Betalingskonti – som må defineres

Sikkerhet og PSD2

- Intensjonen med PSD2 er å legge til rette for mer konkurranse, mer innovasjon, større valgfrihet, men også økt sikkerhet for forbrukerne.
- EBA er gitt fullmakt til å utarbeide *Regulatory Technical Standards* on *Strong Customer Authentication and Common and Secure Communication*.
- Dette dokumentet setter krav til:
  - Sikkerhet for betaler, gjennom innføring av krav til tofaktor Strong Customer Authentication
  - Grensesnittet mellom TPP (PISP/AISP/PIISP) og Account Servicing Payment Service Provider (ASPSP – kontobanken)
  - Sikkerhet i dette grensesnittet

For bankene betyr dette at…

Banken må…	I praksis betyr dette…
… tilby (minst) ett grensesnitt som TPP kan bruke til å koble seg til bankens betalingstjenester	At banken bør tilby et dedikert grensesnitt (API), eventuelt samme grensesnitt som kunden benytter for tilgang til konto (ingen vet helt hva dette er så lenge screen-scraping er forbudt)…
… verifisere identiteten og autorisasjonen til en TPP	At banken skal verifisere identiteten til en TPP ved å validere dennes sikkerhetssertifikat. De enkelte nasjonale myndigheter vil vedlikeholde en liste over TPP'er autorisert i det norske markedet, men bankene skulle gjerne hatt en online spørretjeneste for dette.
… tilby kunden å autentisere seg og autorisere betalinger med samme tofaktor sikkerhetsmekanismer som kunden kan bruke i egen nettbank.	At banken ikke kan tilby andre autentiseringsmekanismer i nettbanken enn de som er godkjent for bruk til PSD2-tjenester til TPP'er. Kun løsninger som kan benyttes med tredjeparter kan benyttes i egen nettbank.

Spesifikt om Strong Customer Authentication (SCA)

Det er i RTS stilt spesifikke krav til mekanismer til Strong Customer Authentication…

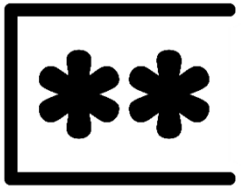
- Kontobanken skal legge til rette for at betaler skal kunne benytte bankens autentiseringsmekanismer til SCA

- Kravet er at kunden skal autentisere seg med <u>minst to</u> av følgende faktorer:

Noe man er

Noe man har

Noe man vet



På bakgrunn av minst to av disse elementene skal det genereres en autentiseringskode som banken kan bruke til å autentisere personen og autorisere betaling….

For betalinger gjelder i tillegg følgende krav

For å autorisere en betaling skal den autentiseringskoden som genereres være 'dynamisk linket' til beløp og betalingsmottaker.

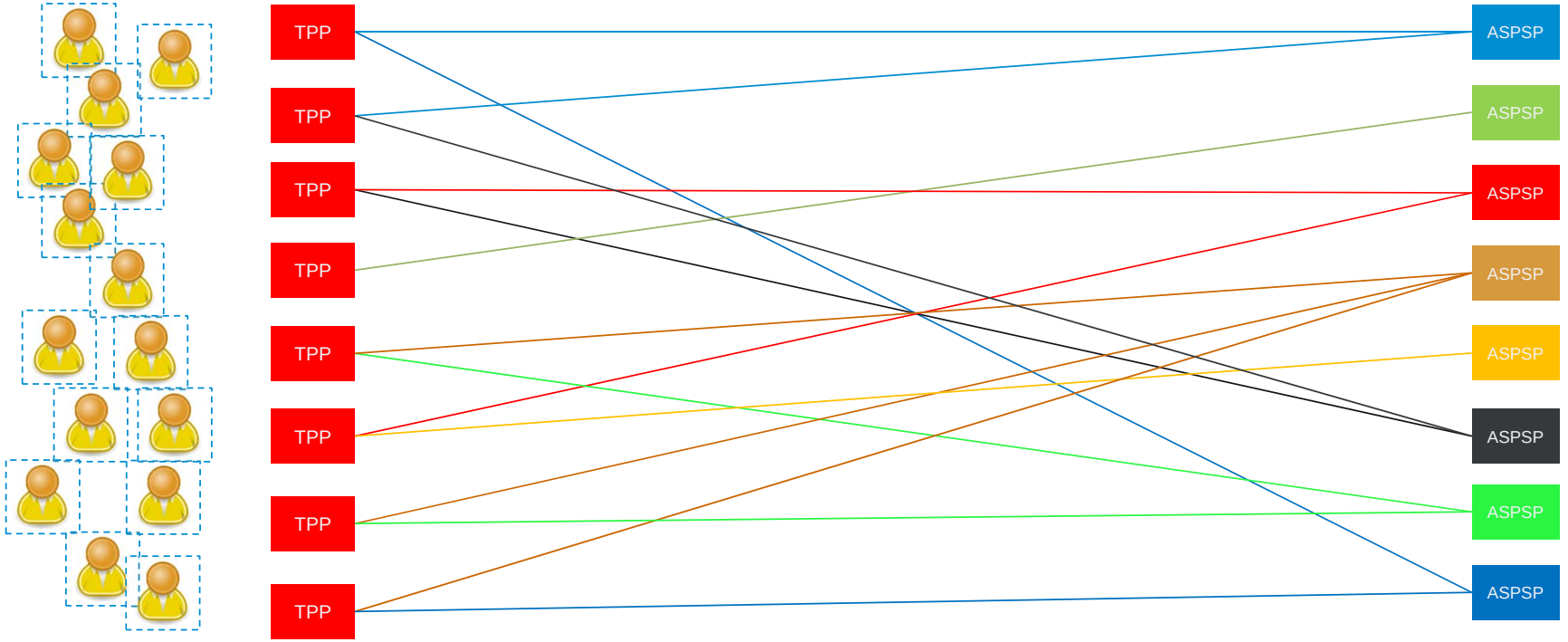
Intensjonsverifikasjon: endring av beløp eller betalingsmottaker skal bli oppdaget av banken før gjennomføring av betaling…

Utover dette er det foreslått en rekke unntak fra bestemmelsene ved små beløp, basert på sanntids risikoanalyse mv.

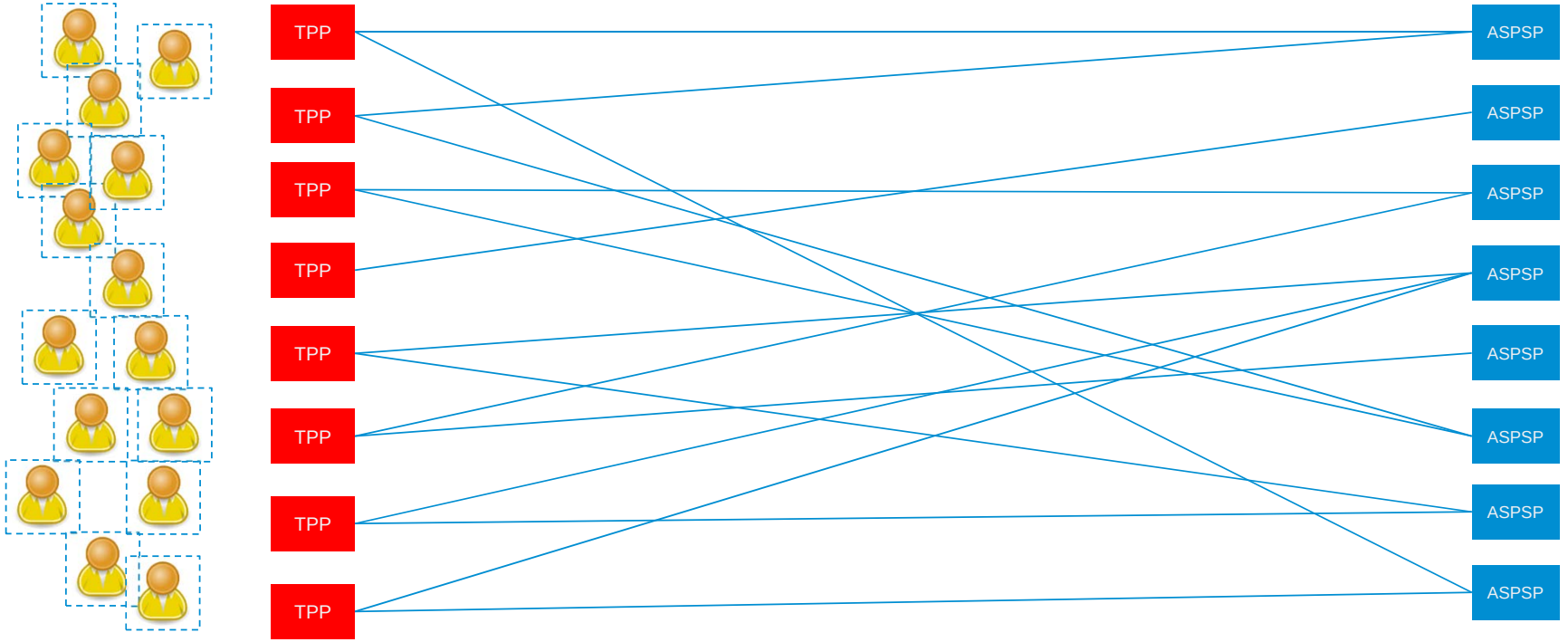
Oppsummering

- Bankene må gjøre sine PSD2-tilpasninger i god tid før direktivet og RTS er i effekt i Norge
- Tilpasning til PSD2 innebærer mer enn bare å åpne opp
  - Bankene må tilgjengeliggjøre alle typer betalinger de tilbyr kundene i dag
  - Bankene må tilgjengeliggjøre alle betalingskonti – med all informasjon som de viser kundene i dag
  - Bankene må tilgjengeliggjøre sine autentiseringsmekanismer og legge til rette for at kunden kan bruke disse sammen med tredjeparts applikasjoner
- Nå skal vi se litt mer på hvordan man kan gjøre dette

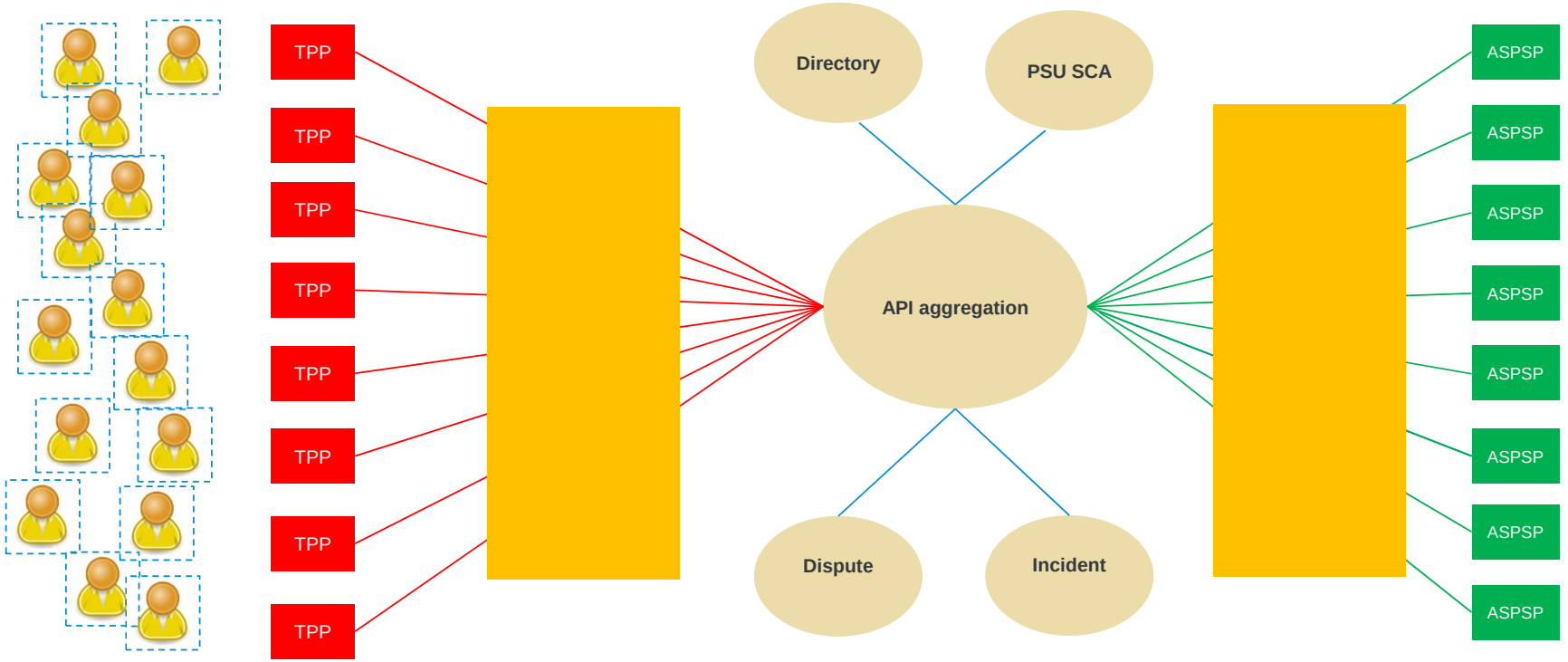
Målet er å unngå en slik situasjon



… og heller oppnå dette

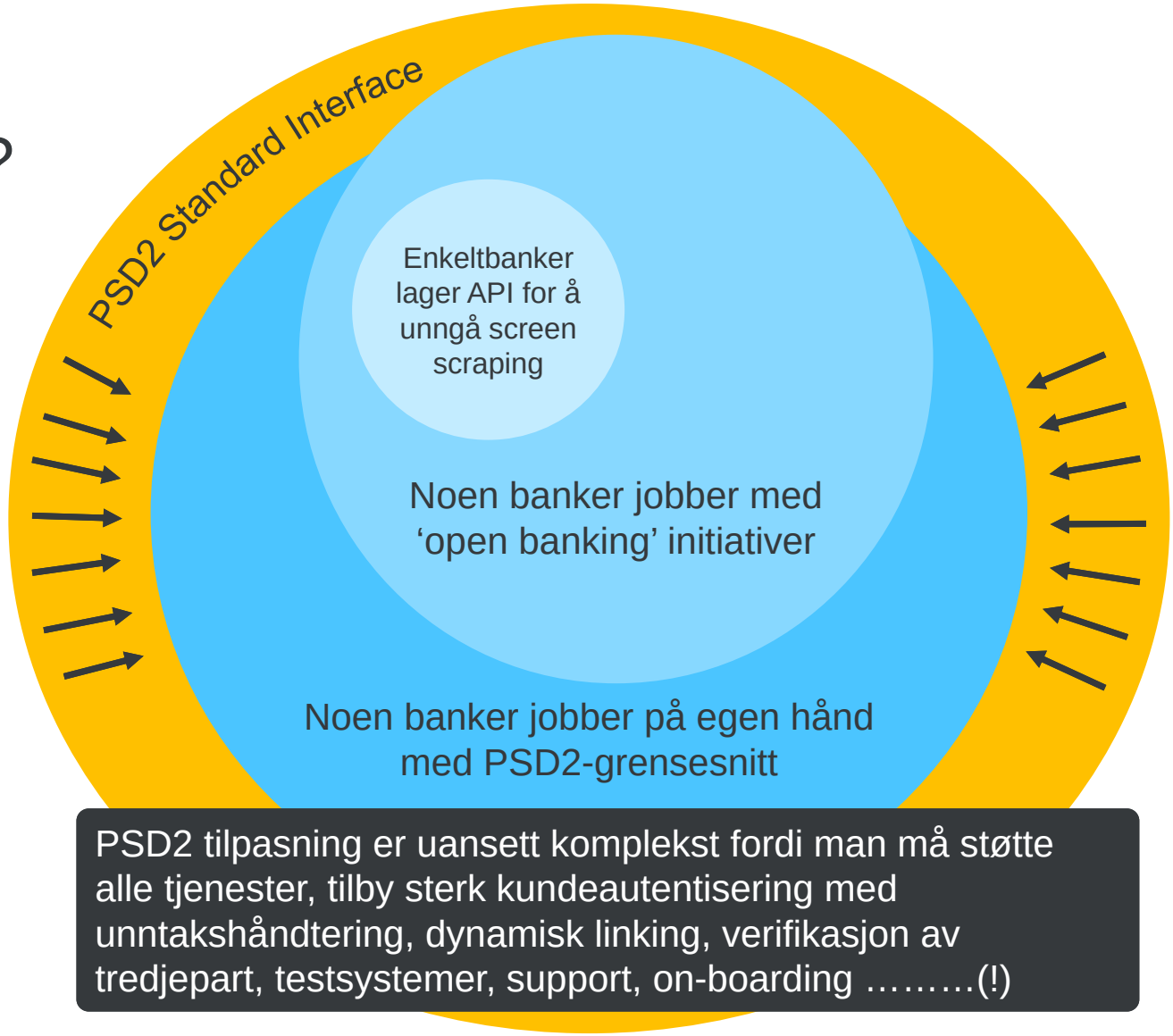


… eller dette


TPP
TPP
TPP
TPP
TPP
TPP
TPP
TPP
Directory
PSU SCA
API aggregation
Dispute
Incident
ASPSP
ASPSP
ASPSP
ASPSP
ASPSP
ASPSP
ASPSP

Hva er status?

EU og norske myndigheter forventer effektive løsninger som dekker compliance og interoperabilitet



Fintech-bransjen flommer over av kreative ideer og nye løsninger

PSD2 tilpasning er uansett komplekst fordi man må støtte alle tjenester, tilby sterk kundeautentisering med unntakshåndtering, dynamisk linking, verifikasjon av tredjepart, testsystemer, support, on-boarding ……(!)

Samarbeid i næringen kan foregå på flere nivåer

Rammeverk

Regelverk
Prosedyrer
Prosesser
Rutiner
Avtaler
Dokumentasjon

Spesifikasjoner

Tjenester
Tjenestenivå
Grensesnitt
Arkitektur
Implementasjon

Tekniske løsninger

Kataloger
Grensesnitt
Felles ‘hub’
SCA
Testmiljøer
Support
Incident
Dispute

Alle banker må etterleve det samme regelverket

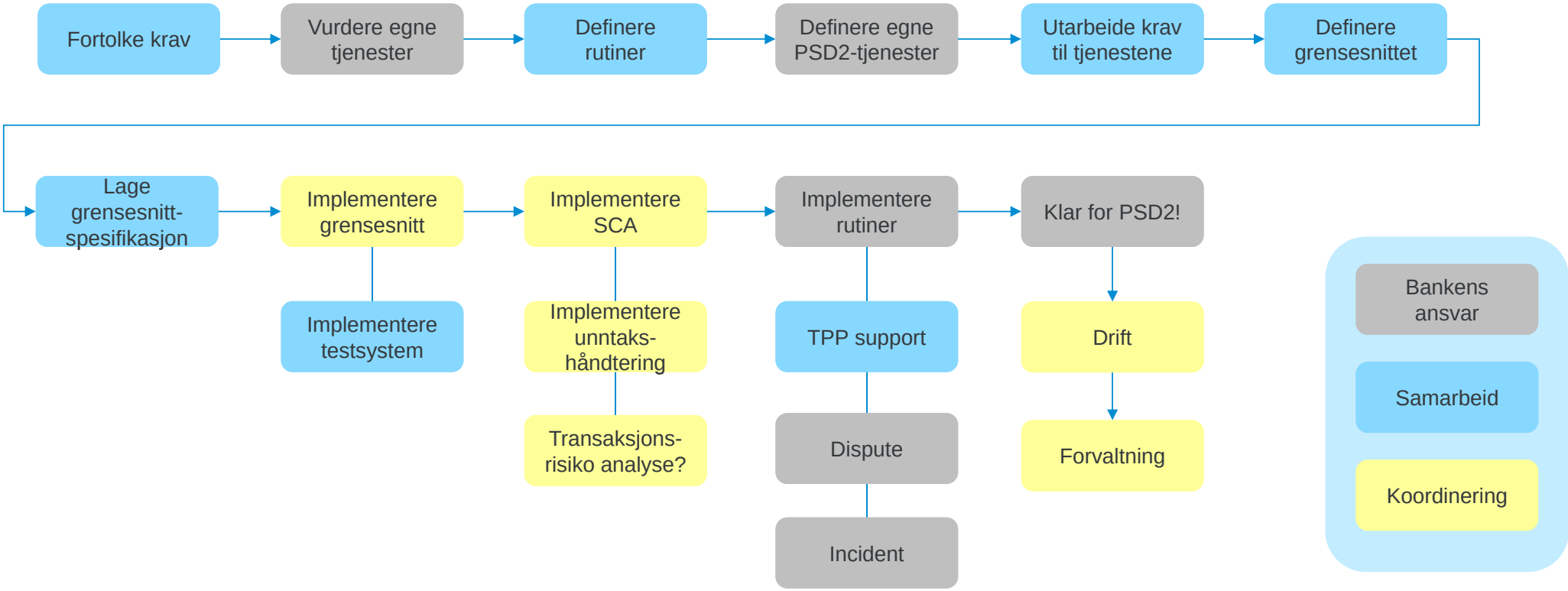
Alle banker må forstå kravene og tilpasse egne systemer og rutiner til PSD2 for sine banktjenester

Alle banker må forholde seg til eksterne rammefaktorer, myndigheter og regler for grensekryssende virkshomhet.

Alle banker må tilpasse seg og levere grensesnitt for ‘compliance’ til PSD2 for sine banktjenester

Banker kan selvfølgelig levere premiumtjenester på toppen av de obligatoriske PSD2-tjenestene

Alle banker må etterleve det samme regelverket



Målsetninger for samarbeid

Tilfredsstille intensjonen med PSD2	• Enhetlig tjenestenivå for forbrukerne og TPPer • Valgfrihet og transparens i markedet • Enhetlig sikkerhetsnivå • Legge til rette for videre innovasjon gjennom fleksible grensesnitt
Interoperabilitet	• Redusert risiko for fragmentering i næringen • TPPer kan nå bankene i næringen gjennom et harmonisert rammeverk • Enhetlig tilgang til markedet • Enkel tilgang til konto for TPP og brukersteder • Reduksjon av PSD2 XS2A kompleksitet
Reduserte kostnader	• Kostnadsreduksjon for utvikling, vedlikehold, forbedringer og test • Bedre, flere, raskere, og billigere tjenester for bankens kunder • Komplett, kostnadseffektiv løsning på ‘compliance’ til PSD2 • Mulighet for felles implementering av grensesnitt • Mulighet for felles implementering av testmiljø og support

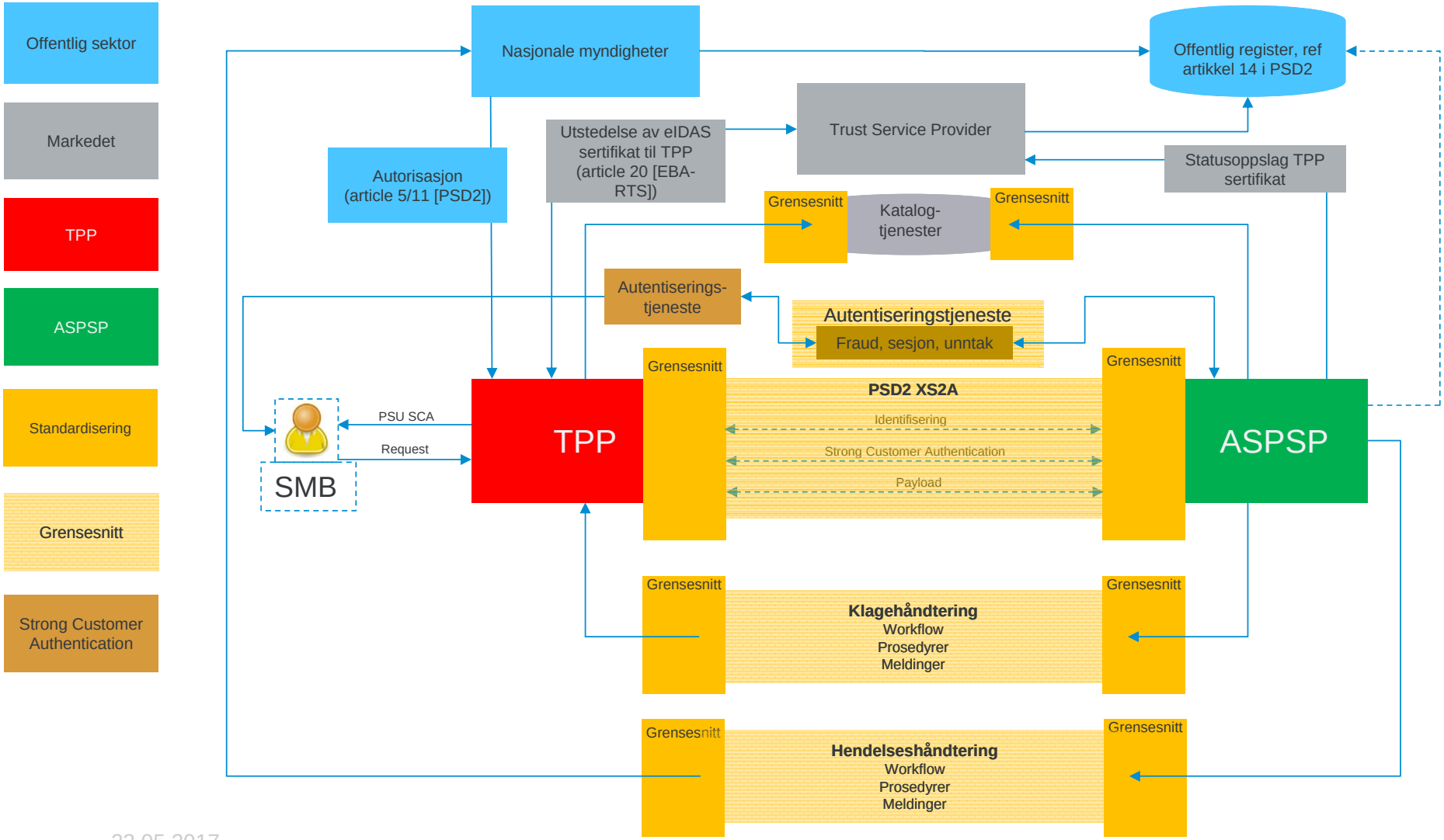
Prosjekt PSD2 XS2A

Bits leder et prosjekt ‘PSD2 XS2A’ med deltagere fra den norske banknæringen.

Målet er å identifisere områder for samarbeid og spesifisere løsninger som kan brukes på tvers i næringen innenfor:

Felles krav	Felles spesifikasjoner	Felles løsninger
• Katalogtjenester • PSD2 grensesnitt • Løsninger for SCA • Hendelseshåndtering • Klagehåndtering	• Katalogtjenester • PSD2 gensesnitt	• Felles implementasjon av katalogtjenester • Felles implementasjon av grensesnitt

Omfattende infrastruktur er nødvendig for effektiv implementering av PSD2



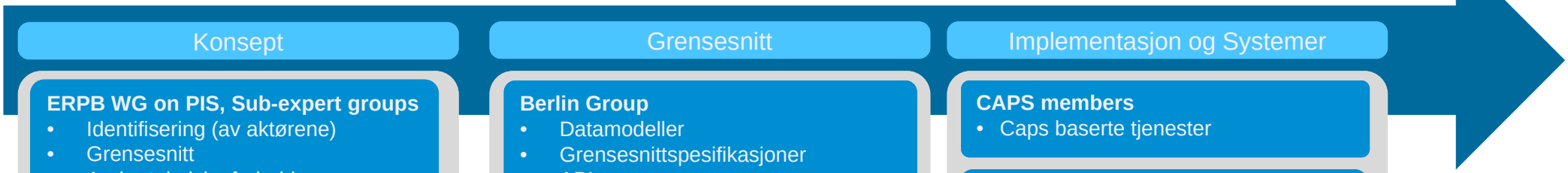
Internasjonalt standardiseringsarbeid

RTS setter krav, men sier ingen ting om hvordan grensesnittet skal se ut

RTS er åpen for fortolkninger

Alle aktører / roller er ikke enige i de prinsippene som er nedfelt i RTS

Ulik fortolkning kan skape ulik praksis og ulike implementasjoner



Konsept	Grensesnitt	Implementasjon og Systemer
ERPB WG on PIS, Sub-expert groups • Identifisering (av aktørene) • Grensesnitt • Andre tekniske forhold	**Berlin Group** • Datamodeller • Grensesnittspesifikasjoner • API	**CAPS members** • Caps baserte tjenester
CAPS • Rulebook	**ERPB WG on PIS, Sub-expert groups** • Identification • Interface	**PRETA** • Katalogtjenester • Testverktøy for onboarding og sertifisering
PRETA • Spesifikasjoner		**Andre aktører**

Takk for meg

Brynjel Johnsen

Bits AS

brynjel.johnsen@bits.no