Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Innovasjoner innen trygge og personvernsøkende elektroniske identiteter fra forskning

Research innovations in information security and privacy in electronic identity management

Dr. Lothar Fritsch, Senior Research Scientist
Information Security, Privacy and Identity Management

FRISC

FRISC Frokostmøte, Oslo, 3. Desember 2014

Agenda

- Kort om e-ID
- Dagens e-ID-økosystemer
- Personvernsutfordringer med e-ID
- Løsninger for e-ID med innebygget personvern
- Utfordringer med bruk av e-ID

Hva er en e-ID?

- …en liten bit digital data basert på algoritmer i programvare eller i hardware som skal overbevise en datamaskin at en visst person sitter foran maskinen
- e-IDer kan være tilknyttet til en ”offisiell” identitet, for eksempel en pass eller en personnummer
- Mange e-IDer er tilknyttet til ”myke” identiteter: e-post-adresser, brukerpseudonymer, …
- E-IDer brukes til mange ulike formål
- E-IDer er tilknyttet til en kommunikasjonskanal, eller ikke
- E-IDer og tilknytning til identitet kan være styrt av brukeren selv (valg av pseudonym eller ID i OpenID), eller påtvunget (pass fra staten, MinID). Det kan i tillegg aggregeres ID-profiler av sosiale medier eller andre tjenester.

Hvorfor brukes e-ID’er?

- Identifisering
  Hvem er brukeren – ved innlogging eller forvalting av personopplysninger i databaser
- Autentisering
  Er det virkelig brukeren? Bevis det!
- Autorisering eller ikke-benektelse
  Legitimering av transaksjoner basert på en e-ID. Betyr ofte at man kan ikke nekter transaksjon.

Oppsummering e-ID

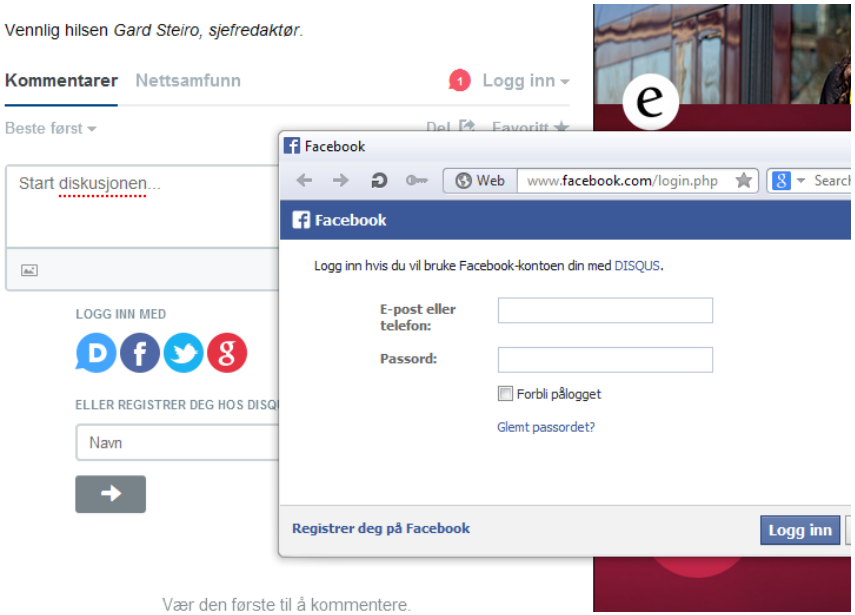
- e-ID brukes til forskjellige formål i applikasjoner og tjenester på nett
- Hvilke opplysninger må tilknyttes til en e-ID for å lage en trygg transaksjon er helt avhengig av applikasjoner som tar i bruk e-IDer
- En e-ID system som utvider bruksområdet til nye applikasjoner kan skape trusler både for den opprinelige applikasjon, den nye område, eller for brukerens personvern
- Løsninger på marked tilbyr varierende sikkerhets- og personvernsegenskaper

Agenda

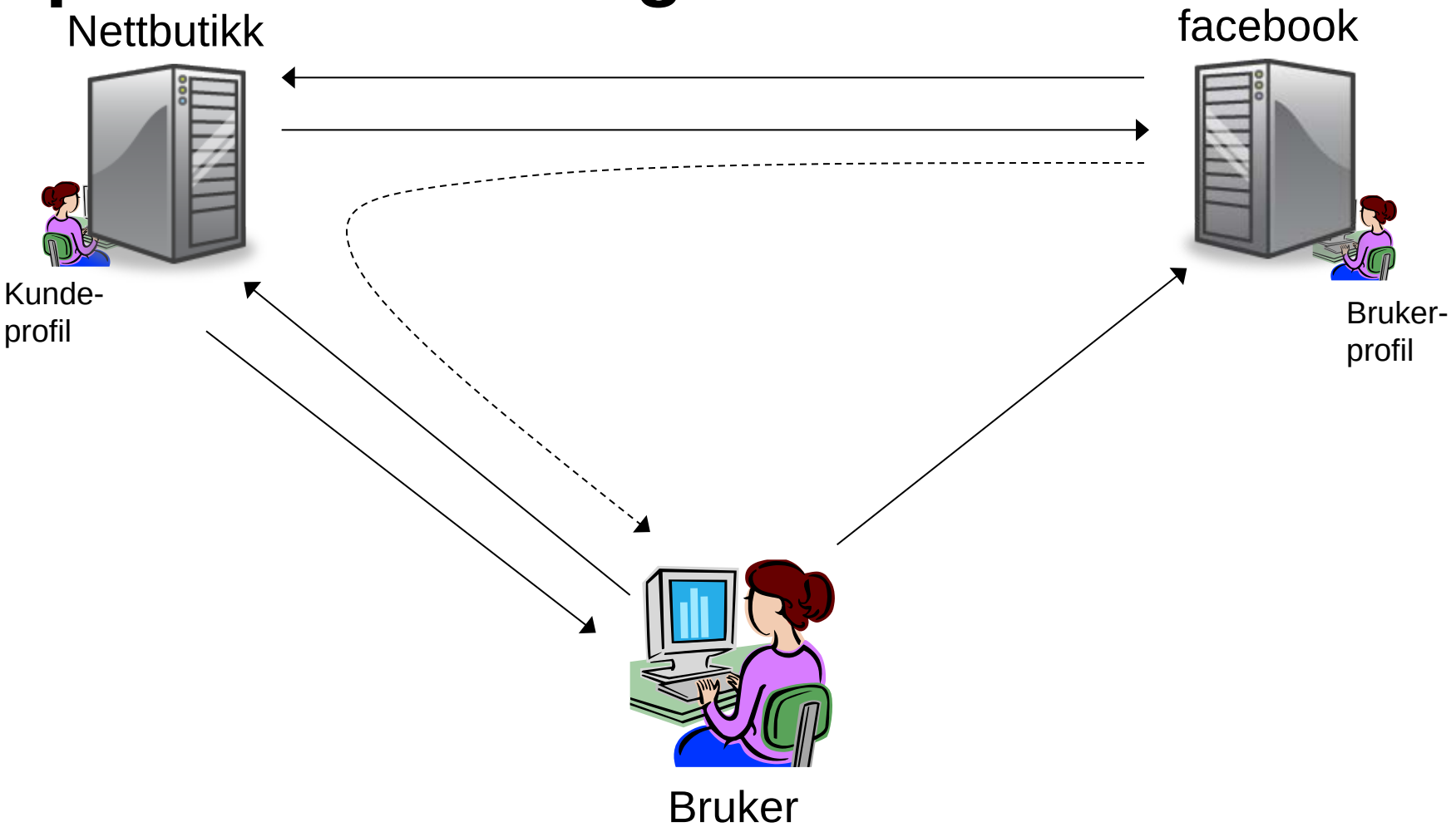
- Kort om e-ID
- Dagens e-ID-økosystemer
- Personvernsutfordringer med e-ID
- Løsninger for e-ID med innebygget personvern
- Utfordringer med bruk av e-ID

facebook, Google, OpenID

- OpenID-protokoll brukes for identifisering på kryss av sosiale medier.
- Konsept: Brukerprofil registrert på ett nettsted, nettsted tilbyr identifikasjon via OpenID til flere tjenester



OpenID – slik fungerer det



Andre e-ID-protokoller

- SAML / OASIS er dagens ledende protokoll for utveksling/deling av ID-attributer, f.eks i ID-porten
- Stor aktivitet hos leverandører for å skape «mobilt e-ID» (f.eks. FIDO alliance)
- Europeisk felles e-ID-infrastruktur basert på e-ID etter EU-direktivet utprøves i EU-finansierte forsøksprosjekter

Implikasjoner med deling av e-ID

- Registrering overlates til OpenID-tilbyder (f.eks. facebook)
- ID provider får med hvilke nettbutikker brukeren pleier å bruke – og hvor ofte. Betalingen for tjenesten er at brukerne utsettes for mer målrettet reklame
- Brukerne kan bruke samme OpenID i flere bruksområder (jobb, privat) – noe som fører til blanding av roller og økt informasjonslekkasje
- OpenID-leverandør er ikke underlagt norsk rett
- Integrasjon av hardware-token er mulig, men knapt i bruk med de store OpenID-økosystemer

Agenda

- Kort om e-ID
- Dagens e-ID-økosystemer
- Personvernsutfordringer med e-ID
- Løsninger for e-ID med innebygget personvern
- Utfordringer med bruk av e-ID

e-ID og Personvern

- e-IDer kan på forskjellige måter skape personvernsrisiko:
  - e-IDer kan inneholder navn, fødselsdato eller andre opplysninger som ikke er nødvendig for alle transaksjoner
  - Bruk av samme e-ID kan sammenknytte forskjellige databaser, applikasjoner og organisasjoner slik at personopplysninger kombineres veldig lett
  - Data som IP-adresser forvandles til en e-ID med stor sporingspotensial hvis tjenesteleverandører og applikasjonseiere tar de i bruk som ID
  - Tilknytting av ny informasjon eller nye tjenester til en e-ID kan skape store personvernsutfordringer (for eksempel name-tagging i digital fotoalbum, bruk av Google-konto gjennom Facebook)

e-ID og Datasikkerhet

- ID-tyveri og andre trusler for e-IDer er avhengig av:
  - Kan e-ID kopieres?
  - Kan e-ID brukes fra en annet sted?
  - Kan e-ID brukes uten videre, hemmelige utlysninger (for eksempel PIN-koder)?
  - Flyttes det avgjørende informasjon sikker over åpne nettverk (for eksempel SMS-meldinger med PIN-koder)?
  - Kan e-ID verifiseres mot brukeren slik at det oppdages bruk av stjalet e-ID?
  - Ligger token, nøkler, registreringsdata og dataspor i land og rettssystemer hvor de er tilgjengelig når det trengs?

Agenda

- Kort om e-ID
- Dagens e-ID-økosystemer
- Personvernsutfordringer med e-ID
- Løsninger for e-ID med innebygget personvern
- Utfordringer med bruk av e-ID

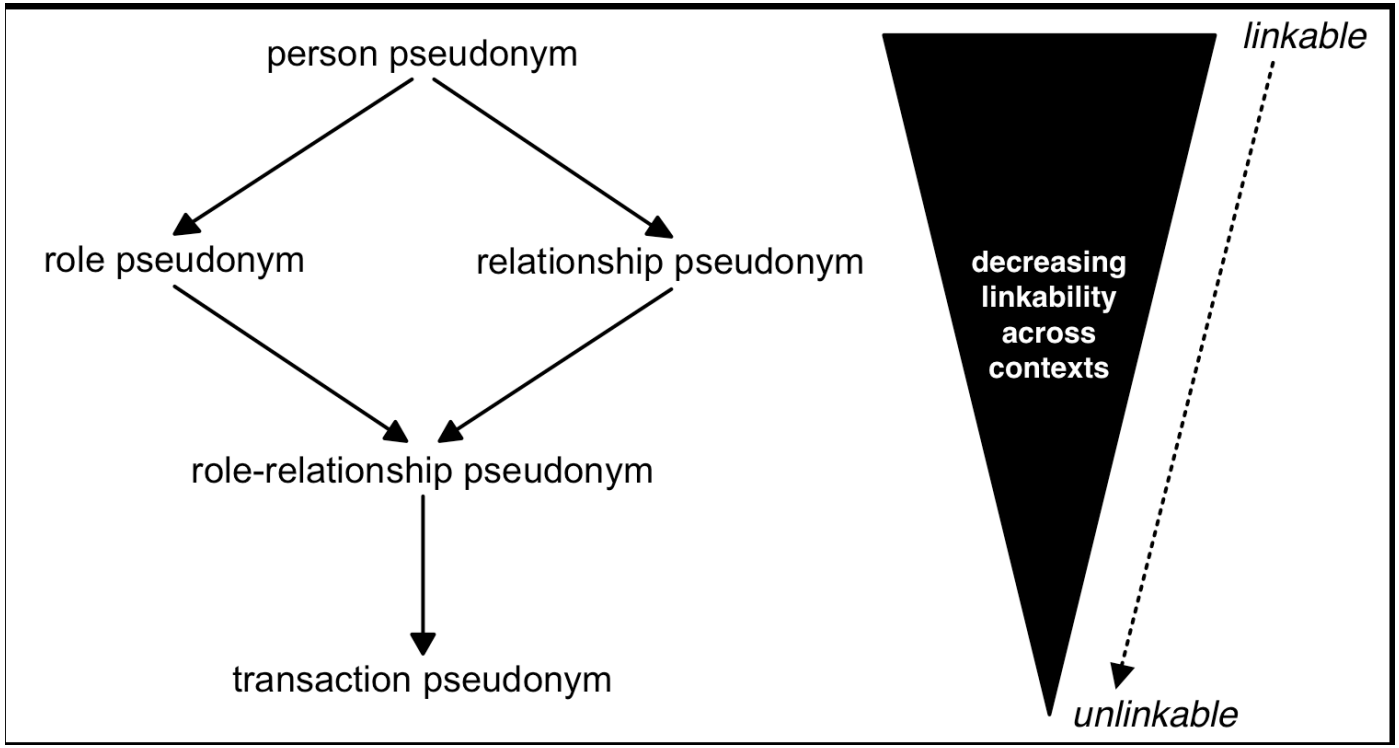
‘Token’ med begrenset rekkevide

- E-ID kan bare brukes til en definert applikasjonsområde
- E-ID har begrenset bruksperiode og løper ut med tid
- E-ID kan bare brukes av autoriserte partnere

- Teknologieksempler:
  - Privacy-Attribute-based credentials (Privacy-ABCs) (www.abc4trust.eu)
  - Autentisering av mottakere for autentisering med tysk digital ID-kort

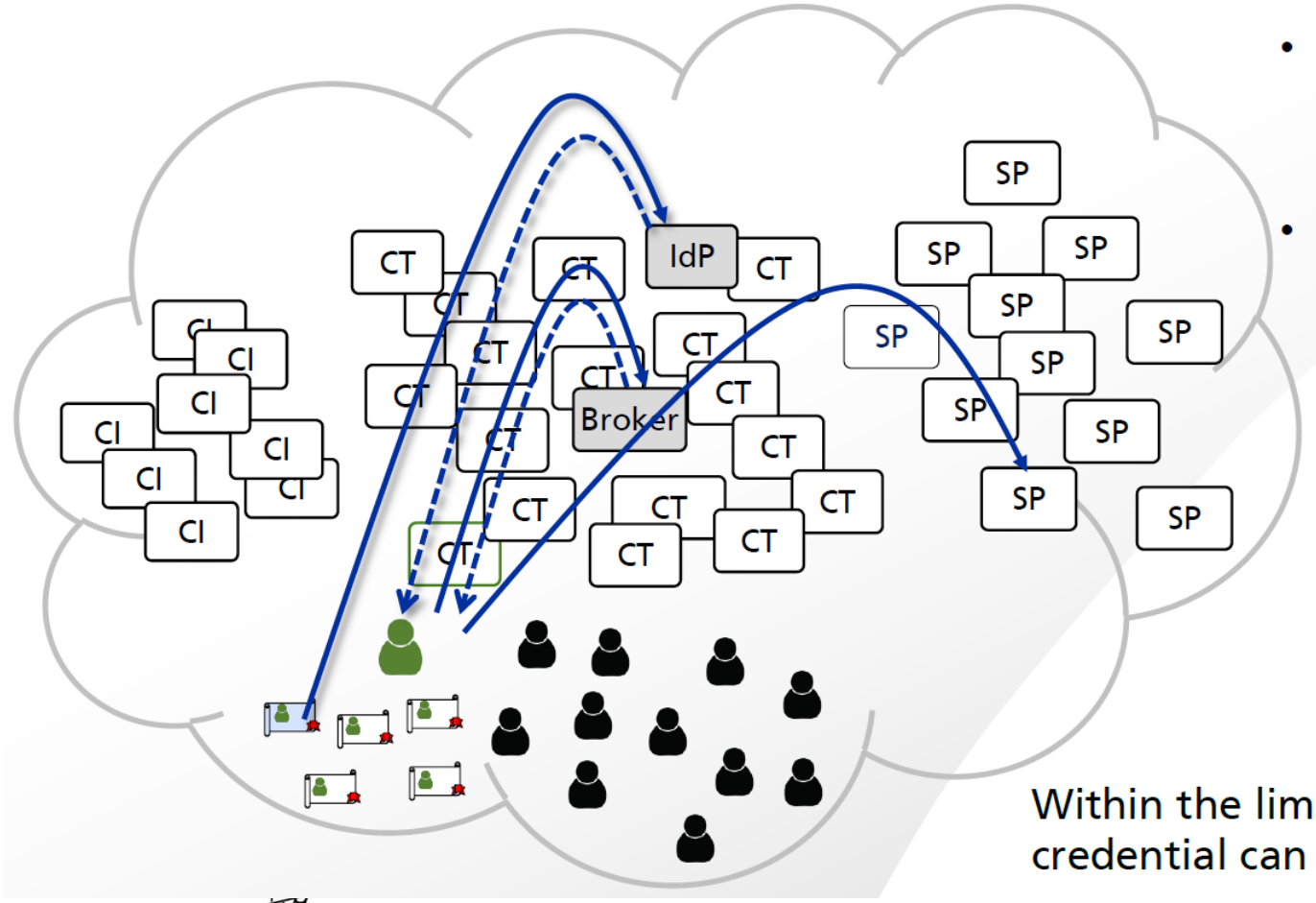
E-ID med variabel identifiserbarhet

- E-ID må ikke alltid inneholde full identifikasjon
- Pfitzmann/Hansen definerer nivåer i pseudonymitet:



A. Pfitzmann, and M. Hansen, *Anonymity, unlinkability, unobservability, pseudonymity, and identity management-a consolidated proposal for terminology, Technische Universität Dresden, Dresden, 2010.*

«Do-not-track»: Identity brokerage i FutureID



- IdP transforms:
  user credential
  to session credential
- Broker transforms:
  - format that SP can consume
  - less privacy exposure
  - etc.

SP and IdP need **not** support the same federation dialect

Within the limits of trust, any credential can be presented to any SP.

FutureID is partly funded by EU FP7 under GA n°318424

Personvern = privathet + transparens

- Beskyttelse av privathet er bare en aspekt i personvern. EU-direktivet setter også fokus på transparens og brukerinvolvering
  - Krav om dokumentert, informert samtykke
  - Innsynsrettigheter
  - Rett å trekke samtykken
  - Rett om å få rettet feil
  - Kommende EU-rett til å bli slettet fra databaser
- Derfor deler forskere personverns-verktøy inn i transparens-verktøy og «opacity»-verktøy.

L. Fritsch, *State of the Art of Privacy-enhancing Technology (PET) - Deliverable D.2.1 of the PET Web project, 1013, Norsk Regnesentral Oslo, Norway, 2007.*

Verktøy for transparens

- Tjenestepolicy med sikkerhets- og personvernspolicy skal tilbys som basis for informert samtykke
  - Samtykke gis til et definert formål -> dokumentasjon
  - Dette stiller krav til databehandler («obligation»): «Obligations management» følger med personopplysninger som regulerer bruksmuligheter
- Sporbarhet: tilrettelegger for innsynsrettigheter
- «Audit trail»: kryptert logging av hva data har blitt brukt til, og av hvem, og hvor.

Agenda

- Kort om e-ID
- Dagens e-ID-økosystemer
- Personvernsutfordringer med e-ID
- Løsninger for e-ID med innebygget personvern
- Utfordringer med bruk av e-ID

Utfordringer med e-ID

- Hvem eier “sikker element”?
- Hvem bestemmer over nøkler og attributer?
- Hvem bestemmer over tilknytning til nye e-ID økosystemer?

Utfordringer med forretningsmodell

- Kan vi akseptere ‘lock-in’ i et lukket økosystem?
- Hvor lenge skal relasjon til kunder/personer være?
  - Engangstransaksjon
  - Kunde som returnerer flere ganger
  - Livslang, f.eks. i forsikringsbransjen (flere bytte over til ny e-ID teknologi, endring i personlige ferdigheter, digitale hjelpemidler, e-inkludering)
- Hvor kritisk er data og kunderelasjon sett mot andre aktører? Er det hemmelig informasjon, kritisk informasjon, eller skadelig informasjon involvert?

Walled gardens – åpne e-ID økosystemer vs. Innstengelse (lock-in)

Dette loves.

Dette leveres.

Og hvem er grisen her?

Akkumulasjon av «datasøppel»

- «Big Data» eller «Big Søppelfylling» med utdatert og dårlig kvalitetssikret data?
- Ukjent datakvalitet, økte søkekostnader
- Økte kostnader til databasedrift med hensikt til regulering, ansvar og personvernsobligasjoner
- Økt risiko for feilhåndtering av data hos databehandleren og behandlingsansvarlig

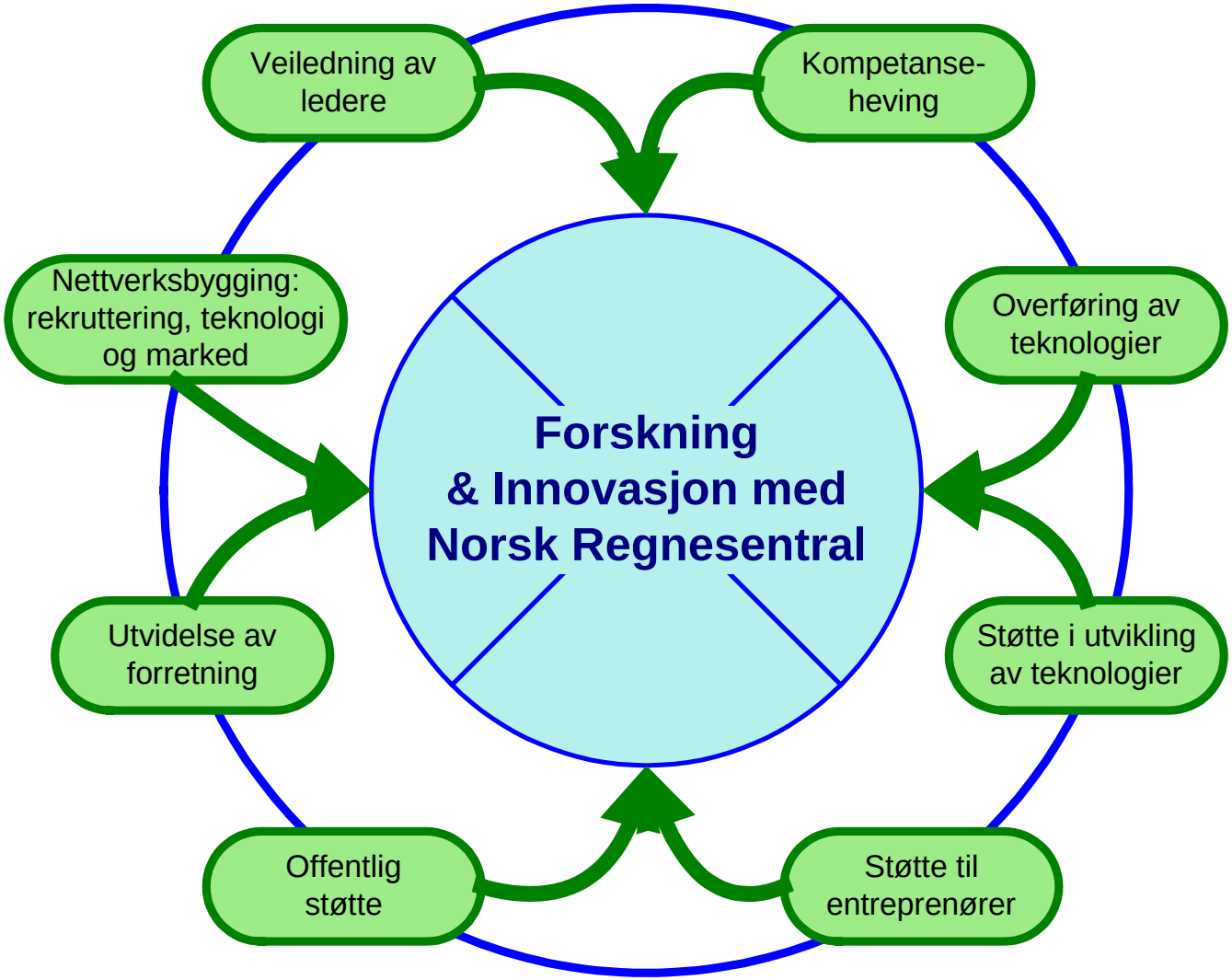
Stor behov for tillitsinfrastruktur

- Transparens med sertifiseringer, juridiske rammer
- Informasjonsinfrastruktur for vurdering av akkrediteringer
- Forretingsinformasjon om sentrale aktører
- Informasjonsutveksling om tillitsnivå til teknisk infrastuktur som brukes av ID-utstedere og andre leverandører
- Risikovurdering med hensikt til langtids-akkumulasjon av personvernsrisiko og med fokus på «systemkritisk størrelse» av e-ID-økosystemer

Oppsummering: e-ID og Personvern

- En e-ID-økosystem kan dø av for mye forurensing med dubletter, falske identiteter, forfalskete eller utløpte attributer osv.
- Livstid og formålsdefinisjon av e-ID er viktig!
- Det er bedre å tilby fairness i behandling av identiteter, profiler og personopplysninger enn å håndtere kunder som med intensjon forfalsker data og bruker engangs e-post-adresser.
- Det lønner seg ikke i alle forretningsmodeller å «invitere hjem» de store sosiale medier med sine reklameorienterte overvåkningsmekanismer, eller dele e-IDer til egne kunder med resten av marked.
- Det fins mange komponenter fra nyere forskning som helper med å skape e-ID-økosystemer med «innbygget personvern».

Spørsmål?


Veiledning av ledere
Kompetanse-heving
Nettverksbygging: rekruttering, teknologi og marked
Overføring av teknologier
Forskning & Innovasjon med Norsk Regnesentral
Utvidelse av forretning
Støtte i utvikling av teknologier
Offentlig støtte
Støtte til entreprenører

Mulige samarbeidsformer med Norsk Regnesentral

- Teknisk workshop (1 dagsverk)
  - Problemanalyse, løsningsskisse
  - Spesifikasjon med kundenes fagavdeling
- Prosjektarbeid etter behov
  - Sammenarbeid med kundenes fagavdeling
- Leveranse med fast pris
  - Oppdrag for konkret leveranse
- Faglig opplæring
  - Seminar eller workshop