Norm for informasjonssikkerhet - www.normen.no

Utgitt med støtte av:

Direktoratet for e-helse

Krav til teknisk løsning ved bruk av betalingsterminal

Støttedokument
Faktaark nr 52
Versjon: 1.1
Dato: 03.10.2018

Formål	Sikre en riktig implementering av løsning for betalingsterminal slik at helse- og personopplysninger ikke kommer uautoriserte i hende eller at systemløsningen for betalingsterminal ikke utsetter EPJ-systemer eller fagsystemer for ikke-akseptabel risiko.		
Ansvar	Virksomhetens leder er ansvarlig for at teknisk løsning for betalingsterminal blir etablert iht. kravene i Normen samt at bruk av betalingsterminal skjer iht. betryggende prosedyrer. I denne sammenhengen må virksomhetenes leder stille krav til leverandør av systemer for betalingsterminal at disse er iht. Normens krav.		
Gjennomføring	Kravene gjelder før etablering av løsning for betalingsterminal og ved bruk av løsningen.		
Omfang	Omfatter etablering og bruk av teknisk løsning for betalingsterminal som er integrert med et EPJ-system eller fagsystem.		
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 28 og 32 • Pasientjournalloven § 22		
Referanser	• Norm for informasjonssikkerhet, kapittel 3.3 og 5.3 • Faktaark 5 - Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet • Faktaark 7 – Risikovurdering • Faktaark 10 – Bruk av databehandler • Faktaark 24 - Kommunikasjon over åpne nett • Faktaark 26 - Sikring av trådløs teknologi • Faktaark 49 - Krav ved bruk av PKI ved ekstern kommunikasjon		

Merknad 03.10.2018: 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.

Definisjoner

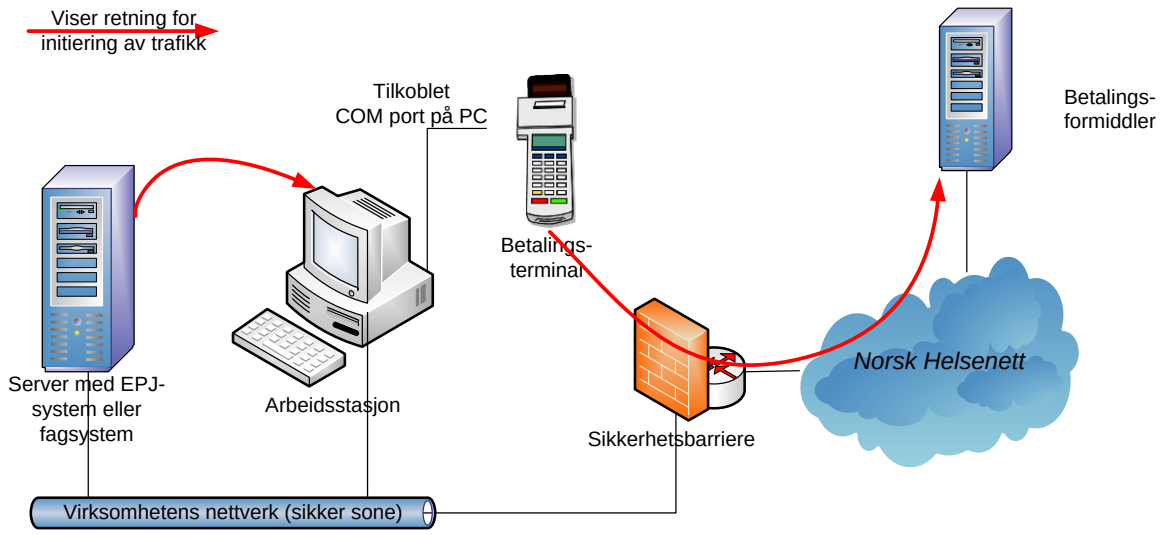
Med "***betalingsterminal***" menes en elektronisk kortavleser som gjør det mulig for en pasient/bruker å betale med de fleste typer betalingskort.

Med "***betalingsformidler***" menes en leverandør av betalingsformidlingstjenester som betalingsterminalen kommuniserer med.

Nr.	Handling
1.	**Fastsette bruk av betalingsterminal** a) Virksomhetenes ledelse skal beslutte bruk av betalingsterminal som er integrert mot et EPJ-system eller fagsystem b) Det skal etableres prosedyrer for bruk av betalingsterminal c) Konfigurasjonskart skal oppdateres med løsning for betalingsterminal d) Det skal inngås en databehandleravtale med leverandør av betalingsterminalløsning. Databehandleravtalen kan inngå som en del av de andre avtalene mellom partene
2.	**Risikovurdering** a) Før etablering av løsning for betalingsterminal skal virksomheten gjennomføre en risikovurdering av løsningen

Nr.	Handling
	b) Eksempler på senarioer som bør vurderes: o Det initieres trafikk fra Internett til betalingsterminal med fare for å kompromittere helse- og personopplysninger i EPJ-systemet, fagsystemet og nettverket o Det initieres trafikk fra ISDN, analog telefonlinje eller mobilbasert kommunikasjon til betalingsterminal og betalingsformidler med fare for å kompromittere helse- og personopplysninger i EPJ-systemet, fagsystemet og nettverket o Det initieres trafikk fra betalingsterminal til server eller arbeidsstasjoner med EPJ-system / fagsystem med fare for å koble (route) trafikk mellom Internett og utstyr med helse- og personopplysninger o Det overføres fødselsnummer og / eller helse- og personopplysninger til betalingsterminal med fare uautorisert tilgang og / eller utlevering av fødselsnumre og helse- og personopplysninger o At virksomhetens nettverk med EPJ-system og betalingsterminal ikke er sikret med minst to uavhengige tekniske virkemidler fra eksterne nett (betalingsformidler) o Betalingsterminal som benytter trådløst Wlan (for eksempel WiFi - IEEE 802.11) blir brukt til å avlytte å omgå andre sikkerhetstiltak i virksomheten med fare for uautorisert tilgang til helse- og personopplysninger c) Virksomheten kan dokumentere risikovurderingen ved at: o Virksomheten gjennomfører risikovurderingen i samarbeid med leverandør av betalingsterminal som utdyper risikovurderingen med sine tekniske spesifikasjoner o EPJ-leverandør eller leverandør av fagsystemet risikovurderer og dokumenterer sin integrasjon mot den aktuelle betalingsterminalen
3.	**Prinsipper for teknisk løsning i nettverket** a) Løsning for betalingsterminal og eksterne nettverk skal sikres med to uavhengige tekniske virkemidler (sikkerhetsbarrierer) b) Om det benyttes betalingsterminaler basert på trådløs LAN (WiFi) for kommunikasjon mellom EPJ-systemet / fagsystemet skal oppkoblingen av betalingsterminalen til virksomhetens trådløse nett skje ved autentisering på sikkerhetsnivå 4 c) Betalingsterminalen skal initiere forbindelse til betalingsformidler. I konfigurasjon av sikkerhetsbarrierene skal det kun åpnes for definert trafikk til en konkret betalingsformidler på definerte tjenester (TCP/IP port numre)
4.	**Prinsipper for integrasjon mot EPJ- eller fagsystem** a) Betalingsterminalen skal konfigureres slik at denne ikke kan initiere trafikk til EPJ-systemet / fagsystemet b) EPJ-systemet / fagsystemet initierer forbindelse til betalingsterminalen og overfører beløpet samt innhenter eventuell kvittering for transaksjonen c) Følgende opplysinger skal ikke overføres til betalingsterminalen: navn, fødselsnummer og helseopplysninger
5.	**Prosedyrer** a) Prosedyrer for bruk av løsning for betalingsterminal bør minst inneholde: o Beskrivelse av korrekt implementering iht. sikkerhetskrav o Krav til gjennomføring av risikovurdering o Krav til integrasjon med EPJ-system / fagsystem o Prosedyre for bruk av løsningen

Eksempel 1
Eksemplet nedenfor viser en betalingsterminal som er tilknyttet en PC via COM port og er integrert med EPJ-systemet / fagsystemet.



Eksempel 2
Eksemplet nedenfor viser en betalingsterminal som er tilknyttet nettverket med TCP/IP og er integrert med EPJ-systemet / fagsystemet.