



BANKENES
STANDARDISERINGSKONTOR



Årsrapport 2014

Risiko, prioriteringer og aktiviteter



BSKs formål er å ivareta forvaltningsoppgaver knyttet til betalings- og informasjonsformidling i bankenes felles infrastruktur.

Om BSK

Bankenes Standardiseringskontor (BSK) ble etablert av Bankforeningens Servicekontor og Sparebanksforeningens Servicekontor høsten 1994 med formål å ivareta forvaltningsoppgaver knyttet til betalings- og informasjonsformidling i bankenes felles infrastruktur. Arbeidet omfatter blant annet fastsetting og oppfølging av krav og standarder for samordning av betalingssystemene, IT-sikkerhet, formater for transaksjons- og informasjonsutveksling mellom banker og mellom felles operative selskaper og banker.

BSK har et styre som pekes ut av Finans Norge bestående av følgende representanter:

- Eldar Skjetne, styrets leder Sparebank1 Alliansen
- Peer Theien, DNB
- Lorang Eriksen, Eika Alliansen
- Kristian Maubach, Sparebanken Vest
- Gunnar Senum, Skandiabanken
- Per Harald Fredriksen, NORDEA

- Bernt Ragnar Pettersen, Danske Bank
- Solveig Lie, Handelsbanken
- Einar Arne Engedahl, Storebrand

I tillegg møter Tor Johan Bjerkedal fra Finans Norge fast som observatør i møtene.

BSK består per i dag av 9 medarbeidere og vi har knyttet til oss kompetanse fra bankene og sentrale leverandører organisert i faggrupper for:

- Kortbetaling
- Nettbanksikkerhet
- Interbank
- Elektronisk regningsbetaling
- BankID

Det er per i dag anslagsvis 40 fagpersoner fast tilknyttet BSK gjennom faggruppene. BSK organiserer også prosjekter og arbeidsgrupper hvor ytterlig andre fagpersoner fra banker og leverandører involveres. Dette gir BSK et stort og kompetent nettverk som vi benytter når vi skal løse oppgaver.

Denne rapporten er laget for å gi bankene en oversikt og innsikt i saker som det jobbes med i vår regi.

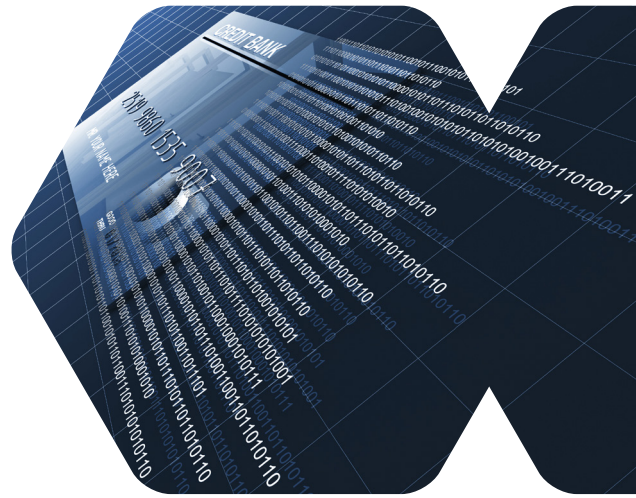
Prioriteringer

Styrets hovedprioriteringer for BSK er:

- Modernisering og videreutvikling av felles infrastrukturer, systemer og løsninger
- Internasjonalisering av virksomheten når det gjelder standardvalg og samarbeidskonstellasjoner
- Videreutvikling av prosesser og kompetanse

Styrets hovedprioriteringer er forankret i en klar overordnet strategi og detaljert i aktiviteter. Prosessen med å definere aktiviteter er styrt av BSKs administrasjon, i et godt samspill med etablerte faggrupper, Finans Norge og dialog med sentrale leverandører. Aktivitetene er også forankret gjennom vedtak i BSK styret ifm budsjettbehandlingen.

2014 - Et år preget av endringer



2014 har vært preget av store endringer som har påvirket BSK og som vil fortsette å ha stor påvirkning på oss og vårt arbeid i årene som kommer.

Bankene har i løpet av 2014 etablert produkselskapene BankID Norge AS og BankAxept AS. BSK skal fortsatt ha ansvaret for kravstilling og oppfølging på sikkerhets- og standardiseringsområdet også for produkter tilbudt gjennom produkselskapene. Samspillet mellom BSK og produkselskapene er avtalerregulert. Vi er opptatt av å videreføre og etablere et tett og godt samarbeid med produkselskapene, for på den måten bidra til selskaperens suksess. Dette blir også viktig for oss i 2015 og årene som kommer. Konkret har vi jobbet tett med BankID ifm gjennomføring av BankID 2.0 prosjektet (for å gjøre bankID java-fri) og med BankAxept er vi nå tett involvert ifm deres prosjekt for å få på plass løsning for kontaktløse kort. I etableringsperioden for BankAxept har vi også vært samlokalisert. I tillegg har vi feiret FinansCERTs ett års dag 1. oktober 2014. FinansCERT spiller en viktig rolle i arbeidet med koordinering av

håndtering av sikkerhetshendelser på tvers av norske banker og livselskap. Det er tett sammenheng mellom FinansCERT sitt arbeid og BSK sin standardiseringsvirksomhet på sikkerhetsområdet. FinansCERT er samlokalisert med BSK.

“

2014 har vært et brytningsår for nye måter å betale på.

Det har videre skjedd store endringer på leverandørsiden hvor spesielt salget og omorganisering av Nets har vært sentralt. Slike prosesser utløser også behov for oss å vurdere samspill og organisering. Vi har også blitt mer kjent med SDC gjennom året som følge av at de har fått nye kunder og engasjert seg sterkere inn i den norske infrastrukturen. Det pågår også prosess for salg av EVRY.

Reguleringen av betalings- og sikkerhetsområdet er i endring. Det viktigste for vår virksomhet har vært den pågående diskusjonen i EU om ny betalingsregulering, herunder Payment Service Directive 2 (PSD2). Fokuset for vår del har vært på myndighetenes ønske om å pålegge bankene å åpne infrastrukturen (tilgang til konto) for tredjepartsbetalingstjenestetilbydere (TPP'er). Utfordringene er hvordan dette kan gjøres på en trygg måte, og uten at bankenes sikkerhet blir forringet. Bankene gis ikke anledning til å avtalefeste sikkerhetskrav til de som skal få tilgang, samtidig sitter bankene med ansvar ovenfor kundene av TPP'ene når det gjelder misbruk og svindel. Vi følger opp dette sammen med Finans Norge og via deltakelse i European Payment Council, Pan Nordic Card Association og direkte ovenfor myndighetene.

I tillegg har 2014 virkelig vært et brytningsår for nye måter å betale på og alt tilsier at 2015 blir enda mer spennende og forhåpentligvis et år hvor de nye betalingsløsningene også oppnår økt praktisk utbredelse.



Sentrale aktiviteter i 2014

Moderniseringsprosjektet

Styret i BSK vedtok 20.06.2013 Moderniseringsprosjektet for å erstatte BALTUS og BDM som er infrastrukturen for on-line meldingsutveksling mellom bankene. Prosjektet ble iverksatt som følge av en erkjennelse av at den etablerte infrastrukturen var foreldet (dog fortsatt meget driftssikker). Prosjektet, som nå skal realisere Baltus 2.0, er definert med en endelig milepæl 31/12-15 hvor all trafikk skal være lagt over på ny infrastruktur og BSK har avsluttet forvaltning av den gamle. Målsettingen med arbeidet er å etablere en mer fleksibel og enda sikrere infrastruktur for online meldingsutveksling mellom bankene, tilrettelegge for nye tjenester/løsninger og åpne for nye aktører (leverandører og samarbeidspartnere). Løsningsdesignet vil også gi bankene, ved Finans Norge, bedre muligheter til å kontrollere trafikken i nettverket gjennom kontroll på den sentrale ruting tabellen (Central Routing Table CRT). Baltus 2.0 kravene utviklet av BSK er forankret i et nytt Baltus regelverk fra Finans Norge, vedtatt i Bransjestyret Betalingsinfrastruktur (BBI). Prosjektet og løsning er i god prosess, vedlagt denne årsrapporten er et white paper som beskriver Baltus 2.0. Spesielt interesserte kan også ta kontakt med BSK for mer informasjon.

ISO 20022

Styret i BSK vedtok 12.03.2014 et veikart for overgang til ISO 20022 som meldingsformat i den norske infrastrukturen. Dette som erstatning for dagens kunde-bank formater (Telepay, PAYMUL, CREMUL) og bankinterne formater (NIBE, BOLS, NISOK). ISO 20022 har vunnet stadig mer terreng i internasjonal meldingsformidling på betalings- (finans-)området. Standarden er også støttet av EU og forankret i deres meldingsregelverk for Euro-



Styret i BSK vedtok et veikart for overgang til ISO 20022 som meldingsformat i den norske infrastrukturen.

betalinger (SEPA). Målsettingen med overgangen er å gi økt mulighet til samordning mellom betalinger i norske kroner og andre valutaer for på den måten tilrettelegge for kostnadseffektivisering, økt konkurranse i leverandørmarkedet, enklere forvaltning og større kompetansetilfang.

Nytt kortdesign

BSK har jobbet med å utforme nytt kortdesign for debetkortene. Arbeidet er gjennomført i tett samarbeid med bankene og målsettingen har vært å øke sikkerheten i kortet, samt å gi det et mer moderne uttrykk. Hele kortets bakside er nå designet på en helhetlig måte og det er satt inn en rekke sikkerhetslementer for å gjøre kortet vanskelig å forfalske og kopiere. De nye kortene er planlagt lansert og slik at bankene kan starte fornying 1. januar 2014.

TIFI-prosjektet

Tredjeparters tilgang til bankenes felles infrastruktur (TIFI-prosjektet) ble etablert som følge av en prosess i BSK styret hvor styret utfordret administrasjonen til å utrede hvordan man kunne se for seg å gi tredjeparter tilgang til bankenes felles infrastruktur på en sikker og kontrollert måte. Det er ikke prosjektets mandat å vurdere om en slik tilgang skal tillates, en slik vurdering er næringspolitisk og vil måtte gjøres i regi av Finans Norge og BBI. TIFI-prosjektet ble etablert uavhengig av «signaler» fra PSD2 prosessen og for å utrede hvordan bankene kan innrette seg dersom nye aktører skal tilbys (avtalefestet og på kommersielle vilkår) å få tilgang



til infrastrukturen. Tilrettelegging for denne type tilgang var også en av føringene fra styret i Baltus 2.0 mandatet, men når Baltus 2.0 fokuserer på meldingsnettverket/infrastrukturen, så fokuserer TIFI prosjektet mer på kravene som skal stilles til aktørenes sikkerhetsarbeid. TIFI arbeidet har også vist seg nyttig for å modne tankene om hvordan vi bør innrette oss til sikkerhetsspørsmålet når det i PSD2 sannsynligvis vil bli pålagt bankene å åpne kontotilgang for tredjepartsbetalingstjenestetilbydere (TPP'er).

Øvrige sentrale aktiviteter

BSK har også realisert en del andre sentrale endringer i løpet av året. Vi har blant annet tilrettelagt for å inkludere mer informasjon om brukersted i kapitaltransaksjonen som følger kortbetalinger gjennom å utvide BOLS formatet (LK27). Dette skal gjøre det enklere å synliggjøre mer informasjon om transaksjonen på kundens kontooversikt i nett-/mobilbank.

Sammen med BankID Norge har BSK satt i gang en forstudie for å teste ut muligheter for å lage en selvbetjeningsløsning for bildefornyelse på bankkort. Hypotesen er at man kan ta et bilde av seg selv (selfie), signere denne med BankID vha mobilen. Bildet sendes deretter inn til bankens leverandør av kortsystem

som gjennomfører en sammenligning av gammel og nytt bilde vha ansikts-gjenkjenningsteknologi. Dersom testen konkluderer positivt, fornyes bildet som så kan benyttes ved neste gang utstedelse av kort. Uttestingen av dette har blant annet omfattet vurdering av juridiske aspekter.

BSK har sammen med BankID Norge og Finans Norge gjennomført en utvidet risiko- og tiltaksvurdering av identitetskontroll ifm utstedelse av ny BankID. Det har vært et særskilt fokus på kvaliteten i Postens PUM-tjeneste. Arbeidet er rapportert og forankret i BSK styret og BBI og det vil bli gjennomført en serie aktiviteter rettet inn mot å sikre at BankID fortsatt kan utstedes med et absolutt minimum av uønskete hendelser.

BSK har bidratt aktivt i realisering av et java-fritt BankID alternativ, BankID 2.0 prosjektet. Vår rolle har vært å fastsette sikkerhetskrav, samt å godkjenne løsning før driftssetting. Prosjektet har vært spennende og krevende og vi er stolt over at BankID Norge har lyktes med å lansere nyvinningen BankID 2.0. BSK bidrar videre til BankAxepts arbeid med å utvikle løsning for å tilrettelegge for kontaktløs betaling. Vår rolle har vært å fastsette sikkerhetskrav, samt å godkjenne løsning før driftssetting. Prosjektet er spennende og krevende og vi er stolt over å bidra i denne viktige prosessen.

“

BSK har bidratt aktivt i realisering av et java-fritt BankID alternativ – BankID 2.0 prosjektet.

BSK har deltatt med kravsetting og standardisering i Kontoadresseringsprosjektet (KAR) og i Straksbetalingsprosjektet begge svært viktige prosjekter for utviklingen av bankenes infrastruktur hvor spesielt KAR vil tilrettelegge for å lage kobling mellom mobiltelefonnummer og bankkonto noe som forenkler utrusting av løsninger for mobilbetaling.

Internasjonalt arbeid

BSK representerer bankene i en rekke sammenhenger og på ulike arenaer. Vår rolle er å ivareta norsk bankers interesser. Vi blir stadig mer påvirket av internasjonale initiativer på betalingsområdet, herunder økt reguleringstrykk, men også som følge av at vi har vedtatt å ta i bruk internasjonale standarder (eks ISO



Vår målsetting med dette er å bidra til å løfte sikkerhetsnivået generelt i samfunnet for å redusere bankenes sårbarhet samt å sikre at gode løsninger kan gjenbrukes.



20022) mer målrettet. I løpet av 2014 har vi derfor styrket vårt fokus på deltakelse på den internasjonale arenaen blant annet gjennom etablering av rolle som fagsjef.

I februar 2014 inngikk vi en samarbeidsavtale med Standard Norge om etablering av betalingsområdet som særskilt fokus i Standard Norge. Dette ble gjennomført i tett samarbeid med SWIFT NNG som allerede hadde tatt initiativ til dette. Det ble etablert arbeidsgrupper innen betalings- og sikkerhetsområdet og en overordnet speilkomite. Vår målsettingen med gjennomføring av disse aktivitetene er å ha gode påvirkningsmuligheter på videreutviklingen av relevante standarder for oss, samt å få tilgang til bredere kompetansenettverk nasjonalt og internasjonalt. Som følge av dette har vi også deltatt i relevante internasjonale komiteer: ISO (betalingsområdet), CEN (efaktura) og ETSI (PKI).

I september tok Finans Norge, BankID Norge, FinansCERT og BSK et initiativ overfor Standard Norge for å se om det var mulig å etablere

en tverrsektoriell løsning for standardisering innen IT-sikkerhets- og personvernområdet i Norge for på denne måten å utnytte knappe ressurser mer optimalt. BSKs daglige leder er medlem av sektorstyret IKT i Standard Norge og ansvarlig for å følge opp dette i en oppstartsfase. Utfallet er i skrivende stund usikkert, men det skal nå gjennomføres aktiviteter for å få på plass finansiering og organisere arbeidet. Vår målsetting med dette er å bidra til å løfte sikkerhetsnivået generelt i samfunnet noe som er viktig for å redusere også bankenes sårbarhet, samt å sikre at gode løsninger kan gjenbrukes.

BSK er medlem i Pan Nordic Card Association (PNC) på vegne av norske banker. PNC er et nordisk kompetansenettverk som også har fokus på samordning av sikkerhetsregelverk og standarder på kortområdet i Norden. PNC representerer videre medlemmene i internasjonale fora, herunder EMVco og PCI.

European Payments Council (EPC) er etablert av den europeiske bank-

sektoren for å bidra til å koordinere og samordne næringen innen betalingsområdet og for å støtte opp under EUs SEPA ambisjoner. DNB har tegnet medlemskap i EPC på vegne av norsk banksektor, mens BSK dekker kostnader relatert til dette på vegne av fellesskapet. Det er flere medarbeidere fra Finans Norge, BSK og DNB som deltar i de ulike arbeidsgruppene i EPC. Aktivitetene er samordnet og koordinert gjennom Fagutvalget for Internasjonale rammebetingelser for Betalingsområdet (FIB). Dette gir oss blant annet nettverk inn mot viktige beslutninger som skjer i EU, samt premisslegging i regi av den europeiske sentralbanken (ECB) og det europeiske finanstillstyret (EBA).

I tillegg til organisasjonene og aktivitetene beskrevet over, deltar BSK i en rekke andre kompetansefora. Spesielt interesserte kan få en fullstendig oversikt og gjennomgang av dette. Dersom noen ønsker å delta og bidra i arbeidet og/eller foraene omtalt over, så er det også mulig å få til dette.



Risikovurdering

BSK sin virksomhet skal rettes inn mot å bidra til å styre risiko slik at den er på et akseptabelt nivå. BSK gjennomfører derfor årlig en vurdering av risiko på ulike nivå; strategisk, taktisk og operasjonelt. Vurderingen er en omfattende og grundig prosess, dokumentert i detalj i egen rapport. Nedenfor følger en oppsummering av risiko som BSK har lagt til grunn ifm vårt planarbeid. **MERK:** nedenfor omtales ikke vurderinger som har lagt til grunn for iverksetting av tiltak i 2013 og 2014 (eks Baltus 2.0), men kun risikoer som trigger nye tiltak og vurderinger. Spesielt interesserte kan ta kontakt for å få mer informasjon, men selve den underliggende rapporten er ikke for bred distribusjon innen næringen.

Strategisk risiko

Vi oppfatter at det er flere strømmer som vil påvirke vårt strategiske risikobilde i 2015:

SELVREGULERING

Endring i regulering og selvreguleringsrommet. Dette gjelder spesielt forholdet til tredjeparter omtalt andre steder i denne rapporten, men kan også bli relevant for andre

områder. Når det gjelder håndtering av dette, så er det spesielt viktig at næringen jobber målrettet for å følge opp myndighetene. Arbeidet er i god prosess i regi av Finans Norge og BSK vil kunne bidra inn med våre synspunkter gjennom denne kanalen.

TILGANG FOR TREDJEPARTER

Tredjeparter som skal/bør få tilgang til bankenes felles infrastruktur er et spørsmål om både trusler og muligheter. Trusler pga sikkerhetsrisikoen dette kan medføre, samt utfordringer for bankenes styringsrett over egen infrastruktur. Mulighetene ligger i å få bredere samarbeidsflate for bankene og større tilgang på innovasjonskraft. Vurdering av om bankene skal gjøre dette er en næringspolitisk sak som ligger hos Finans Norge. Dersom konklusjonen er at man skal åpne for dette (og evt. PSD2 medfører at man må), så vil BSK måtte utforme regelverk, etablere sertifiseringsordninger mv slik at bankenes ikke blir påført uakseptabel risiko. BSK følger opp dette gjennom TIFI og BALTUS 2.0 prosjektet omtalt over, mens diskusjonen om tredjeparter også foregår i regi av Finans Norge i BBI.

LEVERANDØRER

Endringer i leverandørbildet vil også kunne gi oss et endret risikobilde. Nets sin reise i retning økt kommersialisering er ytterligere forsterket som følge av endringer på eiersiden. Dette har også gitt seg utslag i organisatoriske endringer innført fra september 2014. BSK vil ha tett kontakt med Nets for å sikre at vi fortsatt har tilgang på god kompetanse og lik forståelse av næringens sikkerhetsbehov. Det er også tett kontakt med Nets i regi av Finans Norge, BankID Norge og BankAxept.

KOMPETANSE

Tilgang på kompetanse om norsk infrastruktur er kritisk for å kunne forvalte og videreutvikle eksisterende løsninger, samt for å kunne utvikle nye. I en periode med omorganisering og nedbemanning kombinert med endringer i løsninger er det avgjørende at det gjøres tiltak for å sikre kompetanse. BSK har iverksatt tiltak både for å bevare tilgang på kompetanse på eksisterende løsninger, samt å sikre at løsninger er i samsvar med internasjonale standarder, i tillegg har vi ved utvikling av nye kravsett og standarder (eks. Baltus 2.0 og



Vi oppfatter at den norske infrastrukturen er grunnleggende sikker og godt forvaltet.

ISO 20022) dokumentert dette på engelsk.

Taktisk risiko

Vi vil ha særskilt fokus på følgende taktiske risikoer:

APT

Godt forberedte angrep på sentral infrastruktur Advanced Persistent Threat (APT) og på tvers av verdikjeder, er vanskelig å beskytte seg mot fordi det krever en bredde i kompetanse og at sikkerhetstiltak iverksettes på tvers av organisasjoner. Samtidig er det viktig at denne type risiko adresseres aktivt og BSK har derfor satt dette på agendaen for 2015. APT har også utløst behovet for etablering av et sikkerhetslederforum bestående av IT-sikkerhetsledere fra bankene og sentrale leverandører. Vi ser for oss at vi skal etablere et sikkerhetsprogram for målrettet å kunne følge opp dette området over tid. Risikoen kan videre oppstå på tvers av sektorer, noe som også har vært en del av vurderingen vi gjorde som medførte at vi tok initiativ ovenfor Standard Norge om at de burde sette dette på agendaen, jfr omtale over.

KVALITETSSIKRING

Kvalitetssikring av løsninger og leverandører for å sikre at disse er

i samsvar med BSKs krav og standarder er viktig for oss, spesielt i en verden med store endringer og hvor svært mange av angrepene er rettet inn mot å utnytte kjente sårbarheter. BSK vil derfor iverksette aktiviteter for å øke fokuset på sertifisering og kvalitetssikring i 2015.

Operasjonell risiko

Vi overvåker og følger opp en rekke operasjonelle risikoer som ledd i vår forvaltning av de norske løsningene. Vi oppfatter at den norske infrastrukturen er grunnleggende sikker og godt forvaltet. Samtidig er det alltid noen risikoer vi overvåker mer aktivt enn andre i ulike perioder. Hvilke dette er avhenger av diskusjoner vi har i faggruppene, hendelser og trusler i markedet mv. For 2015 oppfatter vi at noen av de mest sentrale operasjonelle risikoene vil være:

SOCIAL ENGINEERING

Social engineering, dvs hvor kjeltringer forsøker å lure bankens kunder til å gi fra seg hemmeligheter som koder og lignende og/eller laste inn virus, er en trussel som stadig er like aktuell. Dette er en krevende trussel å adressere pga det krever bygging av sikkerhetskompetanse bredt i det norske samfunnet uten at man skal skape unødven-

dig utrygghet. BSK har adressert dette gjennom å bygge allianser og gjennom informasjonstiltak. Vi har vært og kommer til å være platinum sponsor for Sikkerhetsmåned som arrangeres av NORSIS, vi har tatt initiativ til tverrsektorielt samarbeid på sikkerhetsområdet ovenfor Standard Norge for å bidra til å øke sikkerhetsfokuset i andre sektorer, vi har kontakt med sårbarhetsutvalget for å få dette på agendaen mv. I tillegg driver bankene omfattende informasjonskampanjer ovenfor sine kunder.

LEGITIMASJONSKONTROLL

Legitimasjonskontroll ved utstedelse av elektronisk ID er omtalt ovenfor. Vi kommer til å følge opp tiltaksplanen som er satt opp som følge av risiko- og tiltaksvurderingen som er gjennomført høsten 2014 i 2015.

FORFALSKNING

Forfalskning av bankkort med bilde er en risiko som er adressert gjennom etablering av nytt kortdesign, samt uttesting av teknologi for selvbetjent bildefornyelse omtalt over. I 2015 vil det fortsatt være kort som ikke er byttet ut og vi vil følge med på om det er endringer i utviklingen når det gjelder omfang av forfalskninger. Dersom dette inntreffer vil vi kunne iverksette tiltak for å adressere dette.

Aktiviteter 2015

BSK styret prioriterer årlig aktiviteter som skal gjennomføres i BSK regi. Aktivitetene prioriteres i en A, B og C liste hvor A-listen inneholder aktiviteter som skal gjennomføres i løpet av året, B-listen aktiviteter som bør gjennomføres og C-listen aktiviteter som kan gjennomføres i løpet av året. Årets A-liste omfatter følgende:

| AKTIVITET | UTDYPING |
|--|--|
| Moderniseringsprosjektet | Realisering av Baltus 2.0 (sluttført innen 31/12-15) |
| BAX Kontaktsløse kort | Krav, realisering (inkl nøkkelsenter) |
| ISO 20022 | Kunde/bank realisering og Bank/bank planlegging |
| Knytning TSM | Standardiseringskrav til bankenes grensesnitt mot Trusted Service Manager (eks TSM Nordic) |
| Efaktura B2B, B2C og CEN | Oppfølging og kravsetting |
| Etablering av forsterket kontrollregime | Analyse, krav og utrulling, inkl terminalregister mv. Fokus på å styrke gatekeeperrollen |
| BankID 2.1 | Krav og godkjenning |
| Advanced Persistent Threat | Analyse, plan og tiltak relatert til godt planlagte angrep mot bankenes infrastruktur |
| Kontoadresserings-register (KAR) | Realisering |
| Virksomhetsstyring BSK | Drift av BSK, faggrupper og deltakelse i enkelte fora, eks styret i PNC, NS mv |

Kontakt



Lars Erik Fjørtoft,
daglig leder



lars.erik.fjortoft@bsk.no



974 74 469

