Norm for informasjonssikkerhet
www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Krav ved bruk av PKI ved ekstern kommunikasjon

Støttedokument
Faktaark nr. 49
Versjon: 2.1
Dato: 02.10.2018

Formål	Gi oversikt over krav til PKI i forbindelse med virksomhetens eksterne kommunikasjon.		
Ansvar	Dataansvarlig er ansvarlig for å etablere løsninger og prosedyrer ved bruk av PKI.		
Gjennomføring	Før, under og ved bruk av PKI-løsninger for signering, autentisering og kryptering ved ekstern kommunikasjon.		
Omfang	Gir en oversikt over krav til bruk av sertifikatklassene virksomhetssertifikat og personsertifikat (Person-Høy) ved ekstern kommunikasjon.		
Målgruppe Dette faktaarket er spesielt relevant for:	☒ Leverandør ☒ IKT-ansvarlig ☐ Forsker ☐ Prosjektleder	☒ Sikkerhetsleder/ sikkerhetskoordinator ☒ Virksomhetens leder/ledelse ☐ Forskningsansvarlig	☐ Medarbeider/ansatt ☒ Databehandler ☐ Personvernombud
Hjemmel	• Personvernforordningen artikkel 32 • Lov om elektronisk signatur § 4.		
Referanser	• Norm for informasjonssikkerhet (Normen), kap. 5.2.2 og 5.5.3 (www.normen.no) • Kravspesifikasjon for PKI i offentlig sektor (https://www.regjeringen.no/no/dokumenter/kravspesifikasjon-for-pki-i-offentlig-se/id611085/) • Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor • KITH Rapport R16/06 Rammeverk for elektronisk meldingsutveksling i helsevesenet • Faktaark 16 - Etablering av løsning for meldingskommunikasjon • Faktaark 29 – Hjemmekontor • Faktaark 20 - Sikkerhets- og samhandlingsarkitektur • Faktaark 32 - Elektronisk pasient- og brukerkommunikasjon		

Merknad 02.10.2018: Utdaterte hjemler og referanser er fjernet, men dokumentet kan inneholde tekst som er foreldet ut fra siste versjon av Normen, ny personopplysningslov, endringer i helselovgivning eller EUs personvernforordning.

Innledning

PKI i sektoren har en rekke bruksområder. Krav ved bruk av PKI er beskrevet en rekke steder, avhengig av bruksområdet. Det er imidlertid noen grunnleggende og generelle krav som gjelder for all bruk av PKI ved ekstern kommunikasjon (inkl. fjernaksess, bruk av hjemmekontor og trådløs kommunikasjon). Dette faktaarket gir en oversikt over disse kravene. For spesifikk bruk av PKI vises det til de ulike faktaarkene og dokumentene som er gitt under referanser.

Definisjon

Med "***Sikkerhetskode for elektronisk ID***" menes den personlige koden som benyttes til å autentisere på sikkerhetsnivå 4

Nr	Handling
1.	**Grunnleggende krav til PKI** a) Før anskaffelse av PKI-løsninger for signering, kryptering eller autentisering for ekstern kommunikasjon skal virksomheten gjennomføre risikovurdering av den konkrete løsningen. Risikovurderingen kan gjennomføres av virksomheten selv eller virksomhetens leverandør

Nr	Handling
	b) Iht. Normen og ”Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor” skal PKI-løsninger i sektoren etableres på sikkerhetsnivå 4 c) Ved gjennomføring av risikovurdering av PKI-løsninger skal nivå for akseptabel risiko settes lik risikonivå 4 i ”Rammeverk for autentisering og uavviselighet i elektronisk kommunikasjon med og i offentlig sektor” d) Om virksomheten utarbeider kravspesifikasjoner for etablering av PKI, skal leveransen ivareta ”Kravspesifikasjon for PKI i offentlig sektor”
2.	**Generelt om sertifikater** a) PKI innebærer at en nøytral og tiltrodd tredjepart (TTP) utsteder et sertifikat. Utstedere av kvalifiserte sertifikater til sektoren må være registrert hos Post- og teletilsynet. For oversikt over registrerte tilbydere av sertifikater etter selvdeklarasjonsordningen, se http://www.npt.no b) Med kvalifiserte sertifikater menes sertifikater utstedt etter en sertifikatpolicy som er i tråd med lov om elektronisk signatur og av en utsteder som er registrert hos Post- og teletilsynet c) Et kvalifisert sertifikat er personlig og fungerer som et legitimasjonsbevis og bekrefter at en kommunikasjonspart er den han utgir seg for d) Før virksomheten anskaffer sertifikater og teknisk løsning for PKI må virksomheten avklare med sin kommunikasjonspart hvilken leverandør som benyttes og om denne kan gjøre oppslag i den aktuelle leverandørens katalog (for eksempel om PKI skal benyttes mellom virksomheter som er tilknyttet helsenettet må det avklares med Norsk Helsenett SF hvilke leverandører av sertifikater som støttes)
3.	**Sertifikatklasse: Person-Høyt** a) Er et personsertifikat for en bestemt fysisk person som entydig identifiseres i sertifikatet. Person-Høyt er basert på kvalifiserte sertifikater b) En PKI-løsning i sektoren kan blant annet inkludere et smartkort og en personlig tilleggsinformasjon, for eksempel en sikkerhetskode for elektronisk ID eller et fingeravtrykk. Smartkortets innhold i kombinasjon med eierens for eksempel sikkerhetskode for elektronisk ID eller fingeravtrykk utgjør den enkeltes personlige signatur og identitetsbevis, og må behandles deretter. Det er krav om å vise godkjent legitimasjon for å få utlevert smartkort og/eller sikkerhetskode for elektronisk ID.
4.	**Sertifikatklasse: Virksomhet** a) Et virksomhetssertifikat tildeles en virksomhet som er registrert i Enhetsregisteret (se www.brreg.no) og som entydig identifiseres i sertifikatet iht. organisasjonsnummeret i Enhetsregisteret b) Virksomheten avgjør hvordan virksomhetssertifikatet skal benyttes, eksempelvis om det skal brukes av en fysisk person autorisert av virksomheten eller av en automatisert prosess under virksomhetens kontroll, for eksempel en server c) Det kan ved behov utstedes flere virksomhetssertifikater til samme virksomhet (f.eks. løsning for utsendelse av epikriser, tilgang fra hjemmekontor mv.)
5.	**Etablere prosedyrer** a) Virksomheten skal utarbeide en prosedyre for oppdatering av eget og kommunikasjonspartneres sertifikat når disse utløper b) Virksomheten bør utarbeide instruks til ansatte med smartkort. Instruksen bør ha med følgende: - Smartkortet skal betraktes som et personlig identitetsbevis og oppbevares på en sikker måte - Lån aldri bort smartkortet ditt til andre - Beskytt din personlige sikkerhetskode for elektronisk ID og gi den aldri til andre - Skriv aldri ned sikkerhetskode for elektronisk ID din slik at den kan leses av andre

Nr	Handling
	- Hvis kortet mistes eller blir stjålet, må dette straks meldes til PKI-leverandørens sperretjeneste - Sikkerhetskode for elektronisk ID på mobiltelefon og nettbrett er ikke det samme som SIM-kortes PIN-kode

Eksempler på bruk av sertifikatklasser:

Personsertifikat:

- Helsepersonellet signerer sykemeldinger, resepter, behandlerkrav mv som pakkes i ebXML konvolutt
- En ansatts personlig autentisering ved innlogging i en hjemmekontorløsning
- En servicemedarbeiders personlige autentisering ved innlogging i en fjernaksessløsning
- En pasients personlige autentisering ved innlogging på virksomhetens løsning for elektronisk pasientkommunikasjon

Virksomhetssertifikat:

- Signere ebXML konvolutt som inneholder en eller flere andre meldinger som kan være signert med personsertifikat
- Autentisering i forbindelse med at en leverandør tilknytter sin supportløsning til virksomhetens nettverk
- Kryptering / dekryptering av meldinger