Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

E-ID, Sosiale Medier, industristandarder - nytteverdi og risiko

Innføring I populære e-ID-systemer

Dr. Lothar Fritsch
Norsk Regnesentral

Norstella workshop
Globale vs. nasjonale eID-løsninger

Oslo, 16. September 2014

Lothar Fritsch

- Forsker innenfor IKT Sikkerhet, Personvernsteknologi og e-ID hos Norsk Regnesentral
- Mastergrad i informatikk, spesialist i informasjonssikkerhet
- Industrierfaring som Product Manager
- Doktorgrad i Frankfurt's Goethe-Universitet innenfor "Information Systems"-avdeling i økonomisk fakultet. Fokus på personvern og e-ID i mobilapplikasjoner
- Jobber med forskjellige prosjekter i Norge og EU-sammenheng

Web: ***http://www.nr.no/ ~lothar***

Agenda

1. Sosiale Medier
2. E-ID – kort definisjon og egenskaper fra en forsker
3. Globale e-ID systemer
    1. Sosiale medier som facebook, Google, og andre OpenID-løsninger
    2. Industriallianser Kantara, Fido Alliance, OASIS
4. Muligheter og risiko
5. Spesielt om personvern

Sosiale nettverk, sosiale medier

- "The term social software characterises infrastructures, platforms and applications that enable users to communicate, collaborate and coordinate themselves via networks, to establish and maintain relationships and thus in some way map social aspects of real life to an online environment."
- Its main functions are:
  - Information Management: finding, evaluating and administration of information
  - Self Management: present aspects of yourself on the Internet
  - Relationship Management: represent and maintain contacts to others via Internet"

(A comparison of privacy issues in collaborative workspaces and social networks, Martin Pekárek & Stefanie Pötzsch, IDIS journal 2009:2, PrimeLife project; Boyd/Ellison 2007)

Sosiale nettverk, sosiale medier

- "Regardless of the purpose of a WBSN, one of the main reasons for participating is to share and exchange information with other users. "

(Carminati et al: Enforcing Access Control in Web-based social networks, ACM Transactions on Information and System Security 2009:1)

Oppsummering Sosiale Nettverk

- Sosiale nettverk er plattformer på nett som krever personlig innlogging og opprettelse av et profil
- Transaksjoner på plattform er enten rettet til egne eller fremmede dataobjekter (”medier”), eller til andre bruker igjennom en modell av sosiale relasjoner og meldingstjenester
- Det fins muligheter til å beskytte sine egne medier med adgangskontrollregler for andre bruker eller grupper av brukere
- Formål til en sosial nettverk er avgjørende for hvilke informasjoner fins, og hva de er brukt til.
- Plattformen får vanligvis godt innsyn i relasjoner og bruk av objekter.

Agenda

1. Sosiale Medier
2. E-ID – kort definisjon og egenskaper fra en forsker
3. Globale e-ID systemer
    1. Sosiale medier som facebook, Google, og andre OpenID-løsninger
    2. Industriallianser Kantara, Fido Alliance, OASIS
4. Muligheter og risiko
5. Spesielt om personvern

Hva er en e-ID?

- …en liten bit digital data basert på algoritmer i programmvare 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

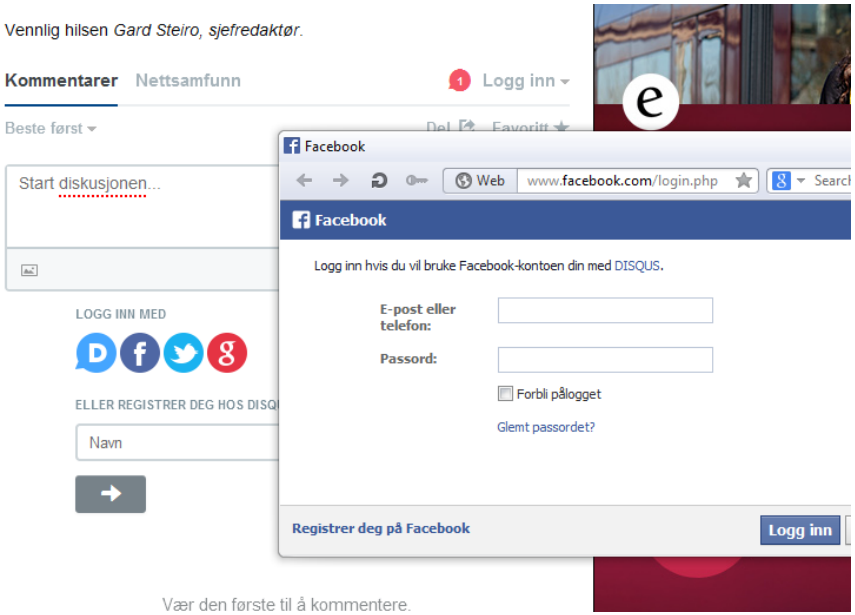
- e-ID brukes til forskjellige formål i applikasjoner og tjenester på nett
- Hvilke opplysninger må tilknyttes til en e-ID for å lage en trygg transaksjon er helt avhengig av applikasjoner som tar i bruk e-IDer
- En e-ID system som utvider bruksområdet til nye applikasjoner kan skape trusler både for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

Agenda

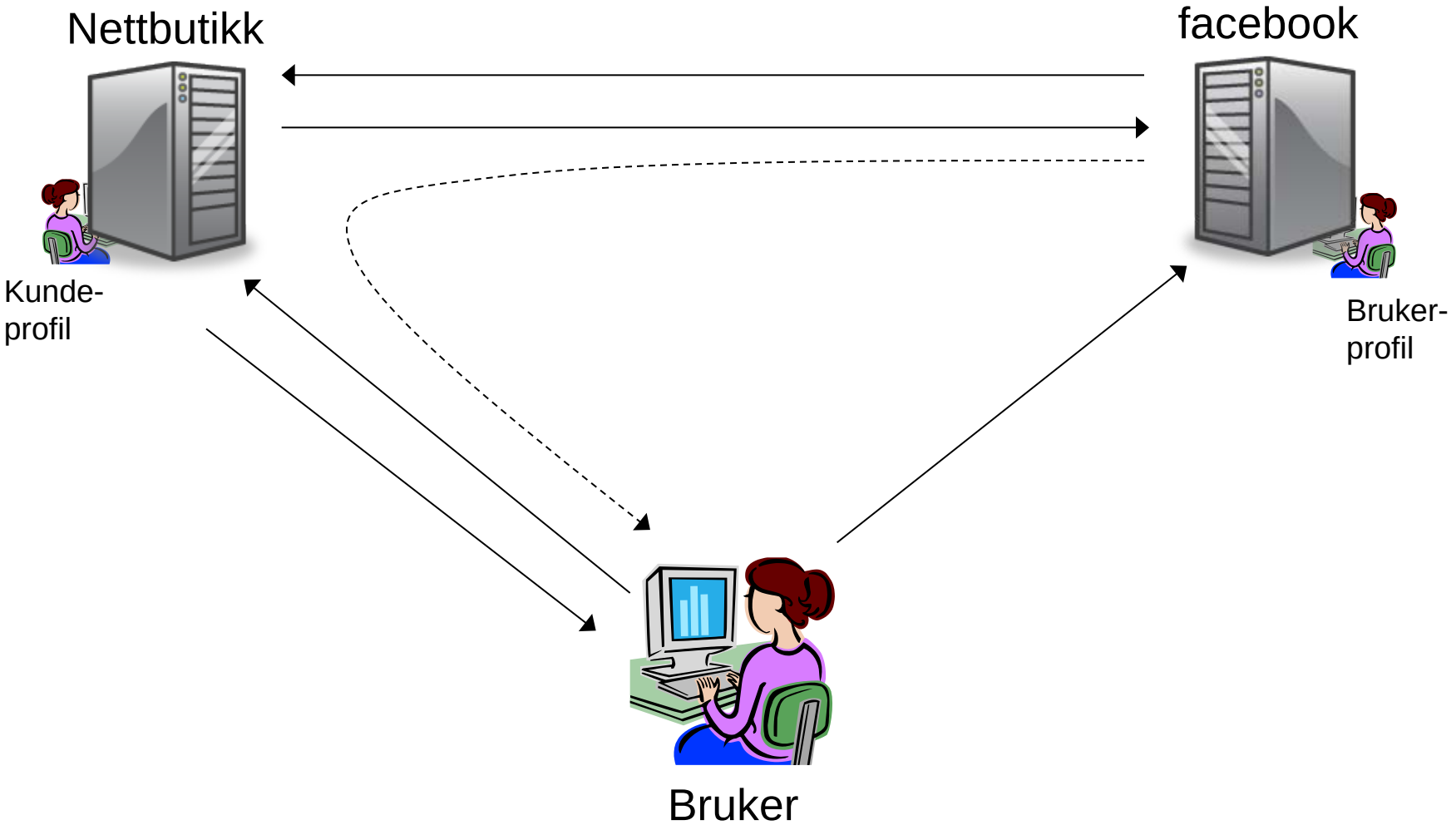
1. Sosiale Medier
2. E-ID – kort definisjon og egenskaper fra en forsker
3. Globale e-ID systemer
    1. Sosiale medier som facebook, Google, og andre OpenID-løsninger
    2. Industriallianser Kantara, Fido Alliance, OASIS
4. Muligheter og risiko
5. Spesielt om personvern

facebook, Google, OpenID

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



OpenID – slik fungerer det



OpenID - implikasjoner

- 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 provider er ofte ikke underlagt norsk rett
- Integrasjon av hardware-token er mulig, men knapt i bruk med de store OpenID-økosystemer

Industri-e-ID I : Kantara

- Oppfølger til Liberty Alliance
- Basert på SAML federations med attributer
- 4 sikkerhetsnivåer (assurance levels), definisjon av skadenivåer, eksempler

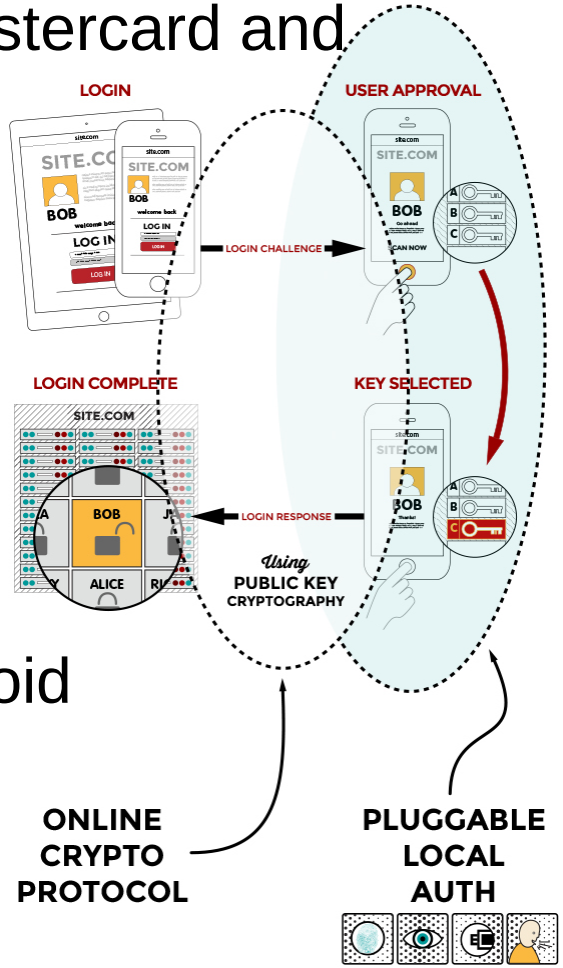
Table 2-1. Four Assurance Levels

Level	Description
1	Little or no confidence in the asserted identity's validity
2	Some confidence in the asserted identity's validity
3	High confidence in the asserted identity's validity
4	Very high confidence in the asserted identity's validity

- Sertifiserings- og akkrediteringsprosedurer

Industri-e-ID II : Fido Alliance

- ARM, Google, Lenovo, Samsung, Mastercard and many other companies
- Aim: password-free authentication with 2 factors: a key & a token
- Strong group with mobile CPU vendor, card vendors, device vendors and ecosystems
- Mobile e-ID ecosystem for ARM/Android

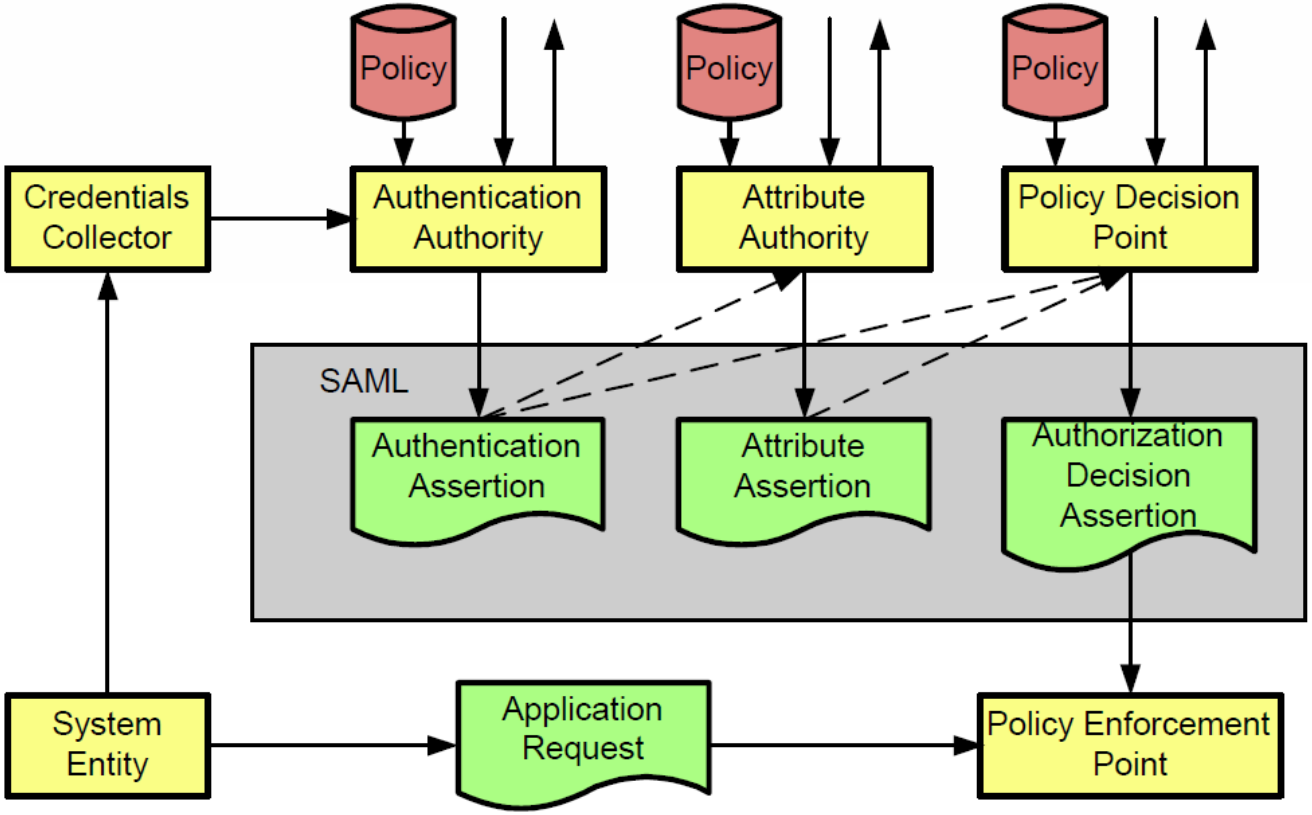


Industri-e-ID III : OASIS

- Organization for the Advancement of Structured Information Standards (**OASIS**)
- OASIS is a member-led, international non-profit standards consortium concentrating on structured information and global e-business standards
- Members of OASIS are
  - Vendors, users, academics and governments
  - Organizations, individuals and industry groups
- Develops **Security Assertion Markup Language** (SAML) 2.0 OASIS Standard
- Used e.g. in Danmark & Norway for e-government

Industri-e-ID III : OASIS

SAML: Scope



Agenda

1. Sosiale Medier
2. E-ID – kort definisjon og egenskaper fra en forsker
3. Globale e-ID systemer
    1. Sosiale medier som facebook, Google, og andre OpenID-løsninger
    2. Industriallianser Kantara, Fido Alliance, OASIS
4. Muligheter og risiko
5. Spesielt om personvern

Muligheter

- Det er mulig å bygge opp meglerinfrastruktur: inkludering av fremmede IDP og brukere i egne webservices.
- OpenID har lave kostader, og lav tilitsnivå mot sosiale medier og sine brukere. Mange brukere!
- Kantara er ikke ulik STORK-spesifikasjon i Europa – 4 sikkerhetsnivåer definert, akkreditering. Internasjonal interoperabilitet.
- OASIS videreutvikler SAML-baserte føderasjoner i nye kontekster, for eks. Cloud access. Passer til en stor antall etablerte webtjenester med brukeridentifisering.
- Fido skaper en hardware-sikkret økosystem for mobile terminaler.

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?

Walled gardens – åpne e-ID økosystemer

Dette loves.

Dette leveres.

Og hvem er grisen her? Tjenesten?

Sikkerhetsmodul

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

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 partier? Er det hemmelig informasjon, kritisk informasjon, eller skadelig informasjon involvert?

Agenda

1. Sosiale Medier
2. E-ID – kort definisjon og egenskaper fra en forsker
3. Globale e-ID systemer
    1. Sosiale medier som facebook, Google, og andre OpenID-løsninger
    2. Industriallianser Kantara, Fido Alliance, OASIS
4. Muligheter og risiko
5. Spesielt om personvern

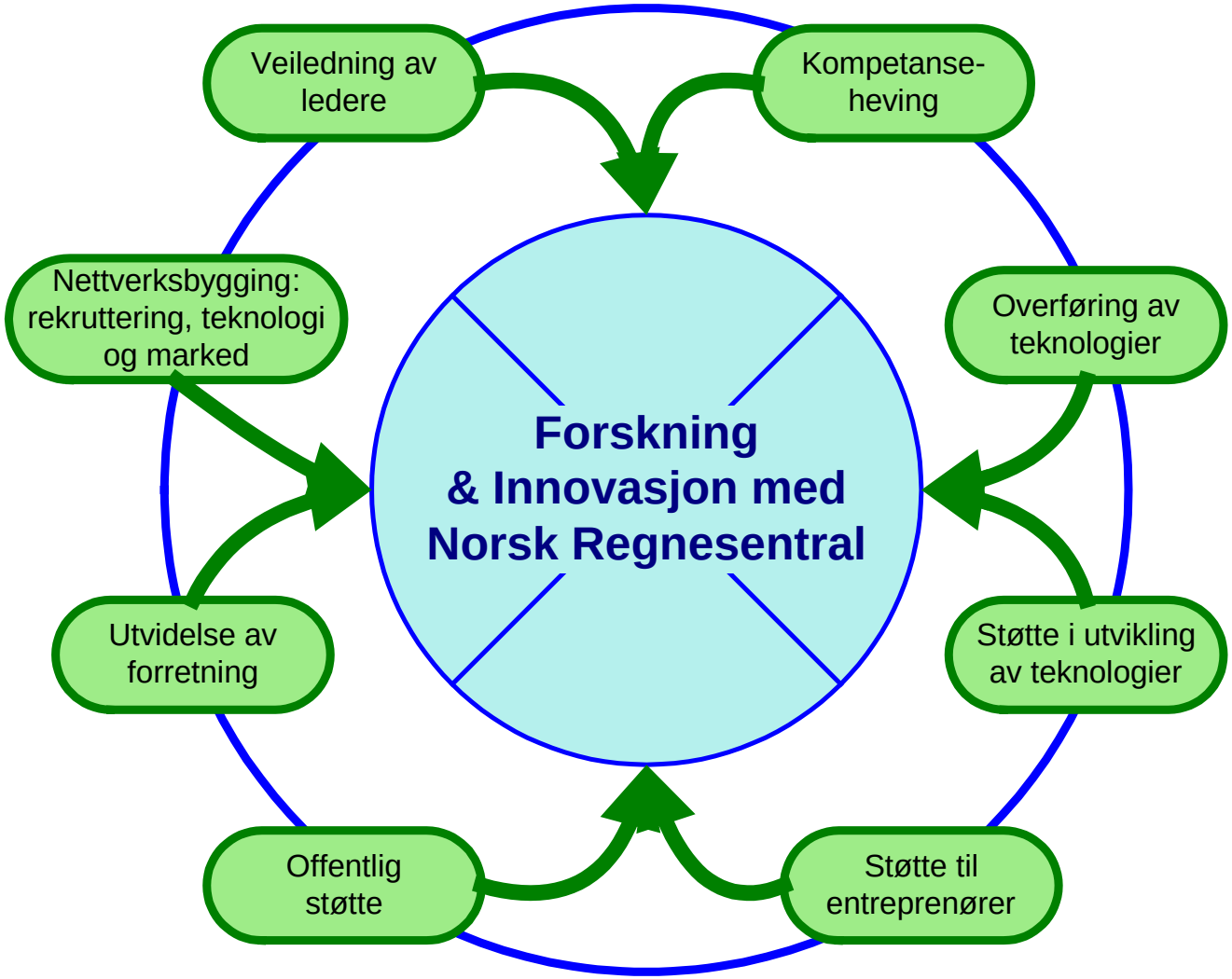
e-ID og Personvern

- 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 Personvern

- En e-ID-økosystem kan dø av for mye forurensing med dubletter, falske identiteter, forfalskete eller utdaterte attributer osv.
- 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

Skap innovasjon med oss!



Mulige sammenarbeidsformer

- 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