ØKONOMISTYRELSEN

Løsningsarkitektur for betalingsafledende systemer

Marts 2021

2021

Indhold

1. Indledning **4**
1.1 Baggrund og formål 4
1.2 Læsevejledning 5
1.3 Begreber 6

2. Minimumskrav til løsningsarkitektur **11**

3. Lovkrav **12**
3.1 Overholdelse af gældende regnskabsrelateret lovgivning 12
3.2 Overholdelse af gældende GDPR-lovgivning 15

4. Systemkrav **19**
4.1 Restriktiv adgangsstyring 19
4.2 Pålidelig backup og genskabelse 21
4.3 Sikring af adgang til kildekode 22
4.4 Sammenhængende systemdokumentation 25
4.5 Robust RPA implementering 26

5. Applikationskrav **29**
5.1 Påkrævet logning 29
5.2 Tydeligt transaktionsspor 31
5.3 Datakonsistens og låsning 33
5.4 Ingen undtagelser fra produktstrategien 34
5.5 Tvungen funktionsadskillelse 35
5.6 End-to-end udbetalingskontrol 37
5.7 Sikker udbetaling via NemKonto 39

6. Tekniske krav **42**
6.1 Overholdelse af de tekniske minimumskrav, jf. SikkerDigital.dk 42
6.2 Kryptering af betalingsdata ved udveksling 43
6.3 Blokering for SQL-injektion 45

Sikker finansiel kontrol baseret på korrekt løsningsdesign

1. Indledning

Sikkerheden for effektive finansielle kontroller forudsætter at de understøttende systemer opfylder særlige krav til løsningsdesign, funktionalitet og teknisk implementering

1.1 Baggrund og formål

Baggrunden for udarbejdelse af minimumskrav til løsningsarkitektur for systemer, der afleder udbetalinger er, at der i 2018 og 2019 blev konstateret et stigende antal sager hvor statslige medarbejdere, enten alene eller i samarbejde med leverandøren, har svindlet for egen vindings skyld. Dette har været muligt grundet et eller flere af følgende forhold:

A. Manglende manuelle og automatiserede systemkontroller
B. Fraværende ledelsesmæssig bevågenhed
C. Udebleven opfølgning på tidligere revisionsanmærkninger

Formålet med de anførte minimumskrav til løsningsarkitektur er, i denne sammenhæng, alene at reducere finansielt svig via etablering og vedligeholdelse af en robust løsningsarkitektur, der sikrer at de nødvendige kontroller og logninger kan udføres, og dermed at adressere punkt A. Kravene vil primært gøre sig gældende ved videreudvikling af eksisterende systemer, eller ved anskaffelse af nye systemer.

Minimumskravene vil forventeligt finde anvendelse ved IT-revision af betalingsafledende systemer og bør endvidere danne udgangspunkt for dialog mellem myndighed og leverandør om nye og eksisterende systemer.

Afgrænsning
I forbindelse med opbygning og vedligeholdelse af en løsningsarkitektur, må sikkerhed nødvendigvis altid rangere højere end effektivitet, såfremt der ikke kan garanteres en samtidig høj sikkerhed og effektivitet. Dette afspejles i minimumskravene.

Der beskrives alene minimumskrav for systemer, der afleder udbetalinger, enten direkte eller ved understøttelse af en eller flere delprocesser, der sikrer, at der effektueres en udbetaling fra et andet system længere fremme i den samlede udbetalingsproces.

Bemærk at Excel ikke betragtes som et system i vedlagte, og at det direkte frarådes at anvende Excel undervejs i en proces, der afleder udbetalinger, da sikkerheden i Excel er begrænset. Dette gælder både indholdsmæssige editeringer og filopbevaring.

Løsningsdesignet bag officielle anerkendte udbetalingsløsninger som NemKonto og evt. netbank løsninger beskrives ikke i nærværende, da denne type af løsninger er underlagt et andet- og langt mere udvidet - sæt af arkitekturkrav og finansielt afledte restriktioner. I tilfælde af integration med pengeinstitut eller NemKonto, følges de formater og protokoller, der er fastlagt ved NemKonto og pengeinstituttet. Integrationskonceptet for disse bankcentraler defineres således som sikre. Ved beskrivelse af integrationen med NemKonto og et pengeinstitut inkluderes alene SKB-konceptet, og dermed ikke OBS-konceptet.

Referenceimplementeringerne tager alene udgangspunkt i systemer, hvor systemejerskabet er forankret i Økonomistyrelsen.

Målgruppe
Beskrivelsen er målrettet IT- ansvarlige herunder Product Owners (PO) og applikationsmanagers og løsningsarkitekter for egne betalingsafledende systemer i alle statslige og selvejende institutioner. Vejledningen er ligeledes relevant for økonomichefer med ansvar for systemer, der indgår i betalingsprocessen. Her kan materialet anvendes som grundlag for dialog med de systemtekniske profiler, om hvilke behov for forretningsmæssig compliance, systemerne skal dække. Desuden vil implementering af de enkelte krav, kunne danne grundlag for beskrivelsen af it-anvendelsen i regnskabsinstruksen jf. §21 i bekendtgørelsen om statens regnskabsvæsen.

1.2 Læsevejledning

Hvert af de angivne minimumskrav kan læses isoleret fra de øvrige minimumskrav. Det er dog hensigtsmæssigt at orientere sig i samtlige minimumskrav forud for etablering af nyt, eller justering af eksisterende, betalingsafledende system. Det er her vigtigt at fremhæve, at kravene beskrevet her, netop kun er minimumskrav, og det derfor forsat er nødvendigt, for den enkelte systemansvarlige, at foretage en samlet vurdering af nyt eller justeret system.

Bemærk at de angivne referenceimplementeringer for de enkelte minimumskrav justeres ved væsentlige ændringer i Økonomistyrelsens egen systemportefølje på de områder, der omfatter udbetalinger. Derfor bør der altid sikres, at der arbejdes med nyeste udgave af dokumentet.

1.3 Begreber

I beskrivelsen af minimumskravene anvendes en række begreber. De væsentligste nøglebegreber er gengivet nedenfor i alfabetisk rækkefølge.

Betalingsafledende system
Et system, der afleder udbetalinger, enten direkte eller ved understøttelse af en eller flere delprocesser, herunder håndtering af stamdata, der sikrer, at der effektueres en udbetaling fra et andet system længere fremme i den samlede udbetalingsproces. Både IndFak og RejsUd er defineret som betalingsafledende system.

Betalingsoplysninger
Betalingsoplysninger er de informationer der entydigt fortæller afsenderbanken hvilken modtagerkonto pengene skal anvises til. Betalingsoplysninger kan være komplette, hvor: registreringsnummer, kontonummer, IBAN nummer, PBS kreditornummer, bankkode, BIC(SWIFT) eller banknummer indgår. Alternativt kan betalingsoplysninger være ukomplette og blot bestå af CPR-, CVR-, SE- eller P-nummer. Uanset betalingsoplysningernes karakter vil de betalingsoplysninger der fremgår af udbetalingsdata angive hvilken bankkonto udbetalingen skal foretages til.

Change Management
Styring af alle de processer der indgår fra der træffes beslutning, om at der er behov for en ændring, til ændringen ligger klar til frigivelse.

Fagsystem
Et selvstændigt system, med lokalt systemejerskab, og som kan fungere som betalingsafledende system.

Funktionsadskillelse
Centralt i udbetalingssystemer, og betalingsafledende systemer, er princippet om funktionsadskillelse, som betyder, at der på tværs af en udbetalingsproces er interne kontroller, der sikrer en personmæssig adskillelse (2 eller flere) mellem adgangen til at disponere, godkende, anvise og betale, såvel direkte som indirekte. Funktionsadskillelse bevirker at en person, inden for samme transaktion, ikke alene kan gennemføre alle handlinger i forbindelse med en forretningskritisk aktivitet.

GUID/UUID
GUID står for Globally Unique Identifier, eller også kaldet UUID (Universally Unique Identifier) og er 128 bit nummer, som kan anvendes til unikke referencer. En GUID dannes ud fra en særlig algoritme som sikrer meget stor usandsynlighed for at to GUID'er vil være ens på globalt niveau.

OBS
Kommuner og regioner bruger OBS, Offentlig betalingssystem, til afregning af beløb mellem staten og kommunen eller regionen. Det omfatter blandt andet indbetaling af A-skat, udbetaling af en række sociale ydelser til borgerne og refusioner eller bidrag i forbindelse med den kommunale udligningsordning og tilskud.

Kommuner og regioner kan anvende et andet pengeinstitut til øvrige ind- og udbetalinger. Men kontrakten med Danske Bank har afløftet udbudsforpligtelsen for kommuner og regioner, der derfor nu kan anvende OBS til alle betalinger.

Pengeinstitut
I minimumskravene anføres pengeinstitut som henvisning til den virksomhed, der er tildelt kontrakten om betalingsformidlingsydelser i staten, og derfor varetager alle betalinger fra statslige institutioner. Ved henvisninger til lovtekster kan pengeinstitut dog forstås som en ordinær bank, sparekasse eller andelskasse.

Privilegerede rettigheder
Privilegerede rettigheder beskrives typisk lidt forskelligt fra system til system, men i nærværende beskrivelse, gælder det at privilegeret adgang er givet ved en adgang, der giver brugeren default læse-, skrive-, redigere- og sletteadgang til samtlige eller særligt kritiske data i systemet samt adgang til at udføre alle eller særligt kritiske funktioner i systemet, samt mulighed for at give sig selv, eller andre privilegerede rettigheder til systemet[1].

Regnskabsmæssig registrering
I et udbetalingssystem vil den regnskabsmæssige registrering udgøres af det datasæt, der ligger til grund for udbetalingen.

Robotbruger
En robotbruger (eller bare "robot") skal ses som kombinationen af en Windows-konto og en virtuel maskine/computer (VDI[2]). Når der i dokumentet beskrives RPA teknologi og minimumskrav hertil, er det med udgangspunkt i UIPath platformen, der anvendes bredt i statslige institutioner. Statens IT understøtter denne platform med en service de kalder RIA[3] og det er med udgangspunkt i denne service, at minimumskravene for RPA er beskrevet. Når en robot skal ses som kombinationen af Windows-konto og virtuel computer, betyder det at de sikkerhedsforanstaltninger der bygges ind i systemer styret på brugerniveau, automatisk vil blive opretholdt. Det vil eksempelvis kræve to robotter hvis man skal opnå fuld automatisering af en funktionsadskilt proces.

---

[1] Kilde: Sikkerdigital.dk: Privilegerede rettigheder

[2] Virtual Desktop Instance. Begrebet anvendes ofte i forbindelse med RPA.
[3] Robot IT Arbejdsplads

SKB
Statsinstitutioner er forpligtede til at anvende Statens Koncern Betalinger (SKB-systemet), jf. § 11 stk. 2 i regnskabsbekendtgørelsen. SKB er et centralt betalingsformidlingskoncept, der understøttes af et privat pengeinstitut til håndtering af statens ind- og udbetalinger, og systemet kan kommunikere elektronisk med alle statsinstitutioner, uanset hvilket økonomisystem institutionerne anvender.

Se også: Økonomistyrelsens hjemmeside om Statens Koncern Betalinger

SSO
Single Sign-On er en session- og brugeradgangskontrol-service, der gør det muligt for brugere at anvende de samme loginoplysninger på tværs af flere uafhængige applikationer. SSO er relateret til begrebet FIM (Federated Identity Management), der omhandler kobling af en brugers elektroniske identitet og attributter imellem flere systemer. I en SSO løsning er en brugers autentificeringsticket eller -token anvendt imellem flere systemer eller sågar organisationer.

Fordele ved SSO er:

- En bruger skal huske færre password.
- Mere strømlinet loginproces.
- Formindsker risikoen for phishing.
- Reduceret support relateret til passwords.

Eksempler på kendte web-baserede SSO løsninger:

- NemLogin
- Google
- Facebook

Systemobjekt
En IT-løsning eller applikation består af flere forskellige systemobjekter. Et systemobjekt kan fx være givet ved: en tabel, et stykke kode, en rapport, et script en dll-komponent eller lignende.

Udbetalingsdata
Når betalingen effektueres i udbetalingssystemet, overgår processen til SKB som varetager den egentlige finansielle banktransaktion. Informationer om modtager, modtagers betalingsoplysninger, beløb, valuta, betalingsdato m.m. der oversendes til banken benævnes alle udbetalingsdata. Udbetalingsdata dannes ofte ud fra den regnskabsmæssige registrering, men er ikke nødvendigvis altid sammenfaldende.

Udbetalingsproces
Udbetalingsprocessen skal her forstås som de handlinger der udføres i et udbetalingssystem, i forbindelse med at starte en betalingstransaktion mellem udbetalingsbanken og modtagerbanken. Processen vil typisk indeholde følgende trin:

- Udsøgning af åbne kreditorposter til betaling
- Delvis godkendelse af betalingsforslag
- Endelig godkendelse af betalingsforslag
- Afsendelse af betalinger til banken
- Registrering/Bogføring af betalingen

Udbetalingsprocessen kan indeholde en række sekundære trin så som:

- Validering af betalingsoplysninger
- Ændring af betalingsoplysninger
- Afvisning/Sletning af betalingsforslag

Udbetalingssystem
Det system der har integrationen til banken eller NemKonto, og som effektuerer betalingen.

Økonomisystem
Et selvstændig system, der både fungerer som kreditorsystem, udbetalingssystem, og typisk ligeledes understøtter alle andre klassiske økonomiprocesser. Navision Stat er fx defineret som Økonomisystem.

Minimumskrav til løsningsarkitektur

2. Minimumskrav til løsningsarkitektur

Der stilles særlige krav til udbetalings- og betalingsafledende systemer, der understøtter processer, hvor igennem der kan effektueres en udbetaling. Dette afsnit beskriver den løsningsarkitektur, der som minimum forventes implementeret for sådanne systemer

De enkelte minimumskrav er beskrevet separat, og kan grupperes i 4 overordnede temaer:

3. Lovkrav

Minimumskravene klassificeret som lovkrav, kan henføres til gældende lovgivning og manglende implementering af disse, kan derfor have juridiske- og strafbare konsekvenser. Det er vigtigt at bemærke, at det til en hver tid er den aktuelle lovtekst der udgør kravene og ikke nødvendigvis teksten i de følgende minimumskrav

3.1 Overholdelse af gældende regnskabsrelateret lovgivning

Formål
Økonomisystemer, udbetalingssystemer eller betalingsafledende systemer, skal nødvendigvis – på samme måde som alle andre løsninger – overholde gældende og relevant lovgivning for de forretningsprocesser, som systemet understøtter.

Lovkravene danner grundlag for de øvrige minimumskrav, og ved at have robuste implementeringer af de system- og applikationsrelaterede samt tekniske krav, sikres overensstemmelse med de lovmæssige krav på området.

Generisk Implementering
Da ressortspecifik lovgivning kan have stor konsekvens for hvilke regelsæt, der er gældende for specifikke systemer, ejet af de enkelte styrelser og institutioner, er denne del ikke konkretiseret her.

Dog gøres opmærksom på Regnskabsbekendtgørelsens § 11, der forholder sig til påkrævet anvendelse af økonomi- og betalingssystemer, der stilles til rådighed af Økonomistyrelsen.

Der henvises til referenceimplementering for Navision Stat, hvor den underliggende lovgivning forventes at dække den basislovgivning, der ligeledes må være gældende for ressortspecifikke systemer suppleret af ressortspecifik lovgivning.

Referenceimplementering
For Navision Stat, der både sender udbetalinger via NemKonto til Danske Bank og direkte til Danske Bank, vedligeholdes løsningen under en overholdelse af nedenstående anført lovgivning med en angivelse af de afsnit, der har særlig betydning for udbetalinger, eller som anses for særlige kritiske i en generel kontekst.

Rigsrevisorloven
Bekendtgørelse af lov om revision af statens regnskaber mm.

- §10, 2: om, at Rigsrevisor skal have adgang til at udtale sig, inden en sådan myndighed i sit regnskabssystem eller sin forretningsgang iværksætter forandringer, der har betydning for revisionen.

Regnskabsbekendtgørelsen: Bekendtgørelse om statens regnskabsvæsen mv.
Bekendtgørelse om statens regnskabsvæsen mv.

- §21,2 om personmæssig adskillelse af medarbejdere, der arbejder med hhv.: systemudvikling, driftsafvikling og regnskabsmæssig registrering/betalingsforretninger
- §24 om personmæssig adskillelse mellem den regnskabsmæssig registrering og betalingen
- §25 om registreringens omfang
- §27 om etablering af transaktionsspor
- §28,2 om risikobaserede kontroller
- §29, om elektroniske overførelser til pengeinstitut
- §44, om opbevaring af regnskabsmateriale i mindst 5 år.
- §45, om opbevaring af regnskabsmateriale i Danmark (som udgangspunkt)
- §49,2 om indsættelse af likvide midler på konto i betalingssystem administreret af Økonomistyrelsen.

Momsloven: Lov om merværdiafgift
Bekendtgørelse af lov om merværdiafgift (momsloven)

- Kapitel 11:Betalingspligtige personer
- Kapitel 13: Regnskabsbestemmelser

Lov om offentlige betalinger
Bekendtgørelse af lov om offentlige betalinger mv.

Hele bekendtgørelsen om lov om offentlige betalinger via udbetaling til en angiven NemKonto følges. I det følgende er særligt §1,1 fremhævet.

- §1,1. Personer over 18 år, som i henhold til lov om Det Centrale Personregister er tildelt et personnummer, og som ikke er registreret som udrejst af Danmark, skal anvise en konto i et pengeinstitut (en »NemKonto«), hvortil offentlige myndigheder med frigørende virkning kan foretage udbetaling af pengebeløb. Det samme gælder personer under 18 år, der i henhold til lov om Det Centrale Personregister er tildelt et personnummer, og som modtager betalinger fra offentlige myndigheder.

NemKontoordningen
Bekendtgørelse om Nemkontoordningen

Om udbetaling til en given angivet NemKonto jf. Lov om offentlige udbetalinger via NemKonto-løsningen. Det samlede regelsæt er relevant.

Elektronisk afregning med offentlige myndigheder – indenrigs
Bekendtgørelse om elektronisk afregning med offentlige myndigheder

Eftersom udbetalinger udspringer af fakturering, og god systemunderstøttelse binder fakturering og udbetaling tæt sammen, er denne lovgivning ligeledes relevant. I det følgende fremhæves §2,1.

- §2,1 Offentlige myndigheder skal stille krav om, at betaling af elektroniske regninger sker således, at betalingen modtages elektronisk. Myndigheden skal med henblik herpå anvise en fremgangsmåde for betaling af regningen, f.eks. ved anvendelse af konto til konto-overførsel, et medfølgende elektronisk eller papirbaseret indbetalingskort eller tilmelding til et system til betaling med automatisk træk.

EU faktureringsdirektivet - europæisk
Bekendtgørelse om elektronisk fakturering i den fælleseuropæiske serviceorienterede infrastruktur

Eftersom udbetalinger udspringer af fakturering, og god systemunderstøttelse binder fakturering og udbetaling tæt sammen, er denne lovgivning ligeledes relevant. I det følgende fremhæves §4, stk. 1 og 2.

- § 4. Offentlige myndigheder skal kunne modtage elektroniske fakturaer, der opfylder kravene i den europæiske standard, som er beskrevet i bekendtgørelsens bilag 1.
- Stk. 2. Offentlige myndigheder skal være registrerede som modtagere i det fællesoffentlige NemHandelsRegister med profilerne fastlagt i bilag 1 og offentliggjort på Erhvervsstyrelsens hjemmeside, når den fælleseuropæiske serviceorienterede infrastruktur tages i brug for myndighedens vedkommende, jf. § 5, stk. 2, i lov om elektronisk fakturering ved offentlige udbud.

Generelle opmærksomhedspunkter

- Ved eventuel konflikt mellem ordlyden for angivet lovgivning, herunder fremhævede afsnit, og eventuel senere opdatering af tilsvarende lovgivning, skal der altid tages udgangspunkt i nyeste udgave af den relevante lovgivning.
- Implementering af ny lovgivning medtages ved opdatering af det samlede dokument, hvorved at det er muligt, at listen herover ikke er udtømmende beskrevet i perioden fra ny lovgivning træder i kraft til dokumentet opdateres.

3.2 Overholdelse af gældende GDPR-lovgivning

Formål
Som udgangspunkt skal en given applikation være kompatibelt med alt den lovgivning og samtlige interne politikker, der er relevante for de forretningsprocesser som applikationen helt eller delvist understøtter.

Persondataforordningen (GDPR) af 25. maj 2018, med fokus på de registreredes rettigheder (fysiske personer), kan imidlertid give helt særlige udfordringer ved applikationsudvikling og vedligehold for langt de fleste applikationer, og er derfor særskilt behandlet her.

For god ordens skyld gengives her et kortfattet overblik over de registreredes rettigheder jf. forordningen:

- Ret til indsigt, art. 15
- Ret til berigtigelse, art. 16
- Ret til sletning, art 17
- Ret til begrænsning, art 18
- Ret til underretning, art. 19
- Ret til dataportabilitet, 20
- Ret til indsigelse, art 21
- Ret til at modsætte sig automatiske afgørelse, art 22

Og derudover har den dataansvarlige *pligt* til at give oplysninger vedr. indsamling af persondata, art. 13 og 14, med mindre indsamlingen er omfattet af undtagelser fra oplysningspligten.

Indholdet i dette afsnit skal ses om en hjælp til opmærksomhedspunkter i lovgivningen, og det vil altid påhvile den systemansvarlige, at sikre overholdelse af gældende GDPR regler.

Generisk implementering
Forordningen definerer personoplysninger som følgende jf. artikel 4, nr. 1

Enhver form for information om en identificeret/identificerbar fysisk person. Hvis oplysningen kan anvendes til at identificere en fysisk person (modsat en juridisk person som fx et selskab) så er det en personoplysning.

- Man behøver ikke at kunne identificere en person alene vha. en enkelt personoplysning. Hvis der er en væsentlig sandsynlighed for, at en oplysning tilhører en bestemt person, så er det en personoplysning.

- Hvis oplysningen kan anvendes – evt. *sammen* med andre oplysninger - til at identificere en person, så vil det også være en personoplysning, fx en interesse/hobby.

- Bestemmelsen er *meget bred*; en IP-adresse vil også typisk være en personoplysning, fordi man i nogle tilfælde kan kontakte sin udbyder og bede om oplysning omkring hvilken person en bestemt IP-adresse tilhører.

Forordningen fastlægger følgende grundprincipper jf. art 5, stk. 1

Definitionen af persondata kombineret med de 6 grundprincipper betyder, at det ved både: anskaffelse, ny egen udvikling og videreudvikling skal sikres følgende:

- at der er hjemmel til at indsamle, behandle og opbevare persondata i applikationen
- at der alene sker en tilstrækkelig og nødvendig registrering af persondata i applikationen.
- at de opbevarede persondata er sikret i applikationen
- at det er muligt at udtrække data fra applikationen for en imødekommelse af indsigtsretten
- at persondata i applikationen kun deles med andre applikationer under relevant hjemmel
- at krav om sletning af persondata i applikationen skal imødekommes, med mindre data hjelmet for fortsat opbevaring, og iht. hjelmet tidsbegrænsning
- at data skal kunne porteres (overføres) fra applikationen, såfremt personen har ønske om at flytte sine data til anden applikation

Mere information hos Datatilsynet

Vejledning om de registreredes rettigheder
Datatilsynet (Juli 2018): Vejledning om de registreredes rettigheder

Behandlingssikkerhed – Databeskyttelse gennem design og standardindstillinger
Sikkerdigital.dk og Datatilsynet: Indbygget databeskyttelse (privacy by design)

Alle vejledninger
Datatilsynet: Vejledninger

Referenceimplementering
I forbindelse med tilretning af Navision Stat for sikring af en overholdelse af både den eksisterende Persondatalov og den nye EU persondataforordning pr. 25. maj 2018, blev der i marts 2016, identificeret følgende for enten videreførelse eller ændring af eksisterende funktionalitet (for implementering i august 2017):

1. Retten til at blive glemt, og dermed få slettet sine data, skal kunne efterkommes med mindre, at det er i strid med regnskabsbekendtgørelsens § 44 om opbevaring af regnskabsmateriale og borgerens egen interesse.
2. Retten til at få indsigt i alle persondata, der opbevares eller behandles af dataansvarlig/databehandler - stamdata såvel som transaktionsdata - skal understøttes.
3. Retten til at få udlæst alle sine persondata, for overførelse til andet system, såkaldt dataportabilitet skal understøttes.
4. Navision Stat indeholder, som økonomisystem, kun almindelige persondata og CPR-data, men ingen følsomme persondata. Det skal i den forbindelse sikres, at CPR-numre kan sløres ved udskrift, i de tilfælde en rapport risikerer at blive brugt til et formål, der ikke er foreneligt med § 1 i regnskabsbekendtgørelsen, hvor det står anført at:

   "Regnskabsvæsenet skal bidrage til en sikker og effektiv økonomiforvaltning på alle niveauer i statsforvaltningen herunder selvejeområdet, og skal i størst muligt omfang foregå digitalt med brug af færrest mulige ressourcer og størst mulig automatisering.

   Stk. 2. Gennem regnskabsvæsenet skal tilvejebringes de fornødne oplysninger til brug for den løbende interne regnskabsopfølgning, den periodiske regnskabsaflæggelse samt den årlige udfærdigelse af statsregnskabet. Endvidere skal regnskabsvæsenet bidrage til udarbejdelsen af årsrapporter.

   Stk. 3. Regnskabsvæsenet skal bidrage med oplysninger til revisionen af regnskaberne i henhold til gældende lovgivning herom"

Ad 1) Retten til at blive glemt

Løsningen tillod allerede at stamdata og transaktionsdata kunne slettes for hele records, så længe dette skete mindst 5 år efter data senest medgik i en regnskabsafslutning. Den eksisterende funktionalitet blev således videreført uændret, og uden mulighed for at slette udvalgte felter pr. record. Dette ligeledes baseret på Offentlighedsloven § 13 om Notatpligt (gældende dansk lovgivning, som går

forud for EU persondataforordningen) og god forvaltningsskik jf.:
Forvaltningsloven om notatpligt, §9.1.2

Ad 2) Retten til indsigt

Indsigtsretten blev understøttet via implementering af en ny rapport, der kan udtrække alle de stamdata og transaktionsdata, hvor der inkluderes et CPR-nummer i datasættet.

Rapporten er således baseret på: Debitordata, Kreditordata, Ressourcedata, Medarbejderdata og Ansættelsesdata. Rapporten er afgrænset således at der kun kan trækkes data for et CPR-nummer ad gangen. Rapporten kan enten udskrives til Pdf eller til Excel for en understøttelse af porteringspligten.

Ad 3) Retten til at få udlæst alle sine persondata

Se rapportbeskrivelsen under punkt 2

Ad 4) Sløring af CPR-nummer ved udskrift

Alle eksisterende rapporter er kontrolleret for visning af CPR-nummer og efterfølgende tilføjet mulighed for at sløre CPR-nummer ved udskrift.

Derudover er der bygget mulighed for at sløre data på testregnskaber, der typisk distribueres bredere end produktionsregnskaber, og hvor formålet med adgang til testdata kan afvige for formålet med adgang til produktionsdata.

4. Systemkrav

Minimumskravene klassificeret som systemkrav omhandler krav, der ikke direkte påvirker funktonaliteten i applikationen, men bidrager til sikkerheden omkring adgangen til systemet.

4.1 Restriktiv adgangsstyring

Formål
Udbetalingssystemer og betalingsafledende systemer skal implementere en restriktiv adgangsstyring for at sikre integriteten i løsningen, og sikre mod uautoriseret adgang til og brug af data.

Det er en helt grundlæggende forudsætning for alle de øvrige minimumskrav, at de personer der har adgang til systemerne også er dem de udgiver sig for, og at de kun har de nødvendige adgange.

Særligt i forhold til lovkrav omhandlende personmæssig adskillelse, som anført under §24 i bekendtgørelsen om statens regnskabsvæsen, er det kritisk, at der er fuld tillid til, at det er de rigtige brugere, der anvender systemet. Implementering af dette krav, sikrer ligeledes en mere smidig og overskuelig brugerkontrol.

Generisk Implementering
I forhold til autentificering (*hvem er du*) skal systemerne i videst muligt omfang følge implementeringsvejledningen beskrevet i IS027002 afsnit 9.4.2 om 'Procedure for sikker log-on' og Passwordvejledningen fra Center for Cybersikkerhed. Af disse anbefalinger kan særligt fremhæves:

- Ingen anvendelse af standardpassword
- Hashing af password ved lagring
- Anvendelse af fler-faktor-autentifikation hvor muligt
- Sløring af indtastede oplysninger ved log-on
- Kryptering af al dataudveksling indeholdende passwords
- Registrering af fejlede log-on forsøg
- Nedlukning af sessioner efter periode uden aktivitet

Det er også værd at bemærke, at det ikke nødvendigvis øger sikkerheden at lade et password udløbe ofte (fx efter 3 måneder). I stedet skal der kræves anvendelse af et password der består af minimum 12 eller flere tegn, med udløb sjældnere, fx efter 12 måneder.

Hvis udbetalingssystemet eller et betalingsafledende system indgår i et Single Sign On miljø, skal man være opmærksom på de risici, der kan være i SSO løsninger. Der skal især tages højde for risikoen for single-point-of-failure, ved

kompromittering af password eller adgang til en ulåst PC. Konsekvenser er, at ved uretmæssig adgang til ét system, fås adgang til alle systemer i SSO miljøet. Denne risiko skal minimeres ved bl.a. at operere med mellemlange passwords på mindst 12 tegn, og uden mulighed for genbrug af passwordtekst, samt andre tiltag der gør passwords i et SSO setup ekstra sikre.

Generelt set skal det mest forretningskritiske system i et SSO setup være styrende for niveauet af sikkerheden, og indføres de ekstra sikkerhedsforanstaltninger, må SSO løsninger betragtes som mest fordelagtige, i forhold til brugerstyring pr. system.

I forhold til autorisation (*hvad må du*) skal der være udarbejdet en politik for adgangsstyring som skal indeholde de elementer beskrevet under ISO27002 afsnit 9.1.1 og overholde nedenstående krav til styring af rettigheder:

- Rettigheder skal være opdelt på et niveau, hvor det er muligt at tildele adgang til systemet svarende til det arbejdsbetingede behov.
- Det skal være muligt at tilgå systemet med adgang til kun at læse data, fx for personer i en controllerfunktion, uden at kunne udføre arbejdsprocesser i systemet, der afleder skrivninger.
- Brugere med privilegerede rettigheder må ikke, alene, kunne gennemføre en udbetaling.
- Brugere med privilegerede rettigheder må ikke samtidig have adgang til kildekoden for systemet.
- Kun brugere med særlige brugeroprettelsesrettigheder må kunne tildele andre brugere rettigheder

For brugere med privilegerede rettigheder gælder desuden at implementeringsvejledningen i ISO27002 afsnit 9.2.3, i videst muligt omfang skal følges.

Referenceimplementering
Navision Stat understøtter flere forskellige metoder til autentifikation. Disse er givet ved: NAV serveren, Windows AD, Microsoft Azure Access Control service (ACS) eller Azure Active Directory (Azure AD).

I driftsscenarier, ved adgang via den klassiske windowsklient, anvendes autentifikation gennem Windows AD, da brugerstyringen derved samles et sted og er underlagt de krav der i forvejen gælder brugernes Windows konto. Dette fungerer i praksis som en SSO løsning, da der er adgang til Navision Stat, så snart der er logget på klientmaskinen.

For brugere oprettet hos Statens-IT er der bl.a. krav om 12 tegn i passwordet og krav til kompleksiteten af passwordet, samt 2-faktor login vha. SMS kode ved VPN forbindelser. Brugerkonti der ikke har været aktive i en periode, bliver desuden spærret.

Rettighedsstyringen i Navision Stat er implementeret ved hjælp af 90 roller (rettighedssæt). Grundprincippet er, at en brugeres rettigheder opbygges lagdelt, så der altid startes med en basis læseadgang, hvorefter der kan gives rettigheder til en mere bred og generel adgang, og til sidst suppleres med specifikke roller til særligt udvalgt funktionalitet.

For en mere detaljeret beskrivelse af rettigheden i Navision Stat se Brugeradministrationsvejledningen her:
Navision Stat brugervejledninger

4.2 Pålidelig backup og genskabelse

Formål
Formålet med minimumskravet for backup og genskabelse er at sikre mod tab af data, samt at give mulighed for at sikre data i et øjebliksbillede, hvis der skulle opstå tvivl om svig f.eks. relateret til udbetalingsfunktionalitet. Systemet skal også garderes mod system- eller medienedbrud, uforudset sletning eller kompromittering af systemdata.

Jf. SikkerDigital.dk og ISO Standard 27002 pkt. 12.3 er det vigtigt at sikre data i sit system. Ifølge SikkerDigital.dk er mangelfuld backup et af de mest almindelige årsager til, at virksomheder mister deres data. Læs mere om dette og de råd, som SikkerDigital.dk giver her:
Invester i en it sikkerhedspakke med backup

Dette krav er særlig relevant for overholdelse af §44 i bekendtgørelsen om statens regnskabsvæsen, da man som institution er forpligtet til, at opbevare regnskabsmateriale og sikre det kan fremfindes, i mindst 5 år fra udgangen af aktuelt regnskabsår.

Generisk Implementering
For at sikre data skal man anvende databasesoftware, der understøtter planlagte backup-rutiner, samt muligheden for at genskabe data. Det anbefales at udarbejde og implementere en backup-politik, der beskriver virksomhedens backup-planer for systemdata, software og systembilleder. Ydermere er det vigtigt at teste alle sine backup-planer og procedurer for genskabelse grundigt, så man hurtigt kan eksekvere i tilfælde af systemnedbrud og akut behov for datasikring. Der skal derfor periodisk foretages gendannelse af sikkerhedskopier fx i forbindelse med en beredskabstest.

Der skal minimum dagligt tages backup af transaktionsdata, så det er muligt at genskabe data i databaser, datafiler eller særskilte logfiler. De data der indgår i betalingsprocesser skal identificeres, og det skal analyseres, hvor længe det vil være hensigtsmæssigt at opbevare kopier af disse data. I overvejelserne er det særligt

vigtigt at inddrage situationer, der uventet kan lukke systemet ned f.eks. ved katastrofer eller medienedbrud. I den forbindelse bør man ligeledes overveje placeringen af disse backups og evt. kopier af backups f.eks. via spejling af miljøer og/eller servere.

For udarbejdelse af backup-politik og underliggende backup-planer henvises generelt til ISO Standard 27002 pkt. 12.3 og SikkerDigital.dk.

Referenceimplementering
For Navision Stat sikres muligheden for backup og genskabelse i et samarbejde med Statens IT (SIT) og KMD, der som hostingleverandør følger kravene i ISO standard 27002.

4.3 Sikring af adgang til kildekode

Formål
Adgang til systemets kildekode skal i videst muligt omfang begrænses. Både ift. almindelig læseadgang, da ikke alle, uden et arbejdsbetinget behov, burde have adgang til at læse koden, men også ifm. udvikling og vedligehold af systemet. Systemudviklere skal begrænses adgang til hovedversionen, og nødvendig adgang bør logges. Dette gøres af sikkerhedshensyn og for at sikre systemets funktionelle integritet[4]. Dette krav bidrager således til en øget positiv risikovurdering af den samlede systemløsning, da sårbarheden, overfor tilsigtet eller utilsigtet ændringer i systemets funktionalitet, mindskes. Denne sårbarhed er særlig vigtig at håndtere, da ændringer på kildekodeniveau kan være særligt svære at identificere og kontrollere. Dette krav har en tæt relation til minimumskrav 2.6 "Sammenhængende systemdokumentation", da systemdokumentationen kun kan være retvisende, hvis man kan garantere kildekodens integritet.

Der er situationer hvor begrænsning af læseadgang ikke giver nogen sikkerhedsmæssig værdi, f.eks. hvis der er tale om systemudvikling i Open Source format.

Generisk Implementering
Sikkerheden i systemet kan kompromitteres, hvis kildekoden publiceres offentligt og derfor bør kildekoden ikke være tilgængeligt fra driften af systemet. Her skal systemet være kompileret eller pakket på en sådan måde, at koden ikke kan aflæses.

Desuden skal man nøje overveje offentlig publicering eller udskrift af kode, hvis

[4] Se ligeledes ISO Standard 27002 afsnit 9.4.5.

der opstår et sådant behov. Dette gælder både hvilken del af koden, der publiceres, og efterfølgende opbevaring af den publicerede del. Det er også vigtigt at integriteten opretholdes, til det formål anbefaler ISO standarden f.eks. anvendelse af digital signatur.

Adgangen til den kildekode, der udgør den faktiske release-bare version af systemet, skal i endnu højere grad begrænses. Dette for at sikre systemets funktionelle integritet ved kun at introducere kode, hvor formål med og dokumentation af koden er kontrolleret og godkendt. Det betyder at man skal overveje hvem, og hvor mange, der skal have adgang til masterversionen af systemet.

Ændringer i kildekoden skal kunne spores for at sikre, at de ændringer der indgår som led i systemvedligehold og -udvikling, er foretaget af personer med passende rettigheder, og at ændringerne desuden stemmer overens med den aftalte og dokumenterede nødvendige systemtilpasning.

Begrænsning af adgang
Der skal helt overordnet set begrænses adgang til kildekode og systemdokumentation. Det skal kun være personer der indgår direkte, eller som led i, systemudviklingen, der kan opnå adgang. Derfor skal supportfunktioner f.eks. ikke bare uden fornuftigt belæg have ubegrænset adgang. Dette kan opnås med rettighedsstyring, og det kan opnås ved at pakke systemet på en måde, der ikke tillader aflæsning af den bagvedliggende kildekode. Koden skal opbevares et centralt sted, med begrænsning af personer med direkte adgang.

Forgrening
Rent udviklingsmæssigt er det selvfølgelig en nødvendighed med adgang til koden. Der bør dog stadig kun være så få udviklere som muligt, med direkte adgang til master-udgaven af systemet. Dette kan løses ved anvendelse af centrale kodebiblioteker og/eller værktøjer, der tillader opbevaring af en master-udgave med tilhørende forgreninger[5]. På denne måde kan udviklere få adgang til deres egen lokale kopi af et system, og ved publicering kan koden pushes til master-udgaven. Dette foregår normalvis ved at udvikleren udfører en pull request og afvikler en anmodning om, at den nye kode bliver en del af masterudgaven.

Frekvent kode-review
Tilpasninger til systemet skal kontrolleres, testes og godkendes, for at sikre rigtigheden af det kode der introduceres. Der skal foretages en risikobaseret udtagning til kode-review, således at der altid kontrolleres for særlig kritisk kode, der f.eks. relaterer sig til udbetalingsprocesser eller rettighedsstyring. På denne måde sikrer man sig formålet med koden, samt at systemets integritet bibeholdes. Kode-review skal foretages af en eller flere andre udviklere, eller man kan udvælge en senior- eller lead-udvikler med ansvar for at kontrollere alle kodemæssige bidrag til systemet.

---

[5] F.eks. GIT eller TFS

Logning af ændringer og versionsstyring
Det er vigtigt at kunne administrere forskellige versioner/udgaver af systemet. Dette for at kunne danne sig et overblik over ændringer fra version til version, og for understøttelse af en eventuel nødvendig tilbagerulning til tidligere version af systemet. De fleste kodebiblioteksværktøjer understøtter, ligesom forgrening, en sådan administrering af versioner. Der skal eksistere en mulighed for at kunne administrere koden pr. ændring (RFC[6]), og på det niveau også kunne se hvilken udvikler der står bag.

Man kan dog godt opnå passende styring og administrering af ændringer, via en mere manuel tilgang uden anvendelse af kodebibliotek, som f.eks. opbevaring af tidligere udgaver fra ændring til ændring, eller blot release til release. Denne håndtering kan dog besværliggøre sporing af ændringer i systemet, hvorfor man enten manuelt eller med automatisering, må sammenligne kode på fil-niveau. Man skal altså sikre sig at ændringer dokumenteres løbende i koden eller på anden vis, hvis man ikke har mulighed for at styre det via værktøjer.

Referenceimplementering
I Økonomistyrelsen anvendes versioner af begge beskrevne modeller ovenover. For hovedparten af de systemkomponenter der udgør Navision Stat, opbevares der en helt central master-udgave af den release-bar version af systemet. Denne udgave er der kun yderst få udviklere, der har adgang til. Udviklere arbejder på deres egne lokale versioner af systemet og lægger ændringer til automatisk merge på central udviklings- og central testudgave af systemet. Dvs. ændringerne ikke med det samme lægges ind på master-udgaven.

På udviklings- og testmiljøet kontrolleres kode via kode-review, automatiseret regressionstest samt manuel test, og først herefter lægges ændringer manuelt ind, af blot én central person, på master-udgaven. Kode-review er risikobaseret og derfor bliver kode der relaterer sig til særlig kritisk funktionalitet, som f.eks. udbetalingsprocesser, særligt kontrolleret og specielt ift. huller der kan udnyttes til svig.

Kodeændringer er bundet til kravnumre oprettet i et change management værktøj. Herfra er krav beskrevet og analyseret, og de personer der har arbejdet på ændringen er noteret. Alle kodeændringer, uden undtagelser, dokumenteres med disse kravnumre. På denne måde er alle ændringer dokumenteret, og al kode til en given ændring kan nemt identificeres og isoleres. Hvis koden ikke er korrekt dokumenteret, afvises den. Se ligeledes afsnittet om dokumentation

[6] Request for Change

4.4 Sammenhængende systemdokumentation

Formål
For at sikre en robust Change Management proces, skal de enkelte ændringer til løsningen dokumenteres fra specifikation af ønsket ændring og frem til en præsentation for forretningen, der beskriver resultatet af den implementerede ændring.

Derudover skal Rigsrevisorloven §10, 2 iagttages, hvor det fremgår at,
Rigsrevisor skal have adgang til at udtale sig, inden en sådan myndighed i sit regnskabssystem eller sin forretningsgang iværksætter forandringer, der har betydning for revisionen.

Denne forpligtigelse over for revisionen, efterfulgt af en eventuel IT-revision, kan kun imødekommes via en robust Change Management proces.

Generisk Implementering
Robust Change management herunder overholdelse af §10, stk. 2 fordrer, at følgende overholdes:

1. Der skal implementeres funktionalitet, eller vedligeholdes simple lister, der giver et udtømmende opdateret overblik over ændringer til løsningen, og deres nuværende status.
2. Der skal udarbejdes kravspecifikationer og testdokumentation.
3. Der skal ske en entydig og konsistent opmærkning af de systemobjekter, der inkluderes i en given ændring.
4. Der skal endvidere sikres en sporbarhed fra det ændrede systemobjekt og frem til beskrivelsen af ændringen, sådan som ændringen præsenteres for forretningen.
5. Der skal udarbejdes dokumentation for en beskrivelse af den samlede ændring af et givent funktionalitetsområde, for en beskrivelse af funktionalitet, før og efter ændringen set ud fra et forretningsmæssigt perspektiv
6. Der skal udarbejdes brugervejledninger i det omfang, dette er nødvendigt for en korrekt anvendelse af funktionaliteten, og disse brugervejledninger skal opdateres ved væsentlige ændringer til funktionalitetsafvikling set fra et forretningsmæssigt perspektiv
7. Der skal udarbejdes installationsvejledninger i det omfang, installationen ikke er selvafviklende, eller hvor installationen sker ved anden enhed end den enhed, der har ansvaret for ændringen.

Referenceimplementering
De anførte krav er implementeret for Navision Stat på følgende vis:

1. Alle ændringer (udviklingsopgaver) registreres i en Change Management database (KVV), med angivelse af status og kobling til den release, hvor ændringen forventes implementeret.

2. Der udarbejdes kombineret krav- og testspecifikationer, der linkes til udviklingsopgaven i KVV.
3. Der sker en entydig og konsistent opmærkning af de systemobjekter, der inkluderes i en given ændring via en opmærkning med udviklingsopgavereferencen fra KVV.
4. Der sikres en sporbarhed fra det ændrede systemobjekt og frem til beskrivelsen af ændringen, ved at mærke alle systemobjekter – relateret til en given ændring, med den reference, som udviklingsopgaven er oprettet med i KVV, og som gengives ved beskrivelsen i 'Nyt i Navision Stat'.
5. Ved hver release (typisk på månedsbasis) dokumenteres alle ændringer via 'Nyt i Navision [Versionsnummer], for en beskrivelse af den ændrede funktionalitet, set ud fra brugerens vinkel og et forretningsmæssigt perspektiv.
6. Der udarbejdes brugervejledninger for den samlede funktionalitet udviklet ved Økonomistyrelsen. Brugervejledningerne opdateres løbende ifm. implementering af større nye funktionalitetsområder. Brugervejledningerne gennemgås endvidere, for nødvendige opdateringer og konsekvensrettelser, minimum 1 gang årligt i forbindelse med et dokumentationssprint i december måned, hvor der ikke frigives ny funktionalitet.
7. Der udarbejdes installationsvejledninger ved hver ny frigivelse for afvikling ved KMD, Statens IT og lokale intern IT enheder.

4.5 Robust RPA implementering

Formål
Anvendelse af RPA (Robotic Process Automation) til automatisering af trivielle forretningsprocesser er efterhånden en kendt løsning, når et givent system ikke (hurtigt nok) kan understøtte automatisering af et givent workflow. Her må implementeringen af RPA ikke kompromittere den indbyggede forretningslogik i applikationen og de sikkerhedsforanstaltninger, der er pålagt systemet. Den automatiserede proces skal således følge samme regler og principper, som hvis det var en bruger der udførte processen.

Dette krav har ydermere til formål at sikre opmærksomhed omkring den øgede risikovurdering og kontrol, anvendelsen af RPA i betalingsprocesser vil medføre. RPA-tilføjelse vil alt andet lige øge kompleksiteten i den samlede løsning, og dermed kontrol og tilsyn. Dette skal vejes op mod de effektiviseringsgevinster, der kan opnås med RPA.

Generisk Implementering
Der gælder de samme minimumskrav for en RPA løsning, som den underliggende applikation. Hvis RPA løsningen udelukkende fungerer som automatise-

ring af de samme handlinger/funktioner en bruger benytter i systemet via grænsefladen, må det ikke, rent teknisk, være muligt for RPA processen at omgå disse krav.

Bemærk, at det endvidere altid kræves at selve varemodtagelsen, afledt af disponeringen, foretages ved et fysisk menneske, som første led i betalingsprocessen. Efterfølgende godkendelser og procestrin, kan udføres af en RPA implementering, så længe det kan verificeres, at data ikke har været ændres efter den første godkendelse. Kravet om garanti for dataintegriteten er således gældende på tværs af alle de systemer, der indgår i betalingsprocessen.

Det er vigtigt at understrege, at man med implementering af RPA, på et eller flere systemer, påtager sig et ansvar som systemejer for processen. Dette forhold er særligt kritisk for processer, der afleder en bogføring eller en faktisk udbetaling fra systemet. Funktionsadskillelse må ikke omgås og RPA løsningen skal altså derfor bygges i mindst to forskellige processer, der afvikles med forskellige konti, således indbygget funktionsadskillelse på brugerniveau overholdes i systemet. De to robotter må selvfølgelig ikke blot blindt godkende hinandens aktivitet, hvilket betyder der skal implementeres et decideret godkendelsesflow i begge processer. Dette flow skal have defineret klare og restriktive regelsæt og robotten skal, ligesom en almindelig bruger, kunne kontrollere udbetalingen op mod det oprindelige grundlag. Hvis robotten ikke kan verificere kontrollen for eksempelvis en udbetaling, skal denne overgå til manuel behandling.

RPA-koden skal kontrolleres for skjult eller uhensigtsmæssig logik. Der skal, ligesom med kildekoden til applikationen, opsættes begrænset adgang og funktionsadskillelse på implementering og vedligehold af koden. Der skal udføres kodereview, der skal sikre robottens funktionelle integritet, og for at forebygge svig.

Der skal opsættes funktionsadskillelse imellem udvikling og drift af for den enkelte RPA-proces i kundens, eller forretningens, produktionsmiljøer. På denne måde sikrer man sig, at robotprocessen altid svarer til den godkendte version, og at processen kun anvendes til det godkendte formål.

Det er ikke hensigtsmæssigt at implementere og vedligeholde en RPA-proces, der blot emulerer samme funktionalitet, som et enkelt system i forvejen understøtter. Det er således vigtigt at få kortlagt processen og sammenholde den med funktionalitet i systemet, og dermed analysere alle mulighederne for at anvende systemets egne funktioner, frem for en RPA løsning. Dette under hensynstagen til både økonomi og mulige kvalitetsløft. Anvendelse af en RPA løsning kan imidlertid bliver relevant og særlig brugbar, når en forretningsproces strækker sig over flere systemer. Et eksempel kunne være kontrol af udbetalinger. Her kan en robot fx kontrollere linjer, der står til udbetaling op i mod grundlaget for betalingerne i et andet system.

Referenceimplementering
I Navision Stat udviklingsenheden er der implementeret RPA processer relateret til intern systemforvaltning. Det er dog fravalgt at implementere RPA på systemets indlejrede udbetalingsprocesser, da systemets indbyggede sikkerhedsforanstaltninger med funktionsadskillelse, kontrol- og godkendelses-flows skal sikres kontinuert opretholdt. Eksempelvis er godkendelsesflows særlig kritiske ift. automatisering, da man ikke blot må opsætte to robotter, der forhåndsgodkender hinandens aktivitet, som beskrevet under den generiske implementering. Begge robotter skal kontrollere betalingerne op i mod grundlaget for den pågældende udbetaling.

Hvis der skulle bygges RPA processer oven på udbetalingsfunktionalitet i Navision Stat, ville det være nødvendigt at opsætte restriktive regler for kontrol og opbevaring af robotkoden, samt at robotten emulerer samme kontrol- og godkendelses-flows, som gælder for almindelige brugere i systemet. Samtidigt hermed kompliceres kodereview, systemtest og revision unødigt.

Eventuel yderligere automatisering på udbetalingsprocesser i Navision Stat, vil derfor ske via udbygning af den eksisterende systemkode, der potentielt sikrer en samlet låst proces fra accept af køb til bogføring af afledt udbetaling.

5. Applikationskrav

Minimumskravene klassificeret som applikationskrav omhandler krav, der sikrer at løsningsdesignet i applikationen understøtter transaktionssporbarhed, funktionsadskillelse og kontrolmuligheder

5.1 Påkrævet logning

Formål
Det er vigtigt at logge alle handlinger i systemet relateret til udbetalingsprocessen, samt at logge tildelingen af rettigheder til at foretage disse handlinger. Formålet med loggen er at fastholde, hvad der er foretaget og for at have et grundlag for at kunne dokumentere compliance med gældende love, regler og principper. Loggen kan både bruges reaktivt i forbindelse med fx en intern revision, eller løbende for proaktivt at overvåge at der ikke sker brud på compliance.

Formålet understøtter således især muligheden for at imødekomme kravet om kontrol af grundlaget og den faktiske effektuering af foretagne udbetalinger jf. §28 stk. 2 i bekendtgørelsen om statens regnskabsvæsen.

Generisk Implementering
Udbetalings- og betalingsafledende systemer skal som minimum logge:

- Oprettelse, sletning og ændring af kreditorers stamdata herunder bank- og betalingsoplysninger. Stamdata skal ses som almene oplysninger som navn, adresse, telefon, mail, men også CVR-, CPR-, SE-, P- og FIK-nummer, banknavn, bankadresse, registreringsnummer, kontonummer, og alle oplysninger om udenlandske banker**.** Det er her værd at bemærke at CPR nummer her betragtes som en betalingsoplysning, på niveau med CVR-, SE- og P-nummer.
- Oprettelse og ændring af udbetalingsdata.
- Alle handlinger relateret til udbetalingsprocessen. Handlinger skal ses som bogføring (regnskabsmæssig registrering) af udbetalingsdata, udsøgning af poster til udbetaling, alle trin af godkendelser af udbetalingen, afsendelse af udbetalingsdata, standsning af udbetalingsdata og lignende handlinger.
- Afsendelse/udlæsning af data fra et betalingsafledende system til et udbetalingssystem.
- Modtagelse/indlæsning af data fra et betalingsafledende system i et udbetalingssystem.
- Tildeling/fjernelse af rettigheder til brugere
- Ændringer af indholdet af en rettighed.
- Oprettelse/nedlæggelse af brugere

Logdata skal være let tilgængeligt i en tabelstruktur (let forståeligt og søgbart), og som minimum give oplysninger om:

- Bruger-id bag ændring
- Tidspunkt for ændring
- Før værdi
- Efter værdi

Logdata yngre end indeværende år, plus 5 år, må som udgangspunkt ikke kunne slettes. Selve sletningen af logdata må kun kunne udføres at brugere med privilegerede rettigheder, og slettehandlingen skal registreres særskilt i loggen.

Hvis udbetalings- eller kreditorstamdata gemmes på en måde, så data kan tilgås ukrypteret og uden at aktivere den normale systemlog, fx direkte via Microsoft SQL Server Management Studio, skal der også her opsættes logning/auditering af adgangene til data.

Referenceimplementering
I Navision Stat er implementeret flere typer af logs, som dækker forskellige funktionsområder:

Ændringsloggen, givet ved standardfunktionalitet i MS Dynamics NAV, gør det muligt på feltniveau at opsætte en logning af oprettelser, ændringer og sletninger af data på tværs af hele applikationen. I Navision Stat er udvalgte kritiske tabeller underlagt obligatorisk logning, og logresultatet kan således ikke fjernes af brugere. Ud over den obligatoriske logning er det valgfrit at opsætte, hvilke data der supplerende ønskes logget, da intensiv logning kan have betydning for performance. Logdata er tilgængelig direkte fra klienten, og kan eksporteres til Excel eller PDF.

Superloggen logger alle handlinger foretaget af brugere med privilegerede rettigheder, herunder brugerens på- og aflogning af systemet. Denne log er altid aktiv og kan ikke omgås. Logdata er tilgængelige direkte fra klienten, og kan eksporteres til Excel eller PDF. Derudover kan en rapport over seneste logs sendes til e-mail modtagere.

Persondataloggen logger alle, der tilgår eller forsøger at tilgå originalbilag, som er markeret for indhold af følsomme persondata, jf. Personal Secure elementet i OIOUBL snitfladen

GIS Integrationsloggen logger alle data, der er modtaget fra blandt andet betalingsafledende fagsystemer. Fra denne log er det således muligt altid at se, hvilke data der danner baggrund for en udbetaling, hvis data stammer fra et eksternt system.

Udbetalingshistorik, logger alle ændringer og statusskifte foretaget på udbetalingsdata i forbindelse med afsendelse til banken.

Bruger- rettighedsloggen, logger alle bruger- og rettigheds til- og afgange. Det er således muligt at se i hvilken periode, en given bruger havde hvilke rettigheder.

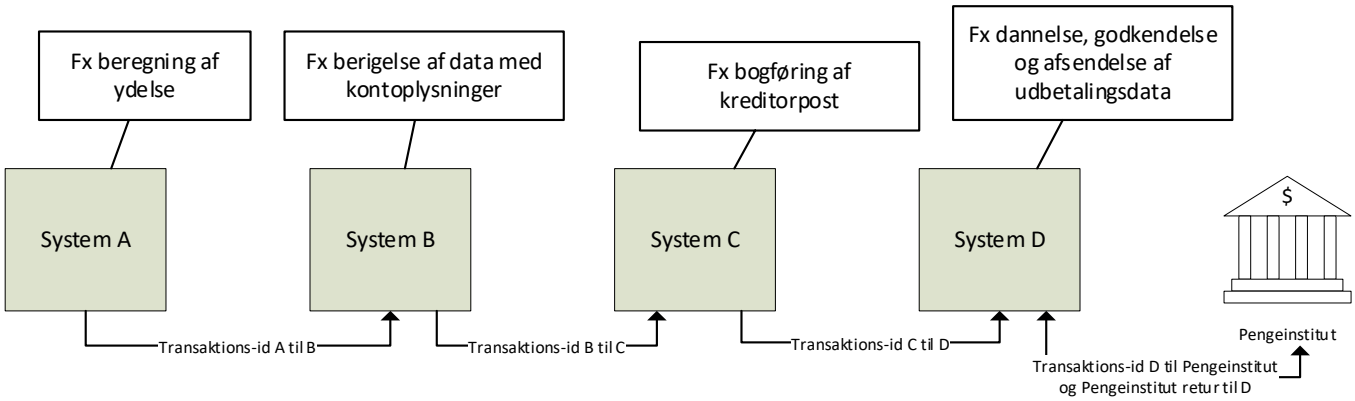
Foruden logningen i selve applikationen anvendes et SIEM (Security information and event management) system. Dette system er ikke tilgængeligt for driftsmedarbejdere med adgang til økonomisystemerne. Ved anvendelse af bl.a. SQL Servers Audit-funktion overføres kritiske handlinger i databaser og på relevante servere til SIEM, hvor en alarmeringsfunktion træder i kraft, hvis en hændelse, ud fra fast definerede kriterier, kræver nøjere udredning. Dette er for at sikre logning af ændringer der sker uden om klienten og opfølgning på uventede hændelser.

Endvidere at der er opsat logning af aktiviteter, relateret til Active Directory via et 3. parts produkt.

5.2 Tydeligt transaktionsspor

Formål
For at sikre entydig sporing af en udbetaling - fra dannelse af grundlaget for betalingen til selve afsendelse til banken - er det vigtigt at alle transaktioner og overgange mellem transaktioner stemples med unikt id.

Sporingen af en betaling er kritisk i forhold til at kunne dokumentere rigtigheden af beløb, prokura og formål i relation til udbetalingen. Det er særligt relevant at kunne spore transaktioner, hvis hele eller dele af udbetalingsgrundlaget er overført mellem et eller flere systemer. Nedenstående figur illustrerer en kæde af systemer, hvorigennem der dannes eller beriges og transmitteres udbetalingsdata. Nedenstående figur illustrerer, at hvert system sender et unikt id pr. transaktion til det foranliggende system.



Så længe alle systemerne i kæden opretholder transaktions-id'er, er det altså muligt at spore en betaling fra en bankkonto tilbage til det oprindelige grundlag.

Indholdet af dette krav er essentielt for at kunne dokumentere og garantere overholdelse af §27 i bekendtgørelsen om statens regnskabsvæsen, da man fx entydigt kan identificere modtagne bilag som dokumentationen for en registrerings rigtighed.

Generisk Implementering
Al data som indgår, helt eller delvist, i udbetalingsgrundlaget skal have et eller flere identifikationsfelter, som entydigt kan identificere den enkelte transaktion. Det kan fx være et automatisk optalt løbenummer, en GUID eller lokalt administreret unikt nummer. Hvis identifikationsfelter ikke udgør primærnøglerne[7] i datasættet, skal det på anden vis sikres at værdierne i identifikationsfelter ikke kan optræde mere end én gang. Det er essentielt at integriteten af identifikationsværdierne opretholdes, og indholdet i disse identifikationsfelter må således ikke kunne editeres, slettes eller på anden måde manipuleres, hverken direkte eller indirekte.

Hvis data i udbetalingsgrundlaget modtages helt eller delvist fra et foranliggende betalingsafledende system, skal det sikres at data indeholder et unikt id. Der må derfor ikke kunne behandles data, hvis et id allerede tidligere har være modtaget.

Hvis data indgår i en eller flere transaktioner inden det afsendes til banken, skal alle disse transaktioner kunne spores tilbage til det unikke id og dermed det oprindeligt modtagne data.

Referenceimplementering
I Navision Stat modtages udbetalingsgrundlag fra flere betalingsafledende systemer herunder et central faktureringssystem og en række lokale fagsystemer. Al data modtages med unikke sporings- eller afsender-id'er, og kan ikke behandles hvis id'erne ikke er unikke

Fra data bliver modtaget til den afledte udbetaling gennemgår det følgende transaktioner:

Fra indbakken til kreditorpost overføres afsender-id'et, og fra kreditorposten til betalingsposten overføres et unikt løbenummer, som gør det muligt at spore betalingen tilbage til den modtagne data i indbakken. Når betalingsposten afsendes til banken angives et UPR-nummer (Unique Payment Reference), som unik reference til betalingen i banken.

[7] Data i et primærnøglefelt er garanteret unikt af databasemanagement systemet

5.3 Datakonsistens og låsning

Formål
Data der udgør udbetalingsgrundlag og som kopieres mellem systemer eller kopieres mellem tabeller internt i ét system, skal sikres mod inkonsistens, så der altid kan være tillid til det oprindelige data. Generelt skal udbetalingsgrundlaget undergå så få procestrin som muligt, så kopiering eller anden behandling af data minimeres.

Implementeringen af dette krav er med til at sikre en nøjagtig og fuldstændig regnskabsmæssig registrering af betalingstransaktioner, og sikrer regnskabsmaterialet mod forvanskning og ødelæggelse som beskrevet i §§ 21 og 27 stk. 7 i bekendtgørelsen om statens regnskabsvæsen.

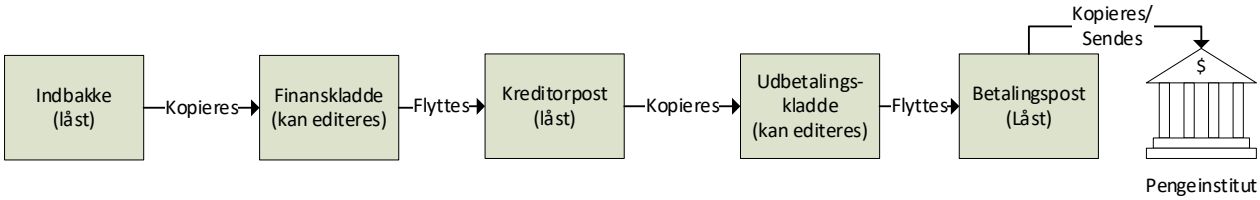
Generisk Implementering
Hvis data i udbetalingsgrundlaget modtages helt eller delvist fra et betalingsafledende system, skal modtaget data gemmes i en indbakkestruktur. Indbakkerne skal altid indeholde al data modtaget fra betalingsafledende systemer fuldstændigt som de blev modtaget. Indholdet i indbakkerne må således ikke kunne editeres, slettes eller på anden måde manipuleres, hverken direkte eller indirekte, uanset rettigheder til systemet[8].

Hvis data i udbetalingsgrundlaget flyttes mellem tabeller internt i systemet, som led i en eller flere delprocesser for yderligere berigelse eller rettelse, skal enhver registrering/bogføring af det ændrede data opbevares, så det ikke kan editeres, slettes eller på anden måde manipuleres, hverken direkte eller indirekte, uanset rettigheder til systemet.

Data der formelt er godkendt skal være låst for editering. Hvis der opstår behov for at rette data efter godkendelse, skal det kræve en eksplicit handling for åbning af data ved brugeren. Dato, tid og bruger-id for aktivering af handlingen skal logges. Enhver sådan ændring skal resultere i nyt godkendelsesflow.

Referenceimplementering
I Navision Stat modtages udbetalingsgrundlag bl.a. fra flere betalingsafledende systemer herunder et centralt faktureringssystem og en række lokale fagsystemer. Data modtages i forskellige indbakker og kopieres og flyttes i delprocesser gennem en række tabeller indtil betalingen sendes til banken. Nedenstående figur skal illustrere på hvilke procestrin data er låst, og på hvilke procestrin data kan editeres:

[8] Kun i særlige tilfælde, i forbindelse med fx datakonvertering eller fejlrettelser, kan data i indbakker eller i låste posttabeller ændres eller slettes. Dette kræver dog særlig udvidet dokumentation og godkendelse.



Som det fremgår vil data i kildetabeller altid være låst, hvis data kan kopieres til videre editering og behandling.

Foruden den viste proces, er det muligt, i udbetalingskladden i Navision Stat, at åbne allerede delvist godkendte betalingsforslag op for editering. Dette sker ved en eksplicit handling, som logges i en historiktabel. Hvis data åbnes for editering skal betalingsforlaget delvist godkendes på ny.

5.4 Ingen undtagelser fra produktstrategien

Formål
De forretningsprocesser et betalingsafledende system eller udbetalingssystem understøtter og dermed opbygger kontrol- og sikkerhedsfunktioner op omkring, er oftest det normale brugsscenarier. I tilfælde af behovet for at afvige fra den normale procedure, kan det være fristende løbende at udbygge systemet så forskellige typer af undtagelser kan håndteres. For enhver variant af standardprocessen der håndteres, tilføres kompleksitet til løsningen og for brugerne, som øger risikoen for programmatiske eller menneskelige fejl.

Generisk Implementering
Det er vigtigt at der udarbejdes en klar strategi og politik for systemets anvendelse og muligheder for udvidelser og tilpasninger, således at systemets funktionalitetsområde og løsningsdesign ikke bevæger sig i en uhensigtsmæssig retning, baseret på komplekse undtagelser.

Kernefunktionaliteten skal understøtte mindst 80% af de normale daglige driftssituationer, og enhver afvigelse fra dette skal fremgå tydeligt i strategien.

Strategien kan fx omfatte følgende punkter:

- Kriterier for redigering af udbetalingsgrundlag inden delvis godkendelse
- Kriterier for anvendelse af komplette betalingsoplysninger
- Kriterier for anvendelse af andre bankcentraler end NemKonto
- Processen for at standse en betaling
- Processen for håndtering af forkerte betalingsoplysninger
- Processen for dokumentation af afvigelser i udbetalingsgrundlaget
- Kriterier for at accept af Change Request til funktionaliteten

- Kriterier for format og datakvalitet modtaget fra betalingsafledende systemer

Strategien skal være med til at minimere behovet for at udvide eller ændre funktionaliteten, ved at være normerende for hvilke forretningsprocesser der understøttes. Change Management skal således være bundet op på strategien, så løsningen ikke knopskyder uden for rammerne angivet i produktstrategien.

Referenceimplementering
I Navision Stat er er funktionaliteten til at understøtte udbetalingsprocessen udviklet af 3. part, som en standardudvidelse til Dynamics NAV 2016 produktet. Denne standardudvidelse er løbende blevet tilpasset de statslige anvendelsesbehov, så brugerne kun tilbydes funktionalitet der falder inden for vore produktstrategi. Via vejledninger i betalingsformidling beskrives de processer der understøttes og hvordan brugeren skal håndtere afvigelser.

I forhold til integrationer med betalingsafledende systemer, er der en opbygget en klar governance struktur, der sikrer, at alle integrationer overholder formater og retningslinjer.

5.5 Tvungen funktionsadskillelse

Formål
Tvungen funktionsadskillelse skal sikre en personmæssig adskillelse (via 2 eller flere brugere) mellem adgangen til at disponere, godkende, anvise og betale, såvel direkte som indirekte, og dermed mindske risikoen for at der, forsætligt eller uforsætligt, foretages ukorrekte udbetalinger. Det må således ikke være teknisk muligt for én person i et udbetalingssystem, både at foretage den regnskabsmæssige registrering, og dermed at danne datagrundlaget for en udbetaling og efterfølgende sende samme betaling. Kontrollen af dette skal altså være fuldt systemunderstøttet og ufravigeligt.

Implementering af dette krav indfører en systemunderstøttet sikring af den lovpligtige personmæssige adskillelse, der er beskrevet i §28 i bekendtgørelsen om statens regnskabsvæsen, hvilket effektiviserer kontrollen med, og dokumentationen af, personadskillelsen.

Generisk implementering
Den personmæssige adskillelse skal som minimum sikres via oprettelse af differentierede brugerkonti, men kan eventuelt suppleres med biometriske kontroller.

Betalingsafledende systemer skal systemunderstøtte en godkendelsesproces, der sikrer, at mindst 2 personer har godkendt det betalingsafledende data, inden det kan sendes til et andet betalingsafledende system eller udbetalingssystem. Dette krav sikrer, at modtagende systemer kan betragte al modtaget data som værende forhåndsgodkendt.

Udbetalingssystemer skal systemunderstøtte en godkendelsesproces, der sikrer funktionsadskillelse ved, at mindst 2 personer har godkendt datagrundlaget, inden det kan sendes til banken.

Der skal i udbetalingssystemet desuden være systemunderstøttet personadskillelse mellem den person, der foretager den regnskabsmæssige registrering af udbetalingen, og den der endeligt godkender udbetalingen.

Alle trin i udbetalingsprocessen skal registreres med: dato, tid og bruger-id på den person der udførte handlingen.

Kontrolfunktionen, der sikrer funktionsadskillelse, skal spærre for at udføre en proceshandling, såfremt funktionsadskillelse ikke kan verificeres.

Enhver ændring i udbetalingsdata efter første godkendelse skal resultere i, at alle udbetalingsdata for den enkelte udbetaling skal have nulstillet godkendelsen og dermed godkendes på ny.

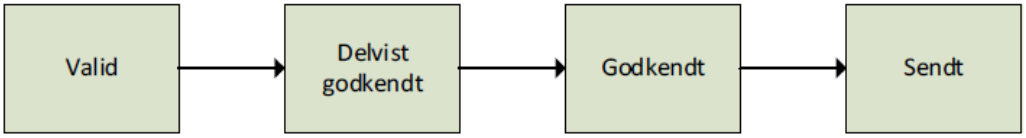
Kontrolfunktionen, der sikrer funktionsadskillelse, skal verificere adskillelsen ud fra bruger-id på den person, der udfører handlingen mod det bruger-id, der er registreret som at have udført den handling, der kontrolleres mod. Kontrollen må således ikke bero på opsætninger, så som rettigheder eller gruppemedlemskaber.

I betalingsafledende systemer eller udbetalingssystemer må én fysisk person ikke råde over mere end ét bruger-id med adgang til systemet, der giver mulighed for at udføre handlinger i udbetalingsprocessen, eller behandle data relateret hertil.

Hvis en bruger tildeles nyt bruger-id til et betalingsafledende system eller udbetalingssystem, efter tidligere at have haft adgang til samme system, skal det kontrolleres, at brugeren ikke indgår i nogle igangværende udbetalingsprocesser, med det gamle bruger-id.

Hvis en bruger har adgang til mere end ét system, der indgår i den samlede betalingsproces, skal bruger-id'et på tværs af systemerne så vidt teknisk muligt være ens. Dette sikrer en nemmere kontrol af det samlede betalingsspor. Hvis det ikke er muligt at anvende samme brugerkonto eller bruger-id, skal der i hvert system være oplysninger relateret til bruger-id'et, der tydeligt kan identificere den fysiske bruger, der er tilknyttet bruger-id'et. Oplysningerne der identificerer den fysiske bruger skal være opdaterede. Udbetalingssystemer skal indeholde funktionalitet til at kunne styre hvilke specifikke brugere, der må indgå i hvilke dele af godkendelsesprocessen af udbetalinger. Det skal således være muligt at angive hvilke brugere der har prokura til at første godkende og hvilke brugere der har prokura til at endeligt godkende. Opsætning af prokurister skal kræve en bruger med særlige rettigheder. Der skal understreges at den systemunderstøttede kontrol af funktionsadskillelsen skal sikre, at uanset prokuraopsætningen, kan samme bruger aldrig endeligt godkende betalinger vedkomne selv har første godkendt.

Reference implementering
I Navision Stat er funktionsadskillelsen i forbindelse med godkendelsen implementeret ved hjælp af et workflow, som sikrer, at betalingsdata skal gennemgå en række statusskifte, før de kan afsendes endeligt til banken. Nedenstående figur viser de nødvendige status som betalingsdata i Navision Stat successivt skal opnå:



Alle statusskift logges i særskilt historiktabel, hvor: data, tid og bruger-id registreres. Ved statusskiftet fra 'Delvist godkendt' til 'Godkendt' kontrollerer forretningslogikken funktionsadskillelsen både mellem brugeren der endeligt godkender og den bruger der har delvist godkendt, men også funktionsadskillelsen mellem brugeren der endeligt godkender og den bruger der har bogført kreditorposten, der har dannet grundlag for betalingen. Hvis der ikke er difference mellem bruger-id'erne afbrydes godkendelsen med fejl.

I Navision Stat findes desuden en omfattende prokuraopsætning, hvor det er muligt at indmelde specifikke brugere i prokuragrupper som tildeles godkendelsesgrænser i procentsatser, beløbsgrænser samt filtre for hvilke konteringsdimensioner der må godkendes betalinger for. Prokuraopsætningen kan ydermere opdeles til kun at gælde for én given bankcentral til én given udbetalingskonto Det kræver en særskilt prokurarolle at kunne foretage prokuraopsætningen.

5.6 End-to-end udbetalingskontrol

Formål
Det er helt essentielt at en udbetaling kan kontrolleres for korrekt formål, beløb og modtager. Kontrollen skal gælde behandlingen af udbetalingsgrundlaget, samt hele udbetalingsprocessen og kunne afdække eventuelle ændringer i data undervejs enten mellem systemer eller internt i et system. En sådan kontrol skal blandt andet kunne danne dokumentation for registreringernes rigtighed over for godkendere og revisioner, og skal sikre overholdelse af §27 stk. 2 i bekendtgørelsen om statens regnskabsvæsen.

Generisk Implementering
Alle betalingsafledende systemer der indgår i den samlede udbetalingsproces skal have implementeret en kontrolrapport der viser, hvilke data der er sendt videre til andre betalingsafledende systemer eller udbetalingssystemer., hvem der har oprettet og godkendt data. Hvis al eller dele af data er modtaget fra et betalingsafledende system, skal rapporten desuden angive om data har været ændret efter

modtagelse, og i givet fald hvad der er ændret. Det unikke id skal fremgå af rapporten for hver datapost, så det muliggør kontrol på tværs af systemkæden. Rapporten skal kunne dannes i et ikke-editerbart format.

For udbetalingssystemer skal der ligeledes kunne foretages en kontrolsammenligning af betalingsgrundlaget op mod det modtagne data, inden betalinger sendes til banken. Dette er i tilfælde hvor det er muligt at berige eller rette data modtaget fra foranliggende betalingsafledende systemer, inden udbetalingen. Al data modtaget fra et betalingsafledende systemer skal anses for værende godkendt ved modtagelse, og enhver afvigelse i kontrolsammenligningen skal kunne dokumenteres, og godkendes inden udbetaling kan foretages. Det skal ligeledes være muligt at foretage kontrollen i udbetalingssystemer bagudrettet på allerede foretagne betalinger.

Foruden den isolerede kontrol af enkelte eller sæt af betalinger, skal systemernes datamodel, hvis muligt, understøtte AI og/eller statistisk baseret afsløring af bedrageri (Fraud detection). Det betyder at relationer mellem dataentiteter skal være udbyggede og entydige, samt at der registreres så mange relevante informationer som teknisk forsvarligt om hvilke data, der ændres eller forsøges ændret, hvilke funktioner der udføres eller forsøges udført, af hvem og hvornår.

Referenceimplementering
I Navision Stat skal der, i forbindelse med den endelige godkendelse i udbetalingsprocessen, foretages en kontrol af om data i udbetalingskladden er ændret i forhold til data modtaget fra et betalingsafledende system. Kontrollen sker vha. en rapport der tydeligt viser afvigelser i data, der er opstået i de mellemliggende processer mellem modtagelse af data og udsøgning til betaling. Rapporten udskrives til PDF format og gemmes på et sikkert drev. Alle eventuelle afvigelser i data der fremgår af udskriften, skal dokumenteres i særskilt proces uden for applikationen. I denne proces gemmes dokumentationen for afvigelserne på samme placering som kontrolrapporten, for fremtidig revision. Hvis data ikke modtages fra betalingsafledende system, men er oprettet manuelt i Navision Stat, via en kladde eller købsfaktura, skal hele udbetalingen dokumenteres, da al data vil fremstå som ændret i kontrolrapporten. En lignende kontrolrapport kan afvikles på alle historiske betalinger, dvs. efter at betalingen er sendt til banken.

5.7 Sikker udbetaling via NemKonto

Formål
Alle udbetalingssystemer, skal understøtte integration til NemKonto-systemet jf. 'Bekendtgørelsen om NemKontoordningen', hvoraf det fremgår at: NemKonto-systemet kobler en borgers eller virksomheds CPR- eller CVR-nummer til en bankkonto, som borgeren eller virksomheden selv har valgt som deres NemKonto. Den koblede bankkonto kan efterfølgende, hvis nødvendigt, let ændres i NemKonto-systemet, uden at de offentlige institutioner behøver at opdatere deres oplysninger.

Samtidigt er offentlige myndigheder forpligtiget til at benytte denne NemKonto til udbetalinger og/eller refusioner.

Ifølge 'Loven om offentlige betalinger' fremgår det at endvidere, at det er obligatorisk for personer og virksomheder at have angivet en NemKonto:

"§ 1. Alle personer over 18 år, samt virksomheder skal anvise en konto i et pengeinstitut ("NemKonto"), hvortil offentlige myndigheder med frigørende virkning kan foretage udbetaling af pengebeløb, medmindre de berørte har anvist en anden konto, hvortil udbetaling kan finde sted. (…)"

Udbetalinger via NemKonto-systemet gør det muligt at afsende såkaldte "ukomplette" betalingsoplysninger fra udbetalingssystemet. Det vil sige at man kan adressere betalingens modtager med en enkelt identifikator, givet ved enten CPR- CVR, SE eller P-nummer.

I NemKonto påføres bankkonto registreringsnummer og kontonummer for den bankkonto, som modtageren har registreret som NemKonto. Således behøver udbetalingssystemet ikke at afsende komplette betalingsdata til Nemkonto, sådan som det aktuelt gør sig gældende, hvis der i stedet anvendes udbetaling direkte til pengeinstitutter.

Dette betyder reduktion af ressourcer til vedligeholdelse af korrekte oplysninger vedrørende bankkonti i det afsendende udbetalingssystem og dermed en tilsvarende reduktion i antallet af fejludbetalinger.

NemKonto kan levere op til 7 forskellige retursvar fra Nemkonto og bank retur til udbetalingssystemet. Dette giver mulighed for en detaljeret historik over udbetalingens rejse fra overførsel til NemKonto til modtagelse på borgerens eller virksomhedens bankkonto.

Loven om offentlige betalinger gælder kun for danske personer og virksomheder. Det er derfor nødvendigt med bankoplysninger for offentlige udbetalinger til udenlandske kreditorer. Disse komplette oplysninger kan ligeledes sendes via

NemKonto, hvor det således stadig er muligt at modtage retursvar fra banken angående status for den pågældende udbetaling.

Generisk implementering
Udveksling af udbetalinger og retursvar med NemKonto kan foregå gennem tre forskellige teknologier:

Websphere MQ Series fra IBM, er et Message Queue produkt fra IBM. Message Queue er en teknologi til asynkron udveksling af dokumenter. Man kan benytte den gratis klient version hvis man har under 25.000 betalinger om året. Ellers skal man benytte server versionen, som ikke er gratis. I begge tilfælde er man bundet af produktet fra IBM.

VANS leverandør, som kan videresende data til NemKonto. VANS står for Value Added Network Service og er et lukket netværk, som fungerer som bindeled mellem samhandelspartnere og evt. andre VANS.

NemHandel, hvor NemKonto er et registreret end point. NemHandel er en teknologi, som gør det muligt at sende forretningsdokumenter nemt og sikkert på RASP[9] protokol via internettet, og som samtidig sikrer, at dokumenterne kan læses af modtagerens it-systemer. Dokumenterne sendes krypteret, og afsender modtager en teknisk kvittering, når dokumenterne er nået frem til modtagers server. Nemhandelsnetværket består af en række webservice end points og et register over end points. Hver enkelt dokumentmodtager udstiller en webservice og registrerer adressen på webservicen i NemHandelsregister (NHR). Dokumentafsendere kan derfor slå op på NHR og finde webservice adressen på den ønskede modtager.

Dokumentformatet for udbetalinger og retursvar er OIOXML og er det samme format for alle tre udvekslingsteknologier.

Uanset valgt udvekslingsteknologi skal man sende betalingsordrer til NemKonto i bundter og være i stand til at modtage retursvar fra NemKonto igennem tilsvarende teknologi.

Reference Implementering
Udbetaling via NemKonto er f.eks. implementeret i Navision Stat således at en betaling, der ønskes udført via NemKonto-Systemet (NKS) genererer en XML-fil, der gennem en sikker forbindelse via Nemhandelsnetværket sendes til NemKonto-systemet (Webservice). Dette sikrer, at data ikke kan tilgås af uvedkommende, da NemHandel via RASP er defineret både pålideligt og sikkert.

Efter afsendelse af udbetalingsdata fra Navision Stat, kompletteres ukomplette udbetalingsdata hos NKS for kobling af bankkonto (udvalgt som NemKonto)

---

[9] Reliable Asynchronous Secure Profile.

forud for videreaflevering til Danske Bank til behandling. Danske Bank afsender retursvar til NKS om status for udbetalingen (inklusiv eventuel afvisning), som sendes videre tilbage til Navision Stat. Disse retursvar danner basis for den videre behandling, logning og eventuel ændring af status for betalingen i Navision Stat, hvorfor det for Navision Stat er valgt at implementere modtagelse for samtlige typer af retursvar. F.eks. modtages information omkring hvilke data der er blevet tilføjet betalingen i NemKonto inden videreforsendelse til Danske Bank.

Kommunikation med NemKonto benytter samme kommunikationskomponent, som Navision Stat benytter ved NemHandel i øvrigt. F.eks. ved afsendelse og modtagelse af forretningsdokumenter som faktura, kreditnota, rykkere og kontoudtog.

De enkelte betalingsordrer og de tilhørende retursvar gemmes i Navision Stat, hvor de kobles til den pågældende betalingspost. Der er således fuld historik i Navision Stat for hver betalingspost, og sagsbehandleren behøver ikke at anvende andre programmer i sagsbehandlingen. Fra Navision Stat er der opslag via Elektronisk Arkiv til en loggingdatabase, som lagrer de originale XML-dokumenter. De kan vises enten i original XML-tekst eller i en brugervenlig version dannet med XML stylesheet.

Der er realtidsopdatering af betalingsposterne i Navision Stat, idet de opdateres lige så snart der modtages retursvar fra NemKonto igennem Nemhandelsnetværket.

6. Tekniske krav

Minimumskravene klassificeret som tekniske krav omhandler krav, der gør systemerne mere robuste overfor eksterne trusler og angreb

Fælles for de tekniske krav er, at de medvirker til en fuldstændighed i de sikkerhedstiltag, der implementeres, og sikrer at alle led i kæden er stærke. De tekniske krav styrker således troværdigheden og gyldigheden af alle de øvrige krav og kontroller, der implementeres i systemet, ved at sikre dataintegriteten. Særligt gælder også, at de tekniske krav især styrker sikring af data jf Persondataforordningens artikel 5 om beskyttelse med uautoriseret behandling af data, da betalingsdata kan indeholde fortrolige personoplysninger.

6.1 Overholdelse af de tekniske minimumskrav, jf. SikkerDigital.dk

Formål
Det giver ingen mening af beskrive minimumskrav til selve løsningsarkitekturen, uden at sikre, at de tekniske minimumskrav for statslige myndigheder samtidigt er opfyldt.

Generisk Implementering
De ufravigelige krav fremgår af

Sikkerdigital.dk: Tekniske minimumskrav

Her er det ligeledes anført at:

- Som led i den nationale cyber- og informationssikkerhedsstrategi er det besluttet, at de statslige myndigheder skal efterleve en række tekniske minimumskrav med henblik på at sikre et højt fælles sikkerhedsniveau i staten. Disse krav trådte i kraft fra den 1. juli 2020.

- Kravene er minimumskrav, som ikke fritager myndighederne fra at foretage egne risikovurderinger og implementere yderligere sikkerhedstiltag i relevant omfang. For størstedelen af myndighederne vil en lang række af kravene allerede være helt eller delvist opfyldt.

I forbindelse med anskaffelse af nye, eller videreudvikling af eksisterende, systemer, er der således afgørende, at få kontrolleret, at applikationen kan afvikles under de rammer, som de tekniske minimumskrav definerer.

Det kan eventuelt overvejes at få skrevet direkte ind i udbudsmaterialet, at en ny løsning skal kunne afvikles med en overholdelse af alle aftalte SLA-mål, under de - til enhver tid - gældende tekniske minimumskrav.

Referenceimplementering
For Navision Stat sikres overholdelsen af de tekniske minimumskrav i et samarbejde med Statens IT (SIT), hvor SIT både er desktopleverandør og hostingleverandør og KMD (som hostingleverandør).

6.2 Kryptering af betalingsdata ved udveksling

Formål
At sikre fortrolighed og integritet af data, samt autenticitet mellem de to kommunikerende parter under udveksling af betalingsdata.

Generisk Implementering
Trafikken af betalingsdata, system til system, over et netværk skal som minimum linjekrypteres og signeres. Ved endelig afsendelse til pengeinstitut eller NemKonto, ligger ansvaret for anvendt sikkerhedsprotokol hos denne tredjepart. Trafik mellem systemer inden for ens egen forvaltning, f.eks. mellem betalingsafledende system(er) og udbetalingssystem, har man selv ansvaret for overholder minimumskravet for kryptering.

Der skal ved filoverførsler systemer imellem anvendes en sikkerhedsprotokol, der kan understøtte sikker kommunikation, ved at opstille en kanal, som data kan flyde sikkert igennem. Den hyppigst anvendte og anbefalede protokol er TLS[10], der blandt andet anvendes ved https og ftps[11] overførsler.

Ved anvendelse af TLS, skal der altid ske en implementering af nyeste version., da protokollen er i konstant udvikling, hvorved identificerede nye usikkerheder bliver elimineret.

TLS protokollen sikrer overførsel af data ved at opsætte en sikker kommunikationskanal. Følgende sikkerhedsforanstaltninger anvendes:

- Fortrolighed: Data er krypteret så det ikke kan aflæses under udvekslingen, f.eks. ved et man-in-the-middle angreb.
- Autenticitet: De to kommunikerende parter autentificeres over for hinanden ved at anvende et SSL/TLS certifikat udstedt af en anerkendt certifikatmyndighed (CA[12]).

---

[10] Transport Layer Security
[11] File Transfer Protocol Secure
[12] Certificate Authority (Anerkendt certifikatmyndighed, der udsteder certifikater til organisationer og private)

- Integritet: Data bliver signeret med en autentificeringskode, som bliver verificeret af modtageren. Hvis data har ændret sig undervejs vil koderne ikke stemme overens og dermed ikke kunne verificeres.

Et kendt alternativ til TLS er SSH protokollen, der eksempelvis anvendes ved sftp overførsler. SSH protokollen sikrer data på samme måde som TLS, der er dog den nævneværdige forskel, at SSL/TLS certifikater er knyttet til et rodcertifikat, der er udstedt af en anerkendt certifikatmyndighed. SSH certifikater selvsigneres og dannes altså af modtageren selv. Dette flytter altså tillidsforholdet væk fra en anerkendt tredjepart(CA), til modtageren selv. Det betyder også, at nøglerne ved SSH protokollen, skal udveksles på en sikker måde manuelt i stedet for via en PKI service. En TLS sikret forbindelse kan dog også etableres med et selvsigneret certifikat, det er dog ikke tilladt at anvende disse med TLS.

Såfremt de endelige udbetalingsdata ikke sendes direkte til f.eks. NemKonto eller pengeinstitut, men i stedet afleveres hos et eller flere mellemled, skal der etableres en komplet end-to-end kryptering, der sikrer data, ikke bare under overførsel, men også helt frem til tiltænkte modtager. Her krypteres ikke kun trafikken, men også det faktiske payload[13].

Jævnfør ISO standard 27002 10.1.1 skal beslutninger omkring kryptografiske løsninger anses som en del af den mere omfattende proces i relation til risikovurdering og valg af kontroller. Der bør ligeledes indhentes ekspertbistand ved udvælgelse af passende kryptografiske kontroller og for at undgå uhensigtsmæssig eller ukorrekt anvendelse.

Reference implementering
Den direkte integration mellem Navision Stat og Danske Bank er eksempelvis opsat ved at banken udstiller en webservice (Danske Bank WebService) over https, der anvender TLS 1.2 sikkerhedsprotokollen. Bankens rodcertifikat er tilføjet til NS applikationsserverens trusted store, og dette rodcertifikat er udstedt gennem en CA der ligeledes er trusted. Nøglerne udveksles gennem en PKI service hostet af Danske Bank.

Et andet eksempel kan være integrationen mellem Navision Stat og NemKonto for ukomplette betalinger, hvor betalingsdata sendes via en lignende sikker forbindelse, og NemKonto herfra overtager ansvaret for sikker opbevaring, og videre sikker afsendelse af de komplette betalinger til tiltænkt bankcentral.

Tredje eksempel er fagsystemer og udbetalingssystemer imellem, hvor fagsystemer danner grundlag for det betalingsdata der sendes afsted fra udbetalingssystemet. På Navision Stat findes flere af sådanne integrationer, der alle integrerer via den Generiske Integrationssnitflade (GIS). Med GIS er det muligt at sende via webservice der anvender TLS, men det er også muligt at anvende en fil/mappe

[13] Pakken/Betalingsfilen indeholdende betalingsdata der sendes over et netværk.

struktur løsning. Her placeres GIS-filer i en dedikeret importfolder på serveren via f.eks. en SFTP eller FTPS løsning. Helt konkret kan nævnes integrationen imellem RejsUd og Navision Stat, hvor rejseafregninger bliver sendt fra RejsUd via filoverførsel med SFTP.

6.3 Blokering for SQL-injektion

Formål
Formålet med dette minimumskrav er at sikre datas fortrolighed og integritet ved at beskytte i mod eksterne såvel som interne SQL-injektion angreb.

Hvis et system er sårbart over for SQL-injektion giver det mulighed for at data kan kompromitteres, og altså enten lækkes, modificeres eller slettes. Angrebene kan komme udefra, hvis en grænseflade er offentligt udstillet (enten forsætligt eller via uberettiget adgang), men angrebet kan også komme indefra. SQL-injektion angreb kan således være særligt farlige, hvis angriberen har et indgående kendskab til datamodellen og løsningsarkitekturen bag et givent system. Det er imidlertid muligt for angriberen at tilegne sig viden om netop datamodellen ved at udføre SQL-injektion.

Hvis udført rigtigt kan SQL injektion, f.eks. i et system der foretager udbetalinger, bruges til at få adgang til følsomme oplysninger, som kontonumre og persondata. Det kan også bruges til at få kendskab til den datamodel, der ligger til grund for udbetalingen. På den måde kan man opnå viden omkring, hvordan data kan ændres til at snyde med eksempelvis udbetalinger. F.eks. kan der indsættes ekstra rækker med betalingsdata, eller kontonumre og beløb kan ændres på allerede oprettede datarækker. Et veludført angreb kan til sidst også bruges til at slette sine spor ved at slette data i post- eller logtabeller.

Andre typer af injektion-angreb
Det er værd at bemærke, at der findes flere forskellige typer af injektion-angreb. SQL-injektion er dog et af de mest udbredte og offentligt bekendte angreb, og da man for langt de fleste systemer anvender en arkitektur der bygger på underliggende databaser, er det derfor også et af de vigtigste angreb at kende til, og beskytte sig imod.

Dog vil det, alt afhængig af det pågældende system og hvilke grænseflader der udstilles i det, være nødvendigt, at sikre sig i mod flere af disse injektion-angreb. Dette gøres, ligesom med SQL-injektion, ved at validere input fra sine grænseflader og sikre snitfladerne imellem interne systemer, ved at anvende anerkendte kodemønstre, der beskytter imod disse forskellige typer af angreb.

Generisk Implementering
SQL-injektion angreb foretages via de grænseflader hvor et system modtager input til databehandling. Det kan være alt fra et simpelt tekstfelt, til et udstillet

API. Al input der i systemet bliver gemt eller anvendt til at behandle data, og dermed indsættes i en query, der afvikles på databasen, er sårbart.

Ved hjælp af angrebet snydes systemet til at afvikle en utilsigtet databehandling. Kernen i at sikre i mod injektion angreb, er at validere al input der sendes ind i systemet. For SQL-injektion angreb kan dette gøres på flere måder.

- Anvend parametriserede query kald til SQL-databasen.
  Den nok mest anbefalede strategi for beskyttelse mod SQL-injektion er at parametrisere sine queries til databasen. På denne måde sikres det at input ikke ændrer ved selve databehandlingen (eller formålet med den givne query), da en query, forberedt på denne måde, aldrig kan ændre sig fra f.eks. en SELECT til en UPDATE eller TRUNCATE. SQL serveren vil behandle alle parametre, som det de er tiltænkt, og man kan aldrig få serveren til at afvikle det, som en anden query.
  De fleste SQL kode-biblioteker understøtter opbygning af queries med parametriserede kald (Ofte kaldet placeholders eller binding).

- Validere input for utilsigtede tegn.
  En anden metode går på at validere det input man får i systemet (ofte kaldet ”sanitize”). Data kan valideres på flere måder f.eks. ved at fjerne alle utilsigtede tegn via ”escaping”. Dette kan f.eks. være et semikolon der i SQL benyttes til at afslutte et statement. En anden måde kan være at tjekke data op i mod nogle indbyggede mønstre, som f.eks. at et forventet dato input kan valideres til en dato, eller at et tekstfelt kun indeholder alfanumeriske tegn.

Man skal som minimum beskytte sig med én af de to ovennævnte (og helst begge) metoder.

Det vigtigste, og formålet med kravet, er at SQL-injektion bliver taget højde for og bliver blokeret. Man skal derfor også teste specifikt imod SQL-injektion, enten vha. tredjepartsværktøjer, eksterne uvildige testere eller egen test.

Referenceimplementering
I Navision Stat har man valgt at anvende parametriserede query kald og altså dermed forberedte query statements, der sikrer at formålet og behandlingen af data ikke uventet kan ændres via de input/parameter, der anvendes i querien.

Navision Stat udviklingsenheden 2021

oes.dk