PKI-basert eID for helsesektoren – hvorfor og hvordan?

FRISC frokostseminar

Oslo, 2. juni 2014

Jon Ølnes, Unibridge AS

http://www.unibridge.no

jon.olnes@unibridge.no

Status eID i helsesektoren i dag

- **Primærhelsetjenesten – og de fleste legevakter**
  - Brukernavn og passord for autentisering – både nettverkspålogging og EPJ
  - Buypasskort med kvalifisert, PKI-basert eID kun for signering (resepter og annet)
- **Sykehus, felles løsninger per helseregion**
  - Overgang til smartkortbasert nettverkspålogging – interne PKI'er, egen «lomme» på Buypasskort
  - Kvalifisert eID fra Buypass i samme kort for de som skal signere eller nå Kjernej.
  - I hovedsak brukernavn/passord for pålogging til EPJ og andre systemer
- **Legevakter, større byer**
  - Smartkortbasert nettverkspålogging som for helseregionene, i hovedsak Citrix el.l. med terminalservere (kan flytte sesjon med å flytte smartkortet)
  - Signering som for helseregionene
- **Andre virksomheter, inkludert hjemmehjelp, sykehjem osv. (omsorg)**
  - Stort sett brukernavn og passord
- **Fellestjenester – Kjernejournal, Reseptformidleren**
  - Autentisering med Buypass kvalifisert eID
- **<u>Gjentatt, tungvint pålogging er identifisert som «tidstyv» i dag</u>**

Styrende dokumenter i dag

- **Helseregisterloven, personopplysningsloven med mer**
  - Grunnlag: Helseopplysninger skal lagres lokalt og ikke deles
- **Norm for informasjonssikkerhet i helse- omsorgs- og sosialsektoren**
  - Omforent sett av krav basert på lovverket
- **Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor**
  - 4 nivåer, sensitiv informasjon krever «nivå 4», som i dag kun kan oppfylles av PKI-basert eID med spesialelektronikk
- **Kravspesifikasjon for PKI i offentlig sektor**
  - Forvaltningsstandard som må oppfylles for at en leverandør/eID skal kunne brukes mot offentlige tjenester – kravspesifikasjon ved anskaffelser
  - Selvdeklarasjon med tilsyn hos Post- og teletilsynet
  - «Person-Høyt», krever at eID er kvalifisert etter:
- **Esignaturloven, som følger av EUs e-signaturdirektiv fra 1999**
  - Definerer «elektronisk signatur», «avansert e-sig», «kvalifisert e-sig»
  - Og kvalifisert sertifikat – med enda en registrering og tilsyn hos PT
- **Eforvaltningsforskriften – for offentlige virksomheter, deler av sektoren**

Nye styrende dokumenter

- **Pasientjournalloven og ny helseregisterlov – i prosess**
  - Pasientjournal – register for behandlingsrettede helseopplysninger
  - Helseregister – «sekundærregistre» for forskning, statistikk med mer
  - Grunnlag: Helseopplysninger skal være tilgjengelige ved behov også på tvers av virksomheter – «én innbygger – én journal»
- **eIDAS – EU-forordning om «electronic identification and trust services for electronic transactions in the internal market»**
  - Gjelder som lov i alle EU-land fra 1. juli 2016 og skal innarbeides i norsk lov
  - Erstatter e-signaturdirektivet
  - Vesentlig økt omfang – vil kaste om på norske spesifikasjoner
  - Rammeverket må endres – kommer spesifikasjon av «assurance levels» fra EU: High, substantial, low – nivå 4, 3, 2 – strengere krav enn eksisterende i Norge(?)
  - Kravspesifikasjonen erstattes av referanser til europeiske standarder(?)
- **Ny personvernforordning er i arbeid i EU – kan bli vedtatt i 2015**

eIDAS scope

General provisions:
- Definitions
- Personal data processing

Electronic identification

Trust services

Align with upcoming EU Data Protection Regulation

"Privacy by design" principle

Conditions under which Member States shall recognise electronic identification means of natural and legal persons falling under a notified electronic identification scheme of another Member State.

Cross-border identification and authentication in the EU – at least for public services

Rules for (qualified) trust services, which are:
- Certificates for e-signature (natural person) and e-seal (legal person)
- Signing and signature validation services
- Time stamp services
- Certificates for website authentication
- Registered delivery services for electronic documents
- Preservation/archiving of signed documents

Admissibility of electronic documents and mutual recognition of *qualified* trust services across the EU.

***Qualified* = fulfilling eIDAS requirements**

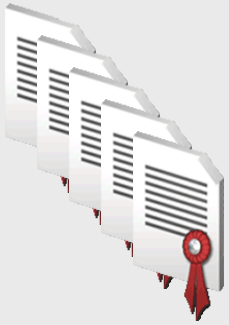
eIDAS, implementing acts and standards

eIDAS regulation

Will apply entirely in all Member States from 1st July 2016

Articles on delegated and implementing acts, and on the eID interoperability framework, apply from <summer 2014>, i.e. start work on these immediately

Delegated and implementing acts



1 delegated act – on certification bodies for QSCD (Qualified Signature Creation Device)

26 paragraphs referring to implementing acts – some state that Commission shall implement, other state may implement

Delegated and implementing acts will apply for all Member States

European and international standards

Implementing acts will to a large degree point to standards

Use of these standards shall provide “presumption of compliance”

ETSI and CEN works according to current standardisation mandate M460 – there is a need to revise and extend this mandate

Will authentication be standardised through the same mandate?

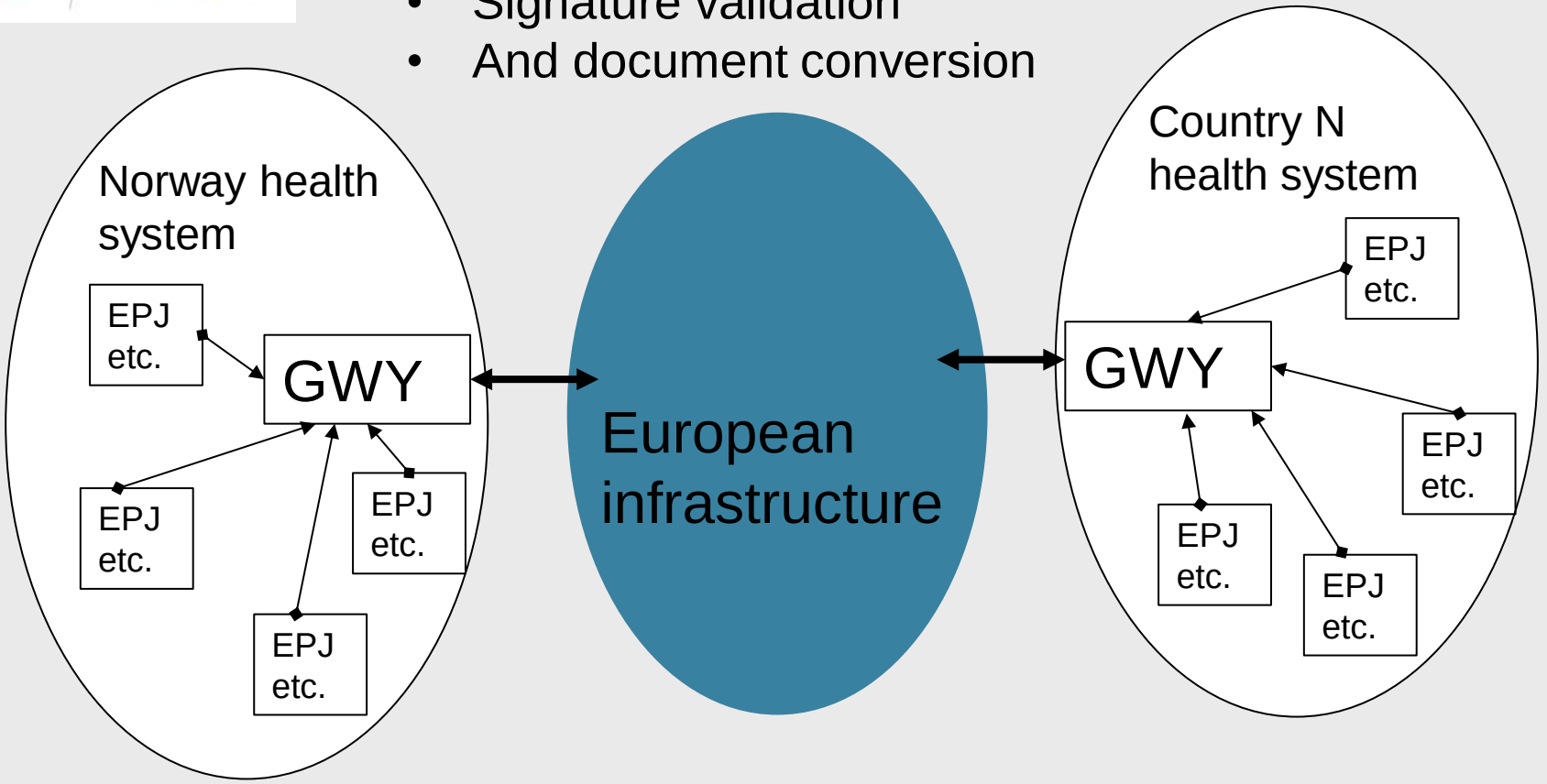
Helsenett og Internett

- **Helsenettet – lukket nettverk for sektoren**
  - Nettverk og samhandlingstjenester, for eksempel registre
  - Kun helsevirksomheter som oppfyller Normen kan være med
  - Kun personell i slike virksomhet kan ha tilgang
  - Pasientjournaler og helseregistre vil være koplet til Helsenettet
- **Internett – tilgang for pasientene selv**
  - Portal: helsenorge.no – «vanlig nivå 4 pålogging» via ID-porten
  - Antar at en del handlinger vil kreve avansert e-signatur – fullmakter for eksempel
  - All informasjon skal etter hvert være tilgjengelig i portalen
  - Skal dette skje i sanntid, eller vil portalen integrere ved asynkron meldingsutveksling?
- **For eID og e-signatur:**
  - eIDAS gjelder ikke for tillitstjenester i lukkede systemer
  - Begrepet «kvalifisert» har bare mening i den grad en skal kommunisere utenfor Helsenettet
  - Signerte dokumenter fra Helsenett til Internett (og til utlandet?)
  - Signerte dokumenter fra pasienter til Helsenettet (eks. fullmakter, samtykker)?

Internasjonalt, epSOS

Gateways issue assertions:

- Identity and authorisations
- Signature validation
- And document conversion



Distribuert og sentralisert informasjon

- **Én EPJ for Norge, all informasjon om en pasient samlet ett sted?**
  - EPJ kan skalere til så mange personer, men migrasjonsjobben er formidabel
- **I dag hver virksomhet sin EPJ – 1000-vis av EPJ'er uten integrasjon**
  - Ut over asynkron meldingsutveksling for noen typer informasjon
  - EPJ'en under pulten til fastlegen kan ikke integreres
- **Dette MÅ reduseres – i hvert fall ned til et 100-talls EPJ'er(?)**
  - Én innbygger – én journal, men med mange EPJ'er
  - **Sentrale metadata** (Kjernejournal?) som viser hvor informasjon finnes

- **«Tilgang på tvers» mellom virksomheter til sensitiv pasientinformasjon**
- **Tilgang bare til autorisert personell og kun ved behov**
- **Hvordan kan en løse dette med tilstrekkelig sikkerhet?**

Kommunikasjonsmønstre

- **Asynkron meldingsutveksling – signatur fra virksomhet og/eller person**
  - Send (strukturert) melding, leses og besvares senere
  - Som dagens eResept med mer
  - System-system eller person-system
- **Synkron meldingsutveksling (Web Service) – autentisert kanal og/eller signatur**
  - Send strukturert melding over oppkoplet sesjon
  - System-system eller med GUI og person-system
  - Strukturert svar vanligvis i samme sesjon (kan ha asynkront svar)
  - Problem 1: Strukturering av alle forespørsler?
  - Problem 2: Meldingsstørrelse for svar (MR-bilder ol. ?)
- **Pålogging direkte til system i annen virksomhet (med GUI)**
  - Men forskjellige EPJer og andre systemer har forskjellig brukergrensesnitt etc.
  - Kan ikke ha opplæring for alle i alle systemer
  - Kan brukes for fellestjenester med ett grensesnitt (Kjernejournal etc.)
  - Alternativ: Uniformt portalgrensesnitt mot «alle» EPJer – neppe realistisk(?)
- **Spesialtilfelle: Pålogging til system i annen virksomhet ved «besøk»**
  - Eksempel (EPJ-standard del 2): Legevaktlege besøker sykehjem – tilgang til EPJ

Hvorfor PKI-basert eID?

- **Person-eID:**
  - Signering er nødvendig for mange meldinger og mange personer
  - Autentisering utenfor egen virksomhet med høy nok kvalitet
  - Helst også for autentisering i egen virksomhet (brukernavn/passord internt kan være OK hvis systemene ellers er godt nok sikret)
- **Virksomhets-eID:**
  - Virksomhetssignatur på (alle) meldinger
  - Meldingskryptering
  - Autentiserte kommunikasjonskanaler mellom virksomheter (proxy-løsninger)
- **Web-serversertifikater:**
  - For alle kommunikasjonskanaler (web front-end løsninger)
- **Annet:**
  - Systemer (f.eks. EPJ), utstyr og annet som trenger autentisering (sensornettverk)

Personautentisering lokalt

1. **Pålogging til operativsystem/nettverk**
   - Kan bruke PKI-eID med smartkort el. på «nettverksnivå». For Microsoft spesielle, virksomhetsspesifikke utvidelser i sertifikatene
2. **Pålogging til EPJ og andre fagsystemer**
   - Implisitt logget inn gjennom trinn 1 (AD el.)
   - PKI-basert eID på «tjenestenivå» direkte mot EPJ (som må tilrettelegges for dette)
   - Engangspålogging (SSO) ved IdP (Identity Provider) internt i virksomheten
   - Pseudo-SSO – portal som lagrer brukernavn/passord mot forskjellige systemer og oppgir på vegne av brukeren. Nivå 4 eller IdP mot portalen.

- **Navn for brukeren (helsepersonell etc.)**
  - UNID i sertifikater (norsk system i dag – ikke fødselsnummer i sertifikatene)
  - Fødselsnummer og D-nummer (FNR/DNR)
  - HPN (Helsepersonellnummer)
  - Brukernavn for operativsystem og for EPJ og diverse systemer
  - En person kan ikke få brukernavn i alle systemer i andre virksomheter – må identifiseres med ett navn på tvers
- **Oversettelse mellom navn er viktig**
  - Virksomhetene må ha oversettelse mellom HPN og brukernavn
  - Til enhver tid oppdatert oversikt over alle brukere med tilganger og roller!
  - Sterkt anbefalt (obligatorisk?) å ha ett sentralt brukerregister for alle systemer
  - Oversettelse kan kreve registeroppslag (HPR) eller tjeneste fra eID-utsteder – utstederne tar betalt for dette per transaksjon i dag
- **Hvilket/hvilke navn skal brukes for tilgang på tvers?**

Autorisasjoner lokalt

- **Lokale autorisasjoner for tilgang til systemer og for tilgang til informasjon om spesifikk pasient**
- **Lokal autorisasjon for bruk av eksterne fellessystemer (som Kjernejournal) og for å hente informasjon eksternt**
- **Autorisasjon for ekstern informasjon for pasient**
  - Autorisasjon for eksternt + autorisasjon for pasient i EPJ + (i mange tilfeller) eksplisitt samtykke fra pasient
  - Kan være både helsepersonell og administrativt personale (?) – hente informasjon kan være administrativ jobb
- **Spesialtilfelle: Blålyssituasjon – gjelder også for tilgang til informasjon eksternt(?)**
- **Utgående tilgangskontroll basert på alt dette**
  - Sjekke at brukeren har lov til å gå ut og hente informasjon
  - **Må antagelig baseres på (revers) proxy** som også autentiserer virksomhet mot eksterne ved TLS-protokollen og/eller virksomhetssignatur på meldinger
  - Bevis kan utstedes av virksomheten (for eksempel signert SAML for identitet, signert XACML for rolle, behandlingssituasjon og samtykke) og legges ved utgående trafikk – «push modell»
  - Eller en kan tilgjengeliggjøre spørregrensesnitt der andre virksomheter kan spørre etter autorisasjoner – «pull modell». Kombinasjon av push og pull mulig, og spørring kan være mot sentralt ansattregister og Helsepersonellregisteret (HPR).

Utgående kall fra virksomhet

1. **Asynkrone meldinger:**
   - Identitet (SAML?) og «bevis» for autorisasjoner (XACML?) i melding
   - Semantikken er viktigst, ikke kodingen…..
   - Signer melding (virksomhetssignatur, eventuelt også personsignatur), krypter melding med mottakers virksomhetssertifikat
2. **Synkrone meldinger:**
   - Sett opp gjensidig autentisert TLS-forbindelse mellom revers proxy og web-server i annen virksomhet. Begge virksomheter autentiseres, kontroll også av utgående trafikk.
   - Nødvendige «bevis» i melding – kan også overføres separat ved oppsett av TLS eller som første meldinger over TLS-kanal
   - Signer melding (virksomhetssignatur, eventuelt personsignatur), krypter eventuelt melding (kanskje ikke nødvendig hvis TLS-kanal)
3. **On-line tilgang:**
   - Sett opp gjensidig autentisert TLS-forbindelse mellom revers proxy og web-server i annen virksomhet – autentiserer begge virksomhetene
   - Overfør nødvendige «bevis» som første trafikk på TLS-kanalen («push modell»)
   - Eller egen (PKI-basert) autentisering av personen
   - Interaktiv tilgang etablert

Autentisering i annen virksomhet eller fellestjeneste

1. **Alle virksomheter må ha web-server for mottak av innkommende trafikk**
   - Må ha EV-SSL eller tilsvarende sertifikat for TLS-kanal
   - Må ha private nøkler for virksomhetssertifikater for dekryptering av meldinger
2. **Autentisere begge virksomheter – proxy for utgående trafikk?**
   - Virksomhetssertifikat – TLS-protokoll og/eller virksomhetssignatur på meldinger
   - Organisasjonsnummer på virksomhetsnivå (dagens virksomhetssertifikater)
   - Behov for å autentisere på nivå avdelinger/enheter – RESH-id kan kanskje brukes
   - MÅ komme fra en virksomhet – ikke lov med tilgang fra «tilfeldig» PC
3. **Identifisere eller (re-)autentisere person?**
   - Identifisere: Stole på identifikasjon av person fra annen virksomhet
   - Reautentisere: Personsignatur på melding, eller (synkron og on-line) omdirigere person for autentisering (egen «ID-port» i Helsenettet?)

Hva må samkjøres?

- **Avtaleverk: Bilaterale avtaler skalerer ikke, men kan brukes i noen tilfeller**
  - «Rammeavtale» eller tilknytningsavtale for tilgang på tvers
  - Nedfelle krav i Normen?
- **Ansvarsforhold må være helt klare**
  - Virksomheter tar ansvar + at person må kunne ansvarliggjøres «på tvers»
- **Identifisering (navngivning)**
  - Personer: HPN (og PNR/DNR for de som har dette) – eller nytt helse-ansattnummer?
  - Virksomheter: Org.nr og RESH-id el.l (avdelinger/enheter)
  - Roller: Roller i Helsepersonellregisteret (andre, for eksempel ikke-helsepersonell?)
- **Autentisering**
  - Personer: e-ID nivå 4 + IdP-tjenester
  - Virksomheter: Virksomhetssertifikat (også for avdelinger/enheter som i RESH?)
- **Autorisasjoner, attributter – utfordringen er semantikk**
  - Utgående: Dokumentere autorisasjon og behandlingssituasjon i egen virksomhet
  - Utgående: Samtykke fra pasient og dokumentasjon av dette
  - Innkommende: Godta dokumentasjon av autorisasjon, behandlingssituasjon og samtykke og autorisere til informasjon etter behov
  - Innkommende: Sjekke registre for verifisering og ytterligere informasjon

Smartkort eller annet?

- **Smartkortløsninger utbres nå – vil være løsning på kort sikt**
  - Kjøpe kort og eID i markedet, som nå?
  - Helsepersonellkort med egen eID for sektoren?
  - Utnytte infrastruktur for Nasjonalt ID-kort med eID når dette kommer?
  - Blanding, for eksempel egen eID for sykehus, men kjøpe for primærsektoren?
- **USB-pinne kan være alternativ (men USB skrudd av en del steder)**
- **Hva med serverbasert lagring av private nøkler?**
  - For tungvint for autentisering (OTP, passord med mer), men kan være et alternativ for signering (autentiseres med smartkortet, signerer på server)
- **Hva med mobilt utstyr – hjemmehjelp, legevisitt osv.?**
  - Utstyr kommer i økende grad med innebygd krypto – bør kunne brukes
  - Men må da antagelig være personlig utstyr

- **Lag generiske krav til eID og evaluer løsninger mot kravene**

Noen utfordringer for eID

- Registeringsprosessen med personlig frammøte
- Utstedelsesprosess med sentral personalisering av kort – tar tid
- Lånekort – også for distriktslegen i Karasjok?
- Felles kort og eID – gir ikke bruk for nettverkspålogging?
- Lokalt utstedt eID gir nettverkspålogging – men god nok kvalitet?
- Kvalifisert eller ikke? Kvalifisert er et juridisk begrep. Ikke-kvalifisert kan ha samme sikkerhet, men gjensidig anerkjennelse er vanskeligere.
- Navngiving person: Fødselsnummer i dag – ikke optimalt (personvern, ikke alle har FNR). HPN for de som har dette (helsepersonell)? Hva med andre? Dagens løsning gir mange oversettelser mellom UNID og FNR, og leverandør tar betalt for disse. Tungvint med mange registeroppslag.
- Navngiving virksomhet: Trenger også nivå avdeling/enhet (RESH?)
- Tilrettelegging av systemer for bruk av PKI-basert eID (eller bruk av IdP)
- Samkjøring av identitetshåndtering på tvers av systemer internt, flere hundre systemer internt i et sykehus…..
- Brukervennlighet og effektivitet !!!