

 <p>Norm for informasjonssikkerhet - <a href="http://www.normen.no">www.normen.no</a></p>	<p>Utgitt med støtte av:</p> 
<h2 style="text-align: center;">Krav til teknisk løsning ved bruk av betalingsterminal</h2>	<p><b>Støttedokument</b>  <b>Faktaark nr 52</b>  Versjon: 1.0  Dato: 01.06.2011</p>

<b>Målgruppe</b>  Dette faktaarket er spesielt relevant for:	<input checked="" type="checkbox"/> Leverandør <input checked="" type="checkbox"/> IKT-ansvarlig <input type="checkbox"/> Forsker <input type="checkbox"/> Prosjektleder	<input checked="" type="checkbox"/> Sikkerhetsleder/ sikkerhetskoordinator <input checked="" type="checkbox"/> Virksomhetens leder/ledelse <input type="checkbox"/> Forskningsansvarlig	<input type="checkbox"/> Medarbeider/ansatt <input checked="" type="checkbox"/> Databehandler <input type="checkbox"/> Personvernombud
<b>Ansvar</b>	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.		
<b>Gjennomføring</b>	Kravene gjelder før etablering av løsning for betalingsterminal og ved bruk av løsningen.		
<b>Formål</b>	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.		
<b>Omfang</b>	Omfatter etablering og bruk av teknisk løsning for betalingsterminal som er integrert med et EPJ-system eller fagsystem.		
<b>Hjemmel</b>	<ul style="list-style-type: none"> <li>• Personopplysningsloven §§ 13 og 15.</li> <li>• Personopplysningsforskriften §§ 2-4, 2-11, 2-12, 2-13 og 2-15.</li> <li>• Helseregisterloven §§ 16 og 18.</li> </ul>		
<b>Referanser</b>	<ul style="list-style-type: none"> <li>• Norm for informasjonssikkerhet, kapittel 4.6 og 5.5.2</li> <li>• Faktaark 5 - Fastsette akseptkriterier for tilgjengelighet, konfidensialitet, integritet og kvalitet</li> <li>• Faktaark 7 – Risikovurdering</li> <li>• Faktaark 10 – Bruk av databehandler</li> <li>• Faktaark 24 - Kommunikasjon over åpne nett</li> <li>• Faktaark 26 - Sikring av trådløs teknologi</li> <li>• Faktaark 49 - Krav ved bruk av PKI ved ekstern kommunikasjon</li> <li>• Datatilsynets veileder om databehandleravtaler etter personopplysningsloven og helseregisterloven: <a href="http://datatilsynet.no/templates/article_2742.aspx">http://datatilsynet.no/templates/article_2742.aspx</a></li> </ul>		

### Definisjoner

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

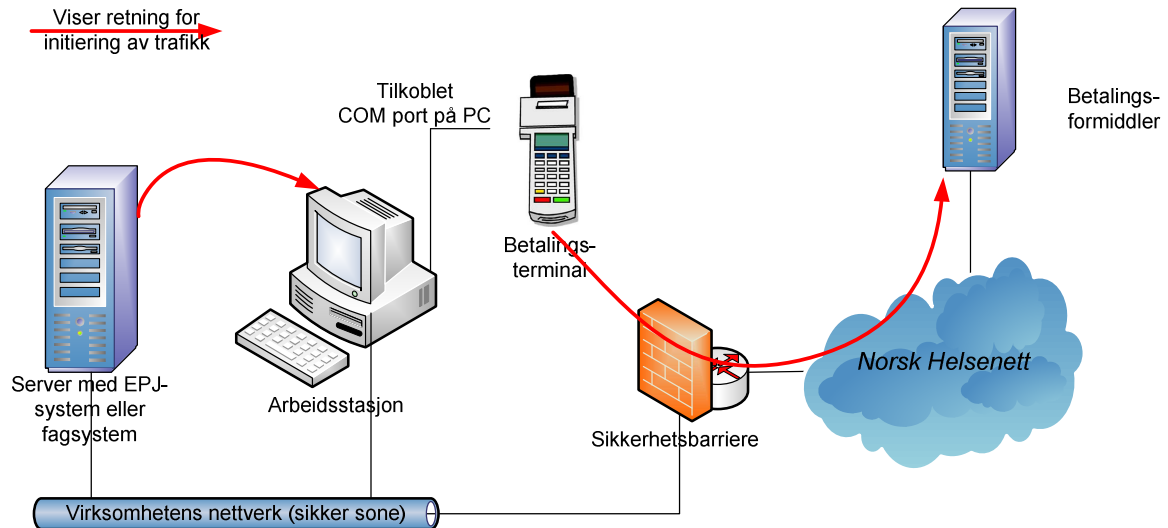
Med ”**betalingsformidler**” menes en leverandør av betalingsformidlingstjenester som betalingsterminalen kommuniserer med.

Nr.	Handling
1.	<b>Fastsette bruk av betalingsterminal</b> <ol style="list-style-type: none"> <li>a) Virksomhetenes ledelse skal beslutte bruk av betalingsterminal som er integrert mot et EPJ-system eller fagsystem</li> <li>b) Det skal etableres prosedyrer for bruk av betalingsterminal</li> <li>c) Konfigurasjonskart skal oppdateres med løsning for betalingsterminal</li> <li>d) Det skal inngås en databehandleravtale med leverandør av betalingsterminalløsning. Databehandleravtalen kan inngå som en del av de andre avtalene mellom partene</li> </ol>
2.	<b>Risikovurdering</b> <ol style="list-style-type: none"> <li>a) Før etablering av løsning for betalingsterminal skal virksomheten gjennomføre en risikovurdering av løsningen</li> <li>b) Eksempler på senarioer som bør vurderes: <ul style="list-style-type: none"> <li>○ Det initieres trafikk fra Internett til betalingsterminal med fare for å kompromittere helse- og personopplysninger i EPJ-systemet, fagsystemet og nettverket</li> <li>○ Det initieres trafikk fra ISDN, analog telefonlinje eller mobilbasert</li> </ul> </li> </ol>

Nr.	Handling
	<p>kommunikasjon til betalingsterminal og betalingsformidler med fare for å kompromittere helse- og personopplysninger i EPJ-systemet, fagsystemet og nettverket</p> <ul style="list-style-type: none"> <li>○ 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</li> <li>○ Det overføres fødselsnummer og / eller helse- og personopplysninger til betalingsterminal med fare uautorisert tilgang og / eller utlevering av fødselsnumre og helse- og personopplysninger</li> <li>○ At virksomhetens nettverk med EPJ-system og betalingsterminal ikke er sikret med minst to uavhengige tekniske virkemidler fra eksterne nett (betalingsformidler)</li> <li>○ 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</li> </ul> <p>c) Virksomheten kan dokumentere risikovurderingen ved at:</p> <ul style="list-style-type: none"> <li>○ Virksomheten gjennomfører risikovurderingen i samarbeid med leverandør av betalingsterminal som utdyper risikovurderingen med sine tekniske spesifikasjoner</li> <li>○ EPJ-leverandør eller leverandør av fagsystemet risikovurderer og dokumenterer sin integrasjon mot den aktuelle betalingsterminalen</li> </ul>
3.	<p><b>Prinsipper for teknisk løsning i nettverket</b></p> <ul style="list-style-type: none"> <li>a) Løsning for betalingsterminal og eksterne nettverk skal sikres med to uavhengige tekniske virkemidler (sikkerhetsbarrierer)</li> <li>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</li> <li>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)</li> </ul>
4.	<p><b>Prinsipper for integrasjon mot EPJ- eller fagsystem</b></p> <ul style="list-style-type: none"> <li>a) Betalingsterminalen skal konfigureres slik at denne ikke kan initiere trafikk til EPJ-systemet / fagsystemet</li> <li>b) EPJ-systemet / fagsystemet initierer forbindelse til betalingsterminalen og overfører beløpet samt innhenter eventuell kvittering for transaksjonen</li> <li>c) Følgende opplysninger skal ikke overføres til betalingsterminalen: navn, fødselsnummer og helseopplysninger</li> </ul>
5.	<p><b>Prosedyrer</b></p> <ul style="list-style-type: none"> <li>a) Prosedyrer for bruk av løsning for betalingsterminal bør minst inneholde: <ul style="list-style-type: none"> <li>○ Beskrivelse av korrekt implementering iht. sikkerhetskrav</li> <li>○ Krav til gjennomføring av risikovurdering</li> <li>○ Krav til integrasjon med EPJ-system / fagsystem</li> <li>○ Prosedyre for bruk av løsningen</li> </ul> </li> </ul>

### 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.

