Spillemyndigheden

Tekniske krav – Monopol

Denne vejledning indeholder beskrivelse af tekniske krav til spiludbydere, som har en tilladelse til at udbyde monopolspil.

Version 1.0

Indhold

1. Indledning

Formålet med dette dokument er at beskrive de tekniske krav, der bliver stillet til spiludbydere, som har tilladelse til at udbyde – monopolspil. Kravene er beskrevet i forhold til de systemer, der skal anvendes i forbindelse med Spillemyndighedens tilsyn med tilladelsesindehaver. Dvs. tilladelsesindehaverens datalager (SAFE), sikkerhedssystemet TamperToken og Register Over Frivilligt Udelukkede Spillere (ROFUS).

Tilladelsesindehaver skal sørge for at udvikle deres spilsystem, så det kan anvende grænseflader til Spillemyndighedens systemer. På denne måde kan Spillemyndigheden behandle data og føre tilsyn med at online spil foregår i overensstemmelse med lovgivningen. Det er et krav, at tilladelsesindehaver anvender de specificerede grænseflader til Spillemyndighedens systemer, som Spillemyndigheden har udviklet til formålet, og at tilladelsesindehaver etablerer en SAFE, som de giver Spillemyndigheden adgang til.

I de næste afsnit vil de tekniske krav blive beskrevet nærmere. Kravene er grupperet i forhold til, hvilket system de tilhører.

Foruden at opfylde kravene i dette dokument skal spiludbydere, der søger om tilladelse til at udbyde monopolspil i Danmark leve op til Spillemyndighedens certificeringsprogram som findes på spillemyndigheden.dk.

1.1 Regelgrundlag

Lovgrundlaget for denne vejledning er spilleloven samt Danske Lotteri Spil A/S' (DLO) og Det Danske Klasselotteri A/S' (KL) tilladelser.

DLO og KL skal hver især overholde de tekniske vilkår, som står skrevet i deres tilladelser jf. spillelovens §32.

Tilladelserne kan findes på spillemyndigheden.dk under "Lotteri – monopoler" og "Liste over tilladelsesindehavere.

Manglende overholdelse af kravene er strafbelagt.

1.2 Versionshistorik

Version	Dato	Kort beskrivelse af ændring
1.0	06.07.2020	Denne vejledning erstatter en række tidligere dokumenter om tekniske krav til spiludbydere og er ved denne version målrettet monopolspil. Krav til opbevaring af data er præciseret.

2. Overordnet beskrivelse af det tekniske setup

Det samlede systemkompleks består af tilladelsesindehavers spilsystem, tilladelsesindehavers datalager (SAFE), et sikkerhedssystem (TamperToken), og Register over frivilligt udelukkede spillere (ROFUS).

SAFE er tilladelsesindehavers eget datalager (en filserver), hvor tilladelsesindehaver skal opbevare data for alle spil, der er udført hos tilladelsesindehaver. Alle tilladelsesindehavere skal etablere et SAFE, og Spillemyndigheden skal kunne få online adgang hertil. Spildata skal overholde kravene beskrevet i "Spillemyndighedens krav til rapportering af spildata på monopolspil".

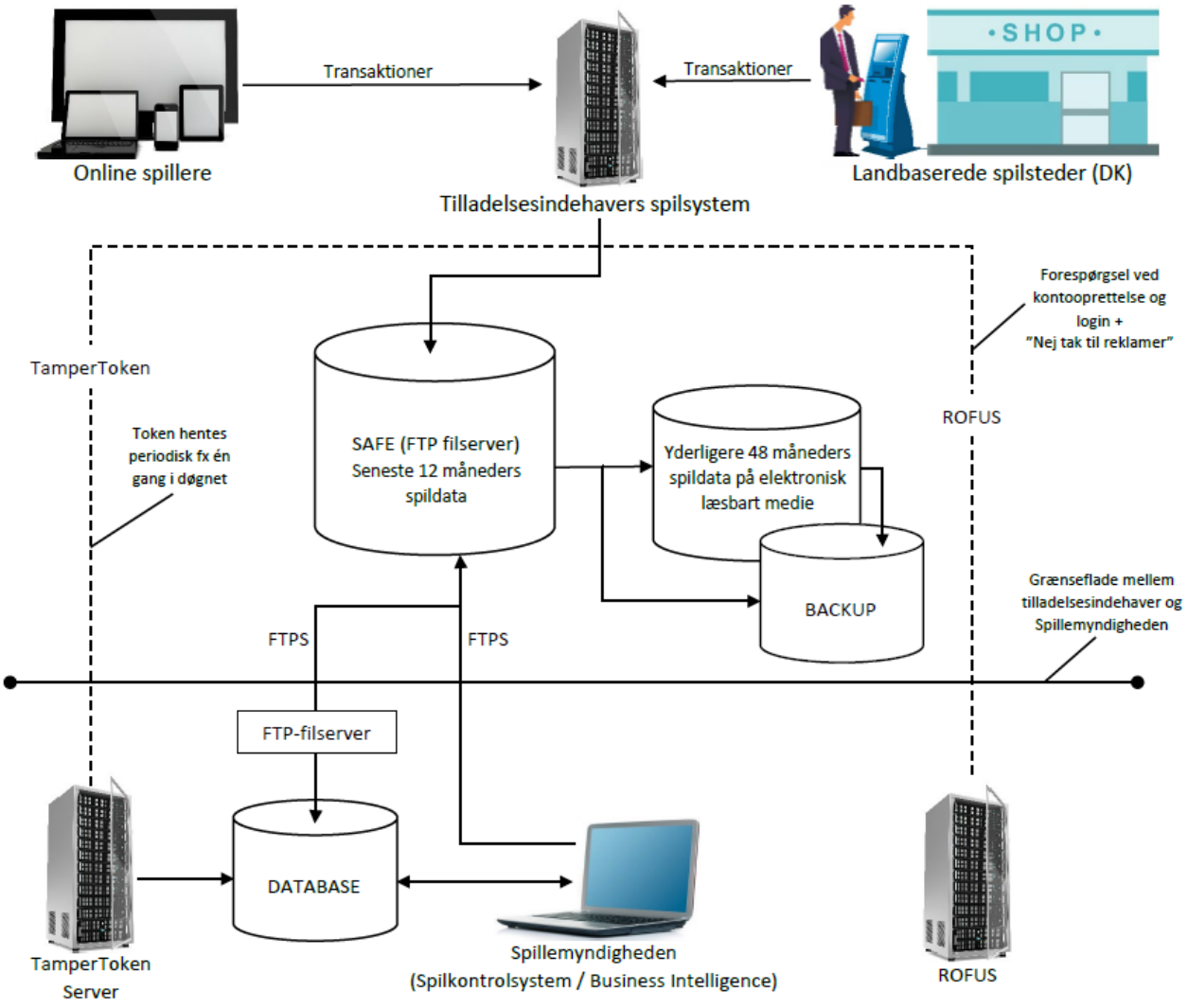
TamperToken er et sikkerhedssystem, der har til formål at sikre at de data, som tilladelsesindehaver lægger i deres SAFE ikke ændres mens de opbevares hos tilladelsesindehaver.

ROFUS er et register over spillere i Danmark, der frivilligt har udelukket sig – midlertidigt eller endeligt – fra at kunne spille online spil i Danmark. Registret er placeret hos Spillemyndigheden, der har ansvaret for at føre registret.

Disse tre systemer udgør tilsammen det tekniske grundlag for at tilladelsesindehavere lovligt kan udbyde online spil i Danmark og kan dokumentere, at de lever op til lovens krav.

2.1 Visuel fremstilling

Det samlede systemkompleks kan illustreres på denne måde:



3. SAFE

I forbindelse med opnåelse af tilladelse til at udbyde monopolspil skal der etableres et datalager (SAFE), som tilladelsesindehaveren skal anvende til at rapportere spildata til.

SAFE etableres af tilladelsesindehaveren. Tilladelsesindehaveren kan anvende en leverandør til etablering og drift af deres SAFE. Tilladelsesindehaver er til enhver tid ansvarlig for drift af deres SAFE.

3.1 Krav til tilgængelighed og forbindelse til SAFE

1. SAFE skal etableres på en separat server, der er fysisk adskilt fra tilladelsesindehaverens spilsystem. Serverne må gerne stå i samme datacenter.

2. Data på SAFE skal være logisk og forsvarligt adskilt fra eventuelle andre data.

3. Tilladelsesindehaver skal sikre, at Spillemyndigheden har online adgang til at hente spildata fra SAFE. Der skal være en garanteret oppetid på minimum 98,5 % målt pr. måned.

4. SAFE skal være konfigureret i UTC tid, så tidsstempler på filer[1] og mapper er angivet i UTC tid.

5. Dataoverførsel skal ske over internettet med FTPS/Implicit SSL i passiv mode på port 990. Genbrug (reuse) af SSL-forbindelse må ikke anvendes. Tilladelsesindehaver skal etablere passende forbindelse, der sikrer en uproblematisk overførsel af data.

6. For at Spillemyndigheden kan tilgå SAFE med FTPS skal tilladelsesindehaver placere et certifikat på FTPS-forbindelsen. Certifikatet skal være udstedt af en Certificate Authority.

7. For at Spillemyndigheden kan tilgå SAFE, skal tilladelsesindehaver åbne for adgang fra disse IP-adresser:
   - 84.255.109.80
   - 84.255.109.85
   - 84.255.109.86
   - 91.230.68.13
   - 91.230.68.190
   - 185.151.193.16
   - 185.151.193.17
   - 185.151.193.18
   - 185.151.193.19
   - 185.151.193.20
   - 185.151.193.21
   - 185.151.193.22
   - 185.151.193.23
   - 194.239.239.10
   - 194.239.239.30
   - 194.239.239.31
   - 194.239.239.32
   - 194.239.239.33
   - 194.239.239.34

8. Spillemyndigheden skal kunne tilgå SAFE med FTPS/Implicit SSL i passiv mode på port 990. Som dataporte skal anvendes et portspænd mellem 40.000 og 50.000. Tilladelsesindehaver kan anvende et mindre portspænd, så længe det ligger inden for de to grænser. TLS-resuming må ikke være aktiveret på FTP-serveren.

[1] Se desuden specifikke krav i "Spillemyndighedens krav til rapportering af spildata på monopolspil", som kan findes på spillemyndigheden.dk

3.2 Krav til opbevaring og backup af data

Spillemyndigheden skal have online adgang til seneste 12 måneders spildata. Yderligere 48 måneders spildata skal opbevares på elektronisk læsbart medie. For spil der løber over en periode og afsluttes via indsendelse af SlutStruktur tælles de 12 og 48 måneder fra afslutningen af det enkelte spil (draw), således alle data for hele spillet er tilgængelige i minimum 12 og 48 måneder efter spilafslutning. Tilladelsesindehaver skal på opfordring kunne levere arkiverede spildata fra elektronisk læsbart medie til Spillemyndigheden inden for fem arbejdsdage.

Tilladelsesindehaver skal sørge for nødvendig backup af alle data. SAFE og backup af SAFE skal være geografisk adskilt, ligeledes skal dataopbevaring på digitalt læsbart medie være geografisk adskilt fra backup af samme.

Med "geografisk adskilt" skal forstås at serverne til SAFE og backup SAFE ikke må stå i samme datacenter.

3.3 Krav til mappestrukturen på SAFE

Tilladelsesindehaver skal opbygge SAFE ud fra denne struktur, og navngive Standard Records ud fra følgende struktur.

Navnene på mapperne er ”case-sensitive”, så det præcise navn skal anvendes:

Niveau 1: Den yderste mappe navngives ”folderstruktur-spilsystem”.

Niveau 2: Her er én mappe, som navngives ”Zip”.

Niveau 3: Her er mapper for hver dag, navngivet efter datoen i formatet YYYY-MM-DD.

Niveau 4: Her ligger et antal zip-filer, som hver knytter sig til én token. Desuden ligger mapper for de tokens som endnu ikke er lukkede. En mappe som endnu ikke er lukket navngives: SpilCertifikatIdentifikationTamperTokenID. Zip-filen som indeholder mappen navngives SpilCertifikatIdentifikationTamperTokenID.zip.

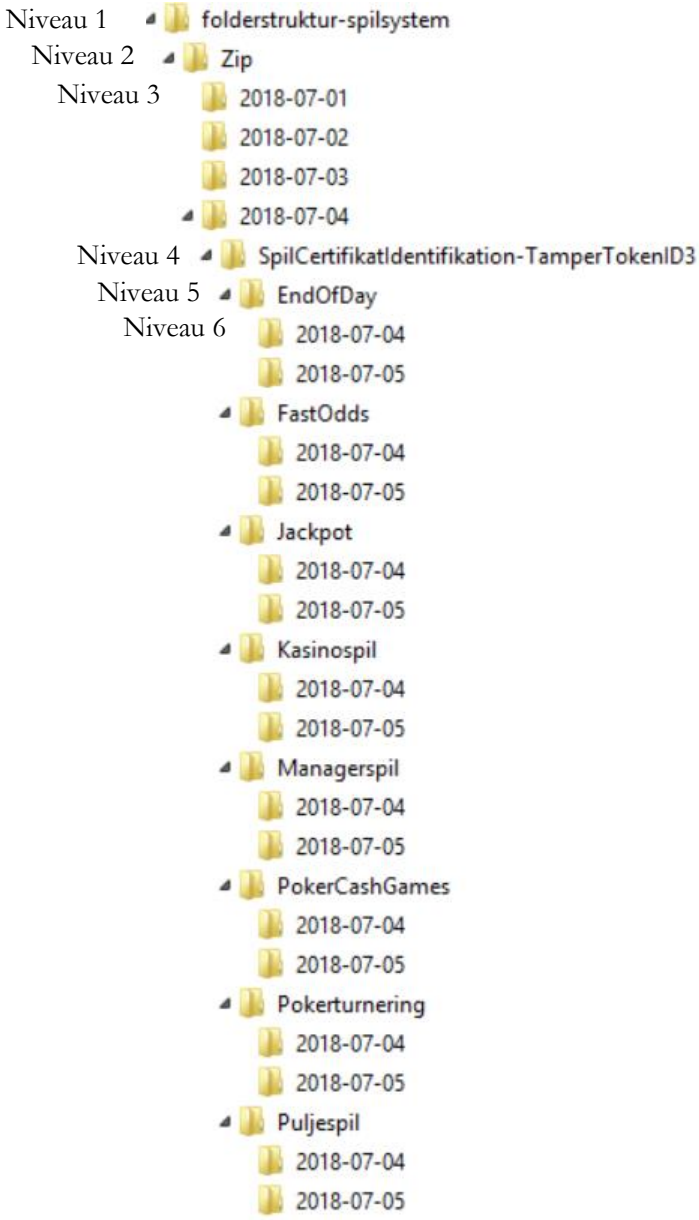
Niveau 5: Her er de mapper som hver enkelt zip-fil indeholder. De navngives eksempelvis: ”Talspil”, ”Fysisk Skrab”, ”Netskrab”, ”EndOfDay”, ”Landedata” og ”Lodtraekning”.

Niveau 6: Her er mapper for de relevante datoer, navngivet efter datoen i formatet YYYY-MM-DD. De enkelte Standard Records placeres på dette niveau eller niveau 7, og placeres i den folder der matcher det tidspunkt hvor filen oprettes. Datoen findes i

”TamperTokenUdstedelseDatoTid”, som returneres ved service-kaldet TamperTokenHent.

Niveau 7 (Valgfri): Der er mulighed for at angive undermapper med tidsintervaller i formatet HH.MM-HH.MM.

Visuel fremstilling af mappestruktur:



3.3.1 Navngivning af Standard Records og zip-filer

Både Standard Records og zip-filer på SAFE skal følge denne navngivning:

Standard Records navngives på følgende måde:
SpilCertifikatIdentifikation-TamperTokenID-SequenceInToken.xml. Standard Records skal gemmes som xml-filer.

Zip filerne navngives på følgende måde:
SpilCertifikatIdentifikation-TamperTokenID.zip

Forklaring til navngivning:

SpilCertifikatIdentifikation:	Tekststreng som tildeles af Spillemyndigheden til tilladelsesindehaver i forbindelse med ansøgningsprocessen. Dette vil være lig med det brugernavn tilladelsesindehaver får til TamperToken systemet.
TamperTokenID:	Identifikation på den enkelte TamperToken, som modtages ved at kalde operationen TamperTokenHent i servicen TamperTokenAnvend.
SequenceInToken:	Et løbenummer, der løber fra 1 og afsluttes med E for "End" (1, 2, 3,…,E) og angiver den rækkefølge de enkelte Standard Records indgår i MAC algoritmen for den enkelte token. Det er tilladelsesindehavers opgave at bygge en mekanisme til generering af sekvensen.

Eksempel:
SpilCertifikatIdentifikation = DLOLoerdagsLotto
TamperTokenID = 1234567
SequenceInToken = 3

Standard Record filen skal have følgende navn DLOLoerdagsLotto-1234567-3.xml. Zip-filen som indeholder denne Standard Record skal have filnavnet DLOLoerdags-Lotto-1234567.zip.

3.4 Krav til pakning af data på SAFE

For at spare diskplads for tilladelsesindehaver og Spillemyndigheden og for at simplificere overførsel af filer skal Standard Record filer løbende komprimeres i zip-filer. Zip-filerne skal pakkes på følgende måde:

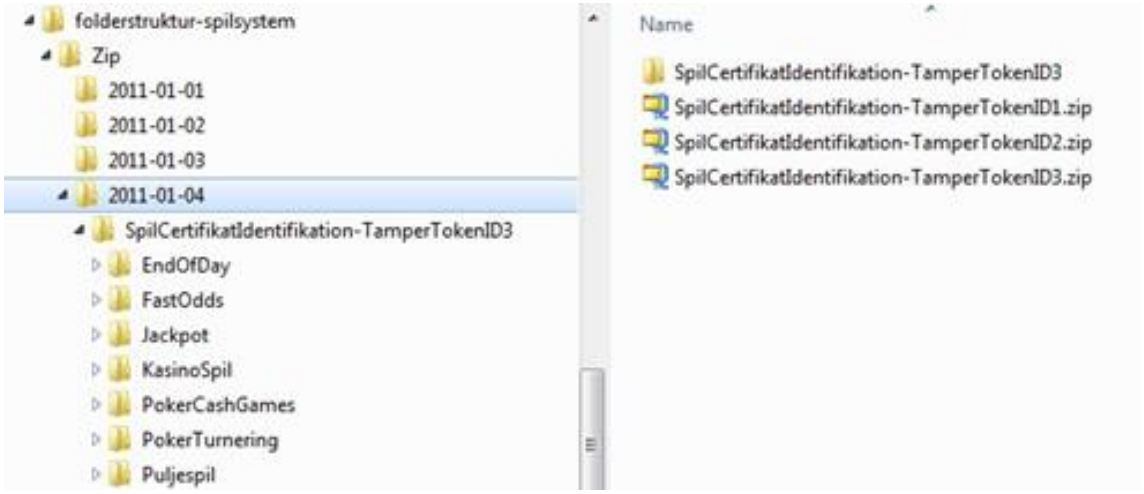
Når Standard Record filerne for en token gemmes, skal der ske følgende:

1. MAC algoritmen køres på hver enkelt fil, som angivet i afsnit 5 - Mekanisme til generering af MAC.
2. Standard Recorden gemmes i mappestrukturen for den relevante token.
3. Standard Recorden tilføjes til zip-filen for den relevante token.

Når token lukkes og alle Standard Record filer er tilføjet zip-filen, slettes den mappe som matcher zip-filen. Det er tilladelsesindehaverens opgave og ansvar at bygge en mekanisme til at sikre at disse tre trin udføres korrekt.

Ovenstående trin kan illustreres med følgende eksempel:
På figuren nedenfor ses det at mappen 2011-01-04 har to lukkede tokens som knytter sig til zip-filerne: SpilCertifikatIdentifikation-TamperTokenID1.zip og SpilCertifikatIdentifikation-TamperTokenID2.zip, samt én åben token som knytter sig til SpilCertifikatIdentifikationTamperTokenID3.zip.

Det ses at SpilCertifikatIdentifikationTamperTokenID3.zip er åben eftersom der både eksisterer en zip-fil og en folderstruktur. De Standard Records der løbende kommer ind og knytter sig til token 3 bliver løbende gemt i folderen SpilCertifikatIdentifikationTamperTokenID3 og tilknyttes SpilCertifikatIdentifikation-TamperTokenID3.zip. Når token 3 lukkes og alle Standard Records er tilføjet zip filen, slettes mappen SpilCertifikatIdentifikation-TamperTokenID3.



3.4.1 Valg af dato mappe for zip-fil

Som beskrevet i afsnittet ovenfor skal zip-filerne placeres under niveau 3 i folderstrukturen på SAFE. Niveau 3 består af mapper med datoangivelse, og zip-filen skal placeres under rette dato.

Zip-filen skal placeres under den udstedelsesdato, der gælder for token. Udstedelsesdatoen findes i svaret fra serviceoperationen TamperTokenHent og er de første 10 karakterer i elementet TamperTokenUdstedelseDatoTid.

I eksemplet nedenfor angives værdien **2011-10-16T15:21:19.221+02:00** i elementet **TamperTokenUdstedelseDatoTid**. Den zip-fil, som bygges med denne token, skal således findes på SAFE under stien folderstruktur-spilsystem/Zip/2011-10-16/.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header/>
  <env:Body>
    <ns:TamperTokenAnvend_O xmlns:ns="http://skat.dk/begrebsmodel/2009/01/15/">
      <ns:Kontekst>
        <HovedOplysningerSvar xmlns="http://skat.dk/begrebsmodel/xml/schmas/kontekst/2007/05/31/">
          <TransaktionsID>895ffb40-9f4a-11e0-8264-0800200c9a66</TransaktionsID>
          <ServiceID>TamperTokenAnvendService</ServiceID>
          <TransaktionsTid>2011-06-25T18:41:30.054+01:00</TransaktionsTid>
        </HovedOplysningerSvar>
      </ns:Kontekst>
      <ns:TamperTokenHent_O>
        <ns:TamperTokenID>1234567</ns:TamperTokenID>
        <ns:TamperTokenStartMAC>91c5e2c0e033e3b18fc66bfa43bb08d4</ns:TamperTokenStartMAC>
        <ns:TamperTokenUdstedelseDatoTid>2011-10-16T15:21:19.221+02:00</ns:TamperTokenUdstedelseDatoTid>
        <ns:TamperTokenPlanlagtLukketDatoTid>2011-10-17T15:21:19.221+02:00</ns:TamperTokenPlanlagtLukketDatoTid>
  </ns:TamperTokenHent_O>
 </ns:TamperTokenAnvend_O>
</env:Body>
</env:Envelope>
```

3.5 Krav til rapportering af spildata

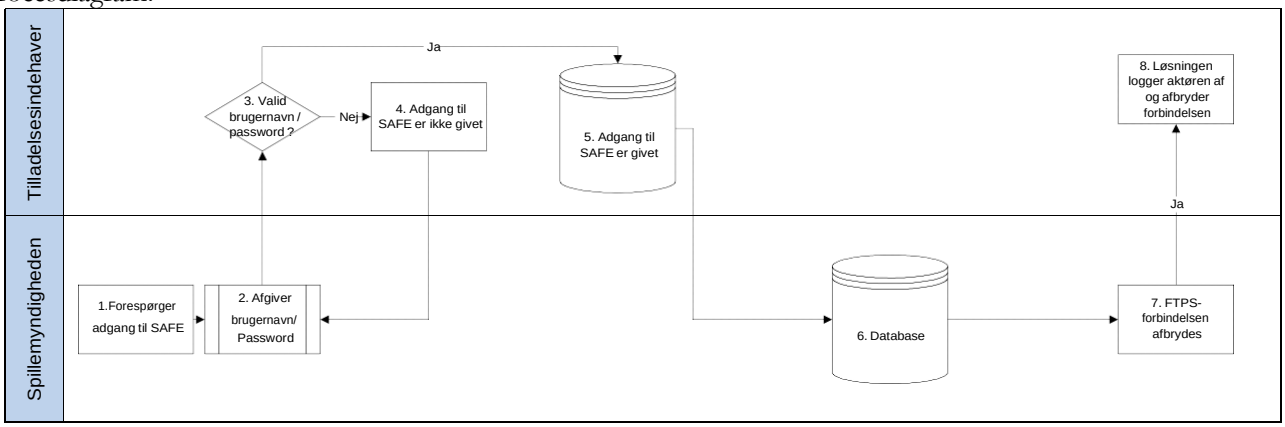
For at Spillemyndigheden kan indlæse data, som rapporteres af tilladelsesindehaverne, skal rapportering af spildata foretages ved brug af datastrukturer, som er udviklet af Spillemyndigheden.

Kravene til datastrukturerne er beskrevet i "Spillemyndighedens krav til rapportering af spildata på monopolspil", som kan findes på spillemyndigheden.dk.

3.6 Spillemyndighedens proces til at hente data

Formålet med dette afsnit er at give tilladelsesindehaver indblik i Spillemyndighedens proces i forhold til at hente data. Tilladelsesindehaver skal gøre det muligt for Spillemyndigheden at hente data fra deres SAFE som beskrevet i nedenstående proces:

Procesdiagram:



Proceskort	
Procesinteressenter	Tilladelsesindehavere og Spillemyndigheden
Formålet med processen	Formålet med processen er at sikre, at Spillemyndigheden kan hente data fra tilladelsesindehaverens SAFE til brug for tilsynet.
Processens grænseflader	FTPS/Implicit SSL i passiv mode på port 990
Input (start)	Processen starter med at Spillemyndigheden forespørger om adgang til SAFE med brugernavn og password som er udstedt af tilladelsesindehaver.
Output (slut)	Processen afsluttes med at Spillemyndigheden har modtaget de ønskede data og er logget af SAFE.

Beskrivelse af procesflow	
Nummer	Beskrivelse
1	Spillemyndigheden anmoder om adgang til SAFE
2	Spillemyndigheden angiver brugernavn og password
3	Systemet validerer brugernavn og password
4	Hvis brugernavn og password ikke er validt, afvises adgang og Spillemyndigheden sendes tilbage til punkt 2
5	Hvis brugernavn og password er validt, gives adgang til at se data på SAFE og download kan påbegyndes
6	Data overføres til Spillemyndighedens server
7	Spillemyndigheden logger af SAFE
8	SAFE logger Spillemyndigheden af

3.7 SAFE i ansøgningsprocessen

I forbindelse med Spillemyndighedens behandling af en ansøgning om tilladelse til at udbyde monopolspil skal følgende trin gennemføres:

1. Ansøgeren udfylder punkter vedrørende SAFE i til ansøgningen. Punkterne indeholder oplysningerne brugernavn, password, IP-adresse og eventuel URL og skal anvendes af Spillemyndigheden til at skabe forbindelse til SAFE. I forbindelse med behandling af ansøgningen tester Spillemyndigheden forbindelsen til SAFE i samarbejde med ansøger.

2. Ansøgeren skal levere testdata til Spillemyndigheden. Testdata leveres via SAFE og ved brug af TamperToken testmiljø, så data kan indlæses i Spillemyndighedens database. Kravene til omfanget af testdata inden for hver spilkategori afhænger af spiltypen. Testdata kan leveres i forbindelse med ansøgerens gennemførsel af TamperToken testcase, jf. afsnit 4 i denne vejledning.

   Når testdata er leveret og indlæst i Spillemyndighedens database foretager Spillemyndigheden en vurdering af de leverede data, så det sikres, at data overholder Spillemyndighedens krav.

3. Ansøgeren skal levere et dokument (description of attributes), hvor ansøgeren med egne ord beskriver indholdet af hvert enkelt dataelement, som indgår i de datastrukturer, som skal anvendes til rapportering af spil data. Dokumentet sendes af Spillemyndigheden til spiludbyder i forbindelse med ansøgningen.

Spillemyndigheden foretager en vurdering af de anførte beskrivelser, og eventuelle uklarheder afklares i dialog med ansøgeren.

3.8 Ændringer eller udskiftning af SAFE

Hvis en tilladelsesindehaver ønsker at foretage ændringer til den eksisterende SAFE, eller ønsker at udskifte den eksisterende SAFE skal Spillemyndigheden underrettes indenfor rimelig tid. Der skal således være tid til at foretage de nødvendige ændringer for at sikre, at forbindelsen til SAFE opretholdes efter ændring eller udskiftning. Nye IP-adresser for SAFE skal whitelistes i Spillemyndighedens system, dette kan tage op til 4 uger.

Spillemyndigheden vurderer i disse situationer i hvilket omfang der skal foretages nye tests. Det vil altid være nødvendigt at foretage handlinger for at kunne skabe forbindelse mellem tilladelsesindehaverens nye/ændrede SAFE og Spillemyndighedens system.

Til brug for Spillemyndighedens opsætning skal tilladelsesindehaver oplyse eventuelle ændringer til URL, IP-adresse og det brugernavn og password til SAFE, som tilladelsesindehaveren har tildelt Spillemyndigheden.

Tilladelsesindehaver skal sørge for at whiteliste de IP-adresser, som Spillemyndigheden forbinder fra. IP-adresserne kan findes i afsnit 3.1.

4. TamperToken

Spillemyndigheden anvender sikkerhedssystemet TamperToken, som har til formål at sikre, at data fra tilladelsesindehaver i form af Standard Records, ikke ændres mens det opbevares på SAFE hos Tilladelsesindehaver.

TamperToken håndterer følgende:

- Skabelse af tokens (nøgler), der anvendes ved beregning af Message Authentication Code (MAC)
- Opbevaringen af MACs til senere kontrol
- Løbende kontrol af at tidsperiode for afslutning af tokens overholdes. Som udgangspunkt er lukkefrekvensen for en token 24 timer medmindre Spillemyndigheden oplyser andet.
- Verifikation af at en hentet serie af Standard Records ikke er ændret ift. den modtagne MAC

Som indledning til TamperToken servicen, indeholder dette afsnit en step-by-step beskrivelse af proceduren fra åbning til lukning af en token. Detaljer om det enkelte trin i processen kan findes i særskilte afsnit. Der er henvisninger til afsnittene under punkterne i procedurebeskrivelsen.

1. Foretag servicekald til TamperTokenHent (se afsnit 4.1.1)
    a) Hvis servicekaldet ikke er succesfuldt, opretter tilladelsesindehaver et incident for at løse fejlen og fortsætter med at anvende den forrige token

b) Hvis servicekaldet er succesfuldt, returnerer kaldet følgende oplysninger: TamperTokenID, TamperTokenStartMAC, TamperTokenPlanlagtLukketDatoTid and TamperTokenUdstedelseDatoTid

2. For den første Standard Record fil anvendes TamperTokenStartMAC til at generere en MAC for filen, som navngives: SpilCertifikatIdentifikation-TamperTokenID-SequenceInToken.xml (se afsnit 4.2 om MAC mekanisme og afsnit 3.3.1 om navngivning af Standard Records)

- SpilCertifikatIdentifikation er "brugernavn til TamperToken"
- TamperTokenID er et resultat fra TamperTokenHent
- SequenceInToken er et fortløbende nummer fra 1 til E ("E" for End når token lukkes)

3. Når en ny Standard Record rapporteres anvendes MAC fra den forrige fil til at generere MAC for den næste fil (se afsnit 4.2.1)

4. Efter generering af MAC tilføjes Standard Record filen (xml) til både en zip-fil og en mappe for den aktuelle token som navngives henholdsvis SpilCertifikatIdentifikation-TamperTokenID.zip (fil) and SpilCertifikatIdentifikation-TamperTokenID (mappe) (se afsnit 3.4 om placering af data på SAFE

- SpilCertifikatIdentifikation er "brugernavn til TamperToken"
- TamperTokenID er et resultat fra TamperTokenHent

5. Fortsæt med at gemme Standard Record filer på SAFE (se afsnit 3.3)

6. Gentag "trin 1" ovenfor for at åbne en ny token før der fortsættes til "trin 7", hvor den aktuelle token lukkes. På denne måde har tilladelsesindehaver altid en åben token, som kan anvendes til rapportering af data.

7. Efter det givne tidsinterval fra TamperTokenHent (TamperTokenPlanlagtLukketDatoTid), foretages kald til TamperTokenLuk servicen for at lukke token (se afsnit 4.1.1)

a) Servicekaldet foretages med TamperTokenID på den token, som tilladelsesindehaver ønsker at lukke, SpilCertifikatIdentifikation og den senest genererede MAC
    - TamperTokenID er et resultat fra TamperTokenHent
    - SpilCertifikatIdentifikation er " brugernavn til TamperToken"
b) Hvis servicekaldet ikke er succesfuldt, opretter tilladelsesindehaver et incident for at løse fejlen og begynder at anvende den nye token (åbnet i "trin 6") til datarapporteringen

8. Når token er lukket sletter tilladelsesindehaver mappen SpilCertifikatIdentifikation-TamperTokenID. Indholdet i denne mapper ligger nu i SpilCertifikatIdentifikation-TamperTokenID.zip filen.

4.1 Tekniske krav i forhold til TamperToken

Tilladelsesindehaver skal implementere TamperToken løsningen, som skal anvendes i forbindelse med rapportering af spildata.

Se afsnit 6 for oplysninger om adgang til TamperToken testmiljø.

4.1.1 Vejledning og eksempler på brug af services

Spillemyndigheden har udviklet en web service ved navn "TamperTokenAnvend", som har to operationer:

1. TamperTokenHent
   Operationen skal anvendes, når tilladelsesindehaver skal hente en token. Operationen TamperTokenHent returnerer en genereret nøgle (TamperTokenStartMAC), som skal anvendes af tilladelsesindehaver til at generere en MAC (Message Authentification Code) se afsnit 4.2.

2. TamperTokenLuk
   Operationen skal anvendes, når tilladelsesindehaver skal lukke en token efter, at data er pakket færdig i en zip fil på SAFE. Operationen returnerer en kvittering med en godkendelse eller fejlmeddelelse.

4.1.1.1 Hovedoplysninger i servicekald

Ved foretagelse af servicekald skal der anføres hovedoplysninger, som har til formål at kunne følge request og response for servicekald og for at kunne rapportere fejloplysninger.

Hoved- og fejloplysninger håndteres på samme måde for TamperToken og ROFUS. Nedenstående oplysninger kan således også findes i afsnittet om ROFUS.

Hovedoplysningerne indsættes i et "any-element" i hver service og skal følge formatet, der er specificeret i XSD-filerne for hovedoplysninger, som findes på spillemyndigheden.dk.

Hovedoplysninger i "request":
Følgende hovedoplysninger skal angives i service-kald fra tilladelsesindehaver:

- TransaktionsID:
  Tilladelsesindehaver skal generere et unikt transaktionsID for servicekaldet. Spillemyndigheden anbefaler at der anvendes standarden Universally Unique Identifier (UUID), hvor id'et består af 32 hexadecimaler præsenteret i 5 grupper separeret af tankestreger på formen 8-4-4-4-12. F.eks.: 07B2A963-26C4-47E0-B517-C7059A598DA3

- TransaktionsTid:
  Tidspunktet for transaktionen. Tidspunktet skal angives på formen YYYY-MM-DDThh:mm:ss.sTZD, hvor YYYY er år, MM er måned, DD er dag, hh er timer, mm er minutter, ss er sekunder, s er et eller flere cifre for sekunddecimaler, og TZD er tidszonen repræsenteret som Z eller +hh:mm eller –hh:mm. F.eks.: 2010-12-07T09:33:51.249+01:00.

Hovedoplysninger i "response":
Følgende hovedoplysninger returneres altid i service response:

- TransaktionsID: Samme som ovenfor
- TransaktionsTid: Samme som ovenfor.
- ServiceID: Navnet på den kaldte service.

Følgende hovedoplysninger returneres også i service response, men returneres kun, når det er nødvendigt:

- Fejl: Fejl rapporteres når et kald ikke er forløbet som forventet.
    - FejlNummer: Id-nummer for fejlen.
    - FejlTekst: Beskrivelse af fejlen.
    - Identifikation: Tekst-kode for fejlen.
    - ServiceID: Samme som ovenfor.

- Advis: Adviseringer er meddelelser, som ikke er fejlbeskeder. Det kan eksempelvis være en meddelelse om at servicekaldet er gået som forventet.
    - AdvisNummer: Id-nummer for adviseringen.
    - AdvisTekst: Beskrivelse af adviseringen.
    - Identifikation: Tekst-kode for adviseringen.
    - ServiceID: Samme som ovenfor.

4.1.1.2 Eksempler på servicekald

For at lette tilladelsesindehavers arbejde med kald af de udviklede webservices, har Spillemyndigheden udarbejdet to eksempler på kald af en service. Eksemplerne viser hvordan man, i hhv. Java og .Net, kan hente webservicebeskrivelser og kalde services med brug af HTTP basic access authentication. Desuden vises hvordan man modtager data fra servicen. Eksemplet tager udgangspunkt i kald til servicen GamblerCheck.

Spillemyndigheden har lavet følgende to eksempelfiler, som kan findes på spillemyndigheden.dk:

- Eksempel i .Net: GamblerServiceExampleClient.cs
- Eksempel i java: GamblerServiceExampleClient.java

Udover eksempelfilerne er nedenfor en række eksempler på service request og response for servicekaldene TamperTokenHent og TamperTokenLuk som tilladelsesindehaver skal kalde for at kunne åbne og lukke en token. Eksemplerne er tænkt som hjælp til tilladelsesindehavers forståelse af de servicekaldene, men det er ikke hensigten at tilladelsesindehaver skal skrive kode baseret på eksemplerne. Til dette formål henvises til XSD skemaer og WSDL-filer.

Eksempel på TamperTokenHent:

Request:

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://skat.dk/begrebsmodel/2009/01/15/">
  <soapenv:Header/>
  <soapenv:Body>
    <ns:TamperTokenAnvend_I>
```

```
        <ns:Kontekst>
          <ns1:HovedOplysninger xmlns:ns1="http://skat.dk/begrebsmodel/xml/schemas/kontekst/2007/05/31/">
            <ns1:TransaktionsID>895ffb40-9f4a-11e0-8264-0800200c9a66</ns1:TransaktionsID>
            <ns1:TransaktionsTid>2011-06-25T18:41:30.054+01:00</ns1:TransaktionsTid>
          </ns1:HovedOplysninger>
        </ns:Kontekst>
       <ns:TamperOperationValg>
         <ns:TamperTokenHent>
            <ns:SpilCertifikatIdentifikation>TamperTokenTest3</ns:SpilCertifikatIdentifikation>
          </ns:TamperTokenHent>
        </ns:TamperOperationValg>
      </ns:TamperTokenAnvend_I>
    </soapenv:Body>
  </soapenv:Envelope>
```

Response:

```
  <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Header/>
    <env:Body>
      <ns:TamperTokenAnvend_O xmlns:ns="http://skat.dk/begrebsmodel/2009/01/15/">
        <ns:Kontekst>
          <HovedOplysningerSvar xmlns="http://skat.dk/begrebsmodel/xml/schemas/kontekst/2007/05/31/">
            <TransaktionsID>895ffb40-9f4a-11e0-8264-0800200c9a66</TransaktionsID>
            <ServiceID>TamperTokenAnvendService</ServiceID>
            <TransaktionsTid>2011-06-25T18:41:30.054+01:00</TransaktionsTid>
          </HovedOplysningerSvar>
        </ns:Kontekst>
        <ns:TamperTokenHent_O>
          <ns:TamperTokenID>1234567</ns:TamperTokenID>
          <ns:TamperTokenStartMAC>a06174fd062bb397894860bd5c20aa08</ns:TamperTokenStartMAC>
          <ns:TamperTokenUdstedelseDatoTid>2011-06-25T18:47:04.481+02:00</ns:TamperTokenUdstedelseDatoTid>
          <ns:TamperTokenPlanlagtLukketDatoTid>2011-06-26T18:47:04.481+02:00</ns:TamperTokenPlanlagtLukketDatoTid>
        </ns:TamperTokenHent_O>
      </ns:TamperTokenAnvend_O>
    </env:Body>
  </env:Envelope>
```

Eksempel på TamperTokenLuk:

Request:

```
  <soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:ns="http://skat.dk/begrebsmodel/2009/01/15/">
   <soapenv:Header/>
     <soapenv:Body>
       <ns:TamperTokenAnvend_I>
         <ns:Kontekst>
          <ns1:HovedOplysninger xmlns:ns1="http://skat.dk/begrebsmodel/xml/schemas/kontekst/2007/05/31/">
            <ns1:TransaktionsID>895ffb40-9f4a-11e0-8264-0800200c9a66</ns1:TransaktionsID>
            <ns1:TransaktionsTid>2011-06-25T18:41:30.054+01:00</ns1:TransaktionsTid>
          </ns1:HovedOplysninger>
        </ns:Kontekst>
        <ns:TamperOperationValg>
          <ns:TamperTokenLuk>
            <ns:TamperTokenID>1234567</ns:TamperTokenID>
            <ns:SpilCertifikatIdentifikation>TamperTokenTest3</ns:SpilCertifikatIdentifikation>
            <ns:TamperTokenMAC>2da9fe732840bc40f05eefbace7bf03fc36e141907a8d6ce7da329fa0f1bb25c
            </ns:TamperTokenMAC>
          </ns:TamperTokenLuk>
        </ns:TamperOperationValg>
```

```
      </ns:TamperTokenAnvend_I>
    </soapenv:Body>
  </soapenv:Envelope>
```

Response:

```
  <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
    <env:Header/>
    <env:Body>
      <ns:TamperTokenAnvend_O xmlns:ns="http://skat.dk/begrebsmodel/2009/01/15/">
        <ns:Kontekst>
          <HovedOplysningerSvar xmlns="http://skat.dk/begrebsmodel/xml/schemas/kontekst/2007/05/31/">
            <TransaktionsID>895ffb40-9f4a-11e0-8264-0800200c9a66</TransaktionsID>
            <ServiceID>TamperTokenAnvendService</ServiceID>
            <TransaktionsTid>2011-06-25T18:41:30.054+01:00</TransaktionsTid>
            <SvarReaktion>
              <Advis>
                <AdvisNummer>0</AdvisNummer>
                <AdvisTekst>Token is now closed</AdvisTekst>
                <ServiceID>TamperTokenAnvendService</ServiceID>
              </Advis>
            </SvarReaktion>
          </HovedOplysningerSvar>
        </ns:Kontekst>
      </ns:TamperTokenAnvend_O>
    </env:Body>
</env:Envelope>
```

4.1.2 Fejlhåndtering for TamperToken services

TamperTokenHent:

Hvis tilladelsesindehaver ikke kan hente en ny token inden den åbentstående token kan lukkes, skal tilladelsesindehaver fortsætte med at pakke data i den åbentstående token, selvom dette kan betyde, at denne token ikke kan lukkes inden det planlagte tidspunkt.

Hvis tilladelsesindehaver ikke selv kan rette fejlen kontaktes Spillemyndigheden.

Når fejlen er rettet, kan tilladelsesindehaver hente en ny token og lukke den gamle token umiddelbart herefter.

TamperTokenLuk:

Hvis tilladelsesindehaver ikke kan lukke en token på det planlagte tidspunkt skal tilladelsesindehaver begynde at pakke data i den nye token, som bør være hentet umiddelbart inden, og derefter undersøge årsagen til fejlen.

Hvis tilladelsesindehaver ikke selv kan rette fejlen kontaktes Spillemyndigheden.

Når fejlen er rettet, kan tilladelsesindehaver lukke token.

Det er vigtigt, at data er på plads inden token lukkes, da Spillemyndigheden begynder kopiering af data fra tilladelsesindehavers SAFE i samme øjeblik en token lukkes.

4.1.3 Håndtering af ubrugte tokens

I tilfælde af at tilladelsesindehaver har åbnet en token med servicen TamperTokenHent, som alligevel ikke skal anvendes, skal tilladelsesindehaver lukke denne token ved at anvende serviceoperationen TamperTokenLuk.

I denne situation skal tilladelsesindehaver rapportere teksten "empty" i feltet TamperTokenMAC, i stedet for den beregnede MAC værdi, som almindeligvis rapporteres. Et sådan servicekald vil se således ud:

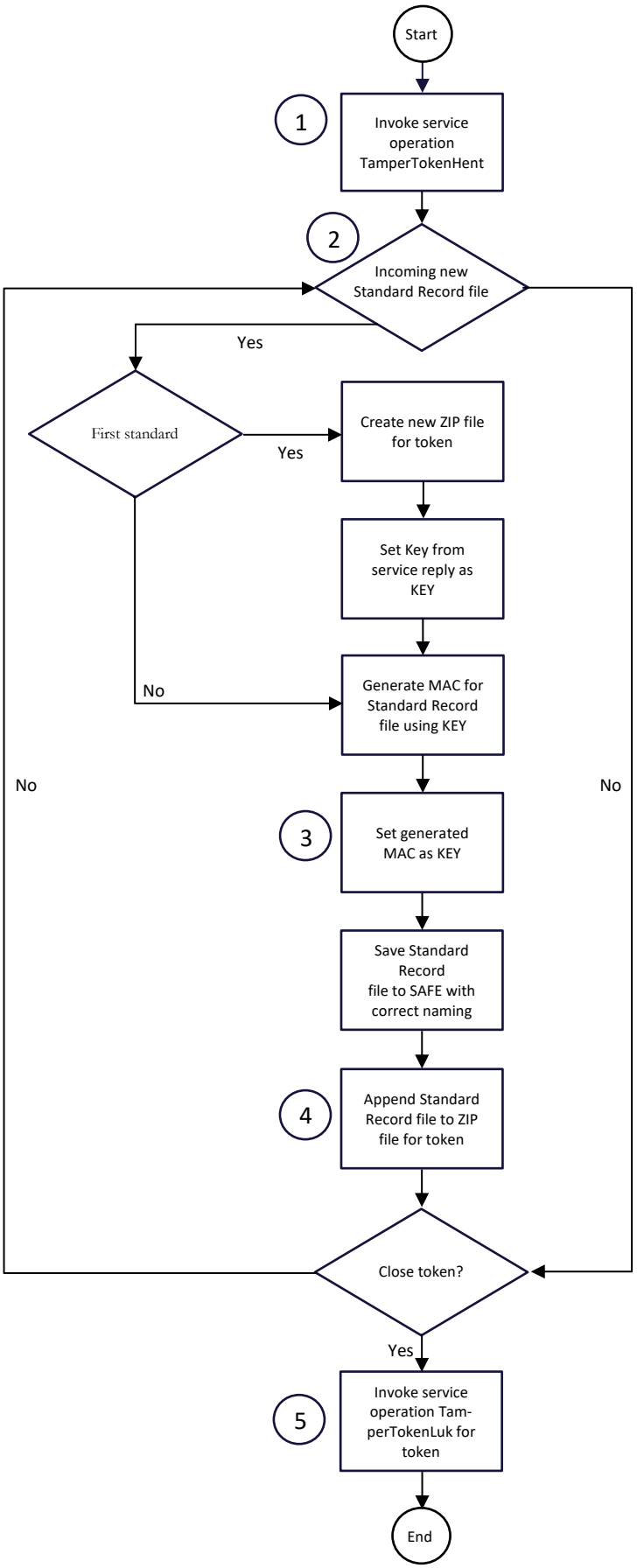
```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:ns="http://skat.dk/begrebsmodel/2009/01/15/">
    <soapenv:Header/>
    <soapenv:Body>
        <ns:TamperTokenAnvend_I>
                <ns:Kontekst>
                    <ns1:HovedOplysninger xmlns:ns1="http://skat.dk/begrebsmodel/xml/schemas/kontekst/2007/05/31/">
                    <ns1:TransaktionsID>895ffb40-9f4a-11e0-8264-0800200c9a66</ns1:TransaktionsID>
                    <ns1:TransaktionsTid>2011-10-15T18:41:30.054+01:00</ns1:TransaktionsTid>
                </ns1:HovedOplysninger>
            </ns:Kontekst>
            <ns:TamperOperationValg>
                <ns:TamperTokenLuk>
                    <ns:TamperTokenID>1234567</ns:TamperTokenID>
                    <ns:SpilCertifikatIdentifikation>TamperTokenTest3</ns:SpilCertifikatIdentifikation>
                    <ns:TamperTokenMAC>empty</ns:TamperTokenMAC>
                </ns:TamperTokenLuk>
            </ns:TamperOperationValg>
        </ns:TamperTokenAnvend_I>
    </soapenv:Body>
</soapenv:Envelope>
```

4.2 Mekanisme til generering af MAC

Dette afsnit indeholder informationer om den MAC algoritme og Application Programming Interface (API), som tilladelsesindehaver skal bygge, og som skal anvendes i forbindelse med pakning af data på SAFE.

Tilladelseshaver skal bygge en mekanisme som kan generere en MAC på den rette måde. Denne MAC skal anvendes i forbindelse med pakning af data på SAFE.

Illustration af mekanismen som skal generere MAC:



Beskrivelse af procesflow for generering af MAC	
Nummer	Beskrivelse
1	Tilladelsesindehaver aktiverer serviceoperation TamperTokenHent og modtager nyt TamperTokenID samt en nøgle (KEY), der anvendes til MAC generering for den første Standard Record fil for den nye token.
2	Når der genereres en ny Standard Record fil, genereres der en MAC af denne record.
3	Den genererede MAC bliver nu den nye KEY for den næste MAC generering.
4	Efter MAC generering tilføjes den aktuelle Standard Record til en samlet ZIP fil for det aktuelle token.
5	Når en token lukkes, aktiveres serviceoperationen TamperTokenLuk med token-ID, den senest genererede MAC samt identifikation af tilladelsesindehaveren.

4.2.1 MAC API

Til generering af MACs skal anvendes klassen SecretKeySpec fra Java 1.8.3. Nedenfor præsenteres et eksempel på hvordan koden kan se ud for trinnet "Generate MAC for Standard Record file using KEY".

For den første fil er argumentet "KEY" nøglen fra serviceoperationen "TamperTokenHent". For efterfølgende fil(er) er argumentet "KEY" MAC fra den forrige fil.

Argumentet "InputStream" indeholder data fra den Standard Record, der skal genereres en MAC ud fra.

Eksempel:

```
     public String getMAC(String key, InputStream input) throws Tam-
perTokenException {
              try {
                Mac mac = Mac.getInstance("HmacSHA256");
                byte[] byteKey = ByteArrayHandler.parseString(key);
                SecretKeySpec keySpec = new SecretKeySpec(byteKey,
                "HmacSHA256"); mac.init(keySpec);
                byte[] data =
                new
                byte[1024];
                int read;
                while((read=input.read(data)) > -1){
                     mac.update(data, 0, read);
                }
                return ByteArrayHandler.toString(mac.doFinal());
              }
          catch (Exception e) {
                     throw new TamperTokenException(e);
              }
       }
```

4.2.2 Eksempel på beregning af MAC

På Spillemyndighedens hjemmeside findes filen TamperTokenTest3-2152.zip, som er anvendt nedenfor til at give eksempel på beregning af MAC.

Eksemplet er lavet for SpilCertifikatIdentifikation = TamperTokenTest3 og TamperTokenID = 2152.

Filen TamperTokenTest3-2152.zip indeholder tre filer:
TamperTokenTest3-2152-1.xml,
TamperTokenTest3-2152-2.xml og
TamperTokenTest3-2152-E.xml.

Der trækkes en start MAC med serviceoperationen TamperTokenHent, og denne er angivet nedenfor som TamperTokenStartMAC. Herefter angiver de mellemliggende MACs, som beregnes på hver enkelt fil. MAC'en fra beregning af den sidste fil rapporteres ved serviceoperationen TamperTokenLuk i elementet TamperTokenMAC.

1. TamperTokenStartMAC =
   fb99919c20c57b01a1ab37fdc576f75a
2. MAC af fil TamperTokenTest3-2152-1.xml =
   148f1bc4bfe2be67cfed691f6a703ed90e780f45faab665b5c86a3c8346ad056
3. MAC af fil TamperTokenTest3-2152-2.xml =
   a79953be54a71069a07d2d7c63566daaab221de984d93c36ae8c7b26d149df90
4. MAC af fil TamperTokenTest3-2152-E.xml =
   1b14a1da76568ab3b96bc64bb7ee02e846fbd7711e3ce40f477b0c66a0663016
5. TamperTokenMAC =
   1b14a1da76568ab3b96bc64bb7ee02e846fbd7711e3ce40f477b0c66a0663016

5 ROFUS – Register Over Frivilligt Udelukkede Spillere

I henhold til tilladelsen er der krav om, at det skal være muligt for en spiller at udelukke sig fra at kunne spille online spil i Danmark, hvilket svarer til Bekendtgørelse om onlinekasino § 24 og Bekendtgørelse om online væddemål § 18. Denne udelukkelse kan være af midlertidig karakter, hvor spilleren udelukker sig for en vis periode, og den kan være endelig.

Spillemyndigheden er ansvarlig for at føre registeret over udelukkede spillere. Spillere kan registrere sig i registret via spillemyndigheden.dk.

Registret indeholder oplysninger om spillere, der har udelukket sig fra at kunne spille online spil i Danmark.

Følgende oplysningerne findes i registret:

- Spillerens CPR-nummer
- Dato og tidspunkt for udelukkelsen
- Slutdato for ophør af den midlertidige udelukkelse (kun ved midlertidig udelukkelse)

En spiller, der er endeligt udelukket, kan tidligst et år efter optagelsen, anmode Spillemyndigheden om at blive slettet fra registret.

For at opfylde kravene til registret, er der en række funktioner, som tilladelsesindehaveren skal stille til rådighed for spilleren.

Tilladelsesindehaver skal:

- Informere om muligheden for at registrere sig i ROFUS og formidle adgang til registret fra tilladelsesindehaverens hjemmeside
- Kontrollere en spillers status i ROFUS ved kontooprettelse og ved alle kontologin

Se afsnit 6 for oplysninger om adgang til ROFUS testmiljø.

5.1 Tekniske krav i forhold til ROFUS

Tilladelsesindehaver skal implementere servicekald til ROFUS, for at gøre det muligt at kontrollere spilleres status for udelukkelse.

Se afsnit 6 for oplysninger om adgang til ROFUS testmiljø.

5.1.1 Vejledning og eksempler på brug af services

Følgende web services skal anvendes i forhold til ROFUS:

- GamblerCSRPValidation
  En service der skal anvendes til at tjekke en spillers alder forud for kontooprettelse. Servicen returnerer også svar på hvorvidt spillerens CPR-nummer eksisterer. Dette er især vigtigt idet ROFUS ikke kontrollerer hvorvidt CPR-nummeret eksisterer. Denne service skal derfor altid udføres før GamblerCheck (se nedenstående).

  Se dokumenterne GamblerCSRPValidationRequest.xsd og GamblerCSRPValidationResponse.xsd på spillemyndigheden.dk for indhold af servicekaldet.

- GamblerCheck
  En service der skal anvendes, når en spiller ønsker at oprette en konto, og ved hvert login. Denne service gør det muligt for tilladelsesindehaveren at kontrollere, om en person er registreret i ROFUS, enten midlertidigt, endeligt eller slet ikke. Denne kontrol sker ud fra spillerens CPR-nummer.

  Se dokumenterne GamblerCheckRequest.xsd og GamblerCheckResponse.xsd på spillemyndigheden.dk for indhold af servicekaldet.

5.1.1.1 Hovedoplysninger i servicekald

Ved foretagelse af servicekald skal der anføres hovedoplysninger, som har til formål at kunne følge request og response for servicekald og for at kunne rapportere fejloplysninger.

Hoved- og fejloplysninger håndteres på samme måde for TamperToken og ROFUS. Nedenstående oplysninger kan således også findes i afsnittet om TamperToken.

Hovedoplysningerne indsættes i et "any-element" i hver service og skal følge formatet, der er specificeret i XSD-filerne for hovedoplysninger, som findes på spillemyndigheden.dk.

Hovedoplysninger i "request":
Følgende hovedoplysninger skal angives i service-kald fra tilladelsesindehaver:

- TransaktionsID:
  Tilladelsesindehaver skal generere et unikt transaktionsID for servicekaldet. Spillemyndigheden anbefaler at der anvendes standarden Universally Unique Identifier (UUID), hvor id'et består af 32 hexadecimaler præsenteret i 5 grupper separeret af tankestreger på formen 8-4-4-4-12. F.eks.: 07B2A963-26C4-47E0-B517-C7059A598DA3

- TransaktionsTid:
  Tidspunktet for transaktionen. Tidspunktet skal angives på formen YYYY-MM-DDThh:mm:ss.sTZD, hvor YYYY er år, MM er måned, DD er dag, hh er timer, mm er minutter, ss er sekunder, s er et eller flere cifre for sekunddecimaler, og TZD er tidszonen repræsenteret som Z eller +hh:mm eller –hh:mm. F.eks.: 2010-12-07T09:33:51.249+01:00.

Hovedoplysninger i "response":
Følgende hovedoplysninger returneres altid i service response:

- TransaktionsID: Samme som ovenfor
- TransaktionsTid: Samme som ovenfor.
- ServiceID: Navnet på den kaldte service.

Følgende hovedoplysninger returneres også i service response, men returneres kun, når det er nødvendigt:

- Fejl: Fejl rapporteres når et kald ikke er forløbet som forventet.
  - FejlNummer: Id-nummer for fejlen.
  - FejlTekst: Beskrivelse af fejlen.
  - Identifikation: Tekstkode for fejlen.
  - ServiceID: Samme som ovenfor.

- Advis: Adviseringer er meddelelser, som ikke er fejlbeskeder. Det kan eksempelvis være en meddelelse om at servicekaldet er gået som forventet.
  - AdvisNummer: Id-nummer for adviseringen.
  - AdvisTekst: Beskrivelse af adviseringen.
  - Identifikation: Tekstkode for adviseringen.
  - ServiceID: Samme som ovenfor.

5.1.1.2 Eksempler på servicekald

Spillemyndigheden har udarbejdet to eksempler på kald af en service. Eksemplerne viser hvordan man, i hhv. Java og .Net, kan hente webservicebeskrivelser og kalde services med brug af HTTP basic access authentication. Desuden vises hvordan man modtager data fra servicen. Eksemplet tager udgangspunkt i kald til servicen GamblerCheck.

Følgende to eksempelfiler kan findes på spillemyndigheden.dk:

- Eksempel i .Net: GamblerServiceExampleClient.cs
- Eksempel i java: GamblerServiceExampleClient.java

Tilladelsesindehaveren får adgang til disse tjenester via GamblerCheck proxy service. Se dokumenterne GamblerCommonTypes.xsd og GamblerService.wsdl på spillemyndigheden.dk for indholdet af denne service.

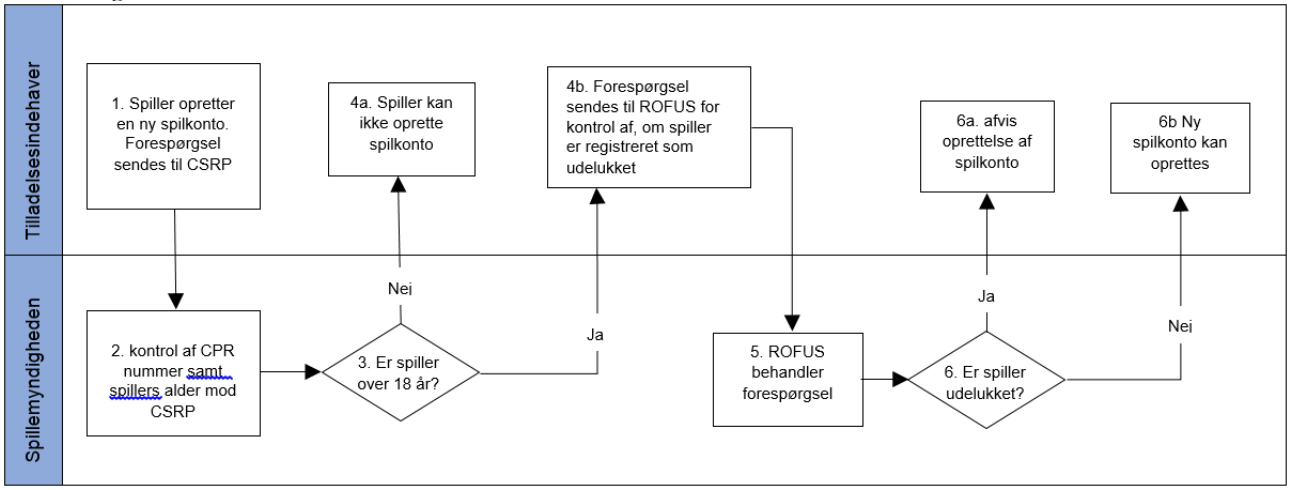
5.1.2 Forespørgsel i ROFUS ved konto-oprettelse og konto-login

For at spillere kan spille på en tilladelsesindehavers hjemmeside, skal de have en spilkonto. Nye spillere skal oprette en ny spilkonto, og eksisterende spillere skal logge sig ind på deres spilkonto, før de kan begynde at spille. Spillerens status i ROFUS skal tjekkes i begge tilfælde

5.1.2.1 Forespørgsel i ROFUS ved konto-oprettelse

I dette afsnit vil processen for en forespørgsel i ROFUS ved oprettelse af en ny spilkonto blive beskrevet. Processen er illustreret med et procesdiagram og efterfølgende beskrevet trinvist i et proceskort. Formålet er at give en præcis information om, hvad tilladelsesindehaver skal udvikle, for at denne proces kan udføres.

Procesdiagram:



Proceskort	
Procesinteressenter	Tilladelsesindehavere og Spillemyndigheden
Formålet med processen	Formålet med processen er at sikre, at tilladelsesindehaver kan forespørge i ROFUS, når en spiller åbner en ny spilkonto.

	Processen skal anvendes hver gang en spiller vil oprette en spilkonto hos en tilladelsesindehaver.
Input (start)	Processen starter med at spilleren vælger at oprette en spilkonto på tilladelsesindehaverens hjemmeside.
Output (slut)	Processen slutter med at tilladelsesindehaver får information om en spillers status i ROFUS. Hvis spilleren er registreret midlertidigt eller endeligt i ROFUS kan spilkontoen ikke oprettes. Hvis spilleren ikke er registreret i ROFUS kan tilladelsesindehaver fortsætte med kontooprettelse.

Beskrivelse af procesflow	
Nummer	Beskrivelse
1	Spilleren indtaster nødvendige oplysninger.
2	Spillerens alder verificeres med CSRP. Ved dette stadie kontrolleres eksistensen af CPR-nummeret også. Hvis CPR nummeret ikke eksisterer kan kontooprettelsen ikke fortsætte.
3	CSRP behandler forespørgslen.
4a	Hvis spilleren er under 18 år, sendes information herom til tilladelsesindehaver og spiller. Kontooprettelsen afvises.
4b	Hvis spilleren er 18 år eller ældre, sender tilladelsesindehaver forespørgsel til ROFUS for at kontrollere, om spiller er registreret som udelukket.
5	ROFUS behandler forespørgslen. Hvis ROFUS ikke svarer, kan spilleren behandles som om spilleren ikke er registreret i ROFUS, og der fortsættes til punkt 6b. Spillerens status skal kontrolleres når ROFUS igen er tilgængeligt. Hvis det viser sig, at spilleren står i registret, skal spillerens konto øjeblikkeligt lukkes.
6a	Hvis spilleren er udelukket i ROFUS afvises kontooprettelsen
6b	Hvis spilleren ikke er udelukket, kan processen med kontooprettelse fortsættes.

5.1.2.2 Forespørgsel i ROFUS ved konto-login

I dette afsnit vil processen for en forespørgsel i ROFUS ved login på en eksisterende konto blive beskrevet. Processen er illustreret med et procesdiagram og efterfølgende beskrevet trinvist i et proceskort. Formålet er at give en præcis information om, hvad tilladelsesindehaver skal udvikle, for at denne proces kan udføres.

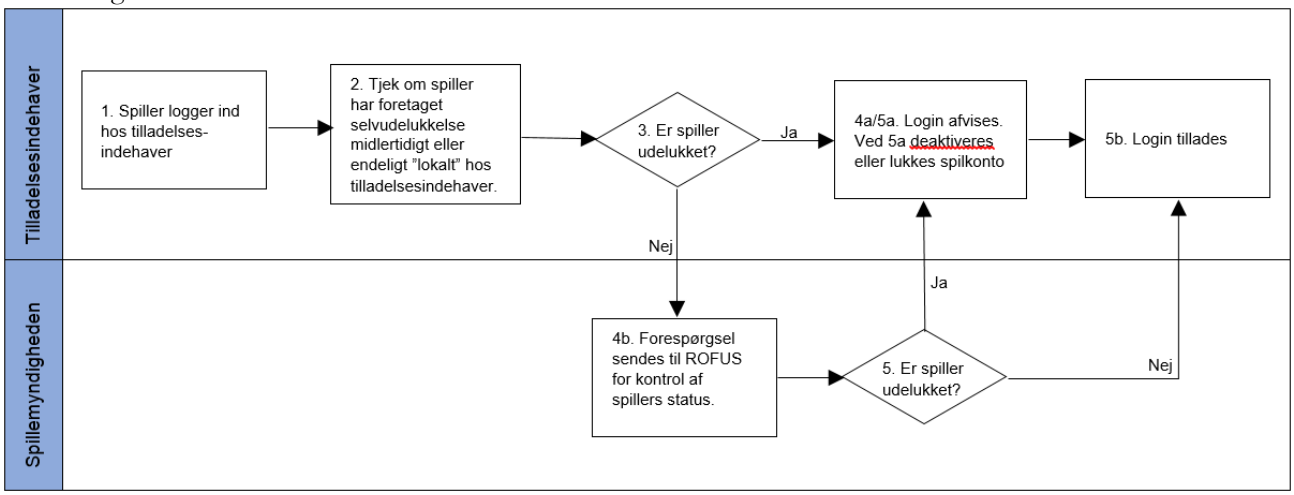
Når en spiller vil logge ind på sin allerede eksisterende spilkonto, skal tilladelsesindehaveren, inden login er gennemført, kontrollere om spilleren er blevet registreret i ROFUS siden sidste login. Hvis spilleren er registreret, afvises login.

Ved midlertidig udelukkelse i ROFUS afvises spillerens adgang til spilkontoen.

Ved endelig udelukkelse i ROFUS afvises spillerens adgang til spilkontoen. Tilladelsesindehaver skal herefter lukke spilkontoen og afslutte kundeforholdet. Kontoen kan herefter ikke genåbnes. Hvis spilleren på et senere tidspunkt ønsker at være kunde igen, skal spilleren gennemgå proceduren for kontooprettelse på ny.

Processen ved forespørgsel i ROFUS ved konto-login er beskrevet nedenfor – bemærk at proceduren også omfatter kontrol af spillerens eventuelle selvudelukkelse direkte hos tilladelsesindehaver.

Procesdiagram:



Proceskort	
Procesinteressenter	Tilladelsesindehavere og Spillemyndigheden
Formålet med processen	Formålet med processen er at sikre, at tilladelsesindehaver kan forespørge i ROFUS, når en spiller logger ind på sin spilkonto. Hvis spilleren er registreret i ROFUS, skal spilkontoen deaktiveres eller lukkes, og spiller kan herefter ikke logge ind. Processen skal anvendes hver gang en spiller vil logge ind på sin spilkonto hos tilladelsesindehaver.
Input (start)	Processen starter med at spiller logger ind på eksisterende spilkonto hos tilladelsesindehaver.
Output (slut)	Hvis spilleren ikke er registreret i ROFUS, afsluttes processen med at spiller bliver logget ind på sin spilkonto. Hvis spilleren er registreret, afvises login. Ved midlertidig udelukkelse i ROFUS afvises spillerens adgang til spilkontoen og kontoen deaktiveres. Ved endelig udelukkelse i ROFUS afvises spillerens adgang til spilkontoen. Tilladelsesindehaver skal herefter lukke spilkontoen og afslutte kundeforholdet.

Beskrivelse af procesflow	
Nummer	Beskrivelse
1	Spilleren foretager login på sin spilkonto hos tilladelsesindehaver.
2	Tilladelsesindehaver kontrollerer i eget system om spilleren er udelukket midlertidigt eller endeligt.
3	Tilladelsesindehaverens system behandler forespørgslen.
4a	Hvis spilleren er udelukket "lokalt" hos den pågældende tilladelsesindehaver, afvises login på spilkonto. Ved endelig udelukkelse, skal spillerens konto lukkes og kundeforholdet afsluttes.
4b	Hvis spilleren ikke er udelukket "lokalt" hos tilladelsesindehaver, kontrolleres det i ROFUS, om spilleren er midlertidigt eller endeligt udelukket.
5	ROFUS behandler forespørgslen. Hvis ROFUS ikke svarer kan spilleren behandles som om spilleren ikke er registreret i ROFUS, og der fortsættes til punkt 5b. Spillerens status skal kontrolleres når ROFUS igen er tilgængeligt.

5a	Hvis spilleren er midlertidigt udelukket i ROFUS, afvises spilleren fra at logge på spilkontoen og denne deaktiveres. Hvis spilleren er endeligt udelukket, skal spillerens konto lukkes og kundeforholdet afsluttes.
5b	Hvis spilleren ikke er udelukket, logges spilleren ind på sin spilkonto.

5.2 "Nej tak til spilreklamer" i ROFUS

Tilladelsesindehaver skal implementere servicekald til ROFUS, for at gøre det muligt at kontrollere, om der må sendes markedsføring til spilleren.

Med *markedsføring* menes enhver form for salgskontakt via telefonnumre, mailadresser, postadresser eller andre informationer, som tilladelsesindehaveren har om spilleren.

Push-beskeder og notifikationer kan være direkte markedsføring, som er omfattet af pligten til at konsultere ROFUS forud for udsendelse. Vurderingen af om der er tale om direkte markedsføring afhænger bl.a. af indholdet af beskeden og af udvælgelsen af modtageren.

Adresseløse husstandsomdelte reklamer og internetreklamer er ikke omfattet.

"Nej tak til spilreklamer" i ROFUS gælder for alt markedsføring fra alle tilladelsesindehavere. Det er derfor underordnet, hvad spilleren har af indstillinger på sin spilkonto, hvad angår modtagelse af markedsføring.

Alle personer, som registrerer sig i ROFUS fra 1. januar 2020, vil blive omfattet af "Nej tak til reklamer". Personer, som har registreret sig før den 1. januar 2020, har haft mulighed for at vælge om vedkommende ville tilmelde sig "Nej tak til spilreklamer". Det betyder, at der kan være personer, som er registreret i ROFUS uden samtidig at være tilmeldt "Nej tak til spilreklamer".

5.2.1 Vejledning til masseforespørgsel i ROFUS (Nej tak til spilreklamer)

Tilladelsesindehavere skal foretage serviceopkald i ROFUS tidligst 24 timer før, der udsendes markedsføring til spillere eller distributører.

Tilladelsesindehaveren må kun forespørge i ROFUS på CPR-numre tilhørende personer, som de har planlagt at sende markedsføring til.

Der kan spørges på højst 1.000 personer ad gangen. Det betyder, at hvis tilladelsesindehaver vil sende markedsføringsmateriale til 20.000 personer, skal servicekaldet foretages 20 gange.

Servicekaldet returnerer CPR-numre på personer, som IKKE må modtage markedsføring.

Hvis ROFUS ikke svarer, skal tilladelsesindehaver undersøge, om fejlen ligger i egne systemer. Hvis ikke det er tilfældet skal Spillemyndigheden underrettes med besked om tidspunkt for fejlen og fejlbeskeden.

5.2.2 Servicekald og CPR-numre

Følgende servicekald skal anvendes:

Input:

GamblerMultiReklameCheck_I

```
(
    *InformationAktørValg*
    [
        TilladelsesindehaverNavn

        * SpillemyndighedBrugerIdentifikation *
        RessourceNummer
    ]
)

*SpillerListe*

0{
    PersonCPRNummer
}
```

Output:

GamblerMultiReklameCheck_O

```
 *SpillerListeReklameFravalgt*

0{
    PersonCPRNummer
}
```

Dataelement	Datatype	Beskrivelse
PersonCPRNummer	base: string maxLength: 10 pattern: ((((0[1-9]|1[0-9]|2[0-9]|3[0-1])(01|03|05|07|08|10|12))|((0[1-9]|1[0-9]|2[0-9]|30)(04|06|09|11))|((0[1-9]|1[0-9]|2[0-9])(02)))[0-9]{6})|0000000000	CPR-nummer er et 10 cifret personnummer der entydigt identificerer en dansk person.

Servicekaldet kan testes i Spillemyndighedens ROFUS testmiljø. Se afsnit 6.3 for adgang til ROFUS testmiljø.

6 Adgang til og test af TamperToken og ROFUS

En ansøger får adgang til TamperToken og ROFUS testmiljøet i forbindelse med ansøgningen om tilladelse. Efter modtaget ansøgning opretter Spillemyndigheden adgang til TamperToken og ROFUS og udsteder brugernavn og password.

Spillemyndigheden giver ikke adgang til testmiljøet uden, at der er indgivet en ansøgning om tilladelse.

Spillemyndigheden sender sammen med brugernavn og password de testcases, der skal gennemføres af ansøger i forbindelse med ansøgningen.

6.1 Ansøgers test af TamperToken og ROFUS

Ansøger skal gennemføre de tests som er angivet i test casen, som sendes til ansøgeren i forbindelse med behandling af ansøgningen om tilladelse. Ansøgeren skal rapportere modtagne svar i skemaet sammen med eventuelle bemærkninger, som ansøgeren måtte have.

For at bestå testen skal ansøger, ved returnering af den gennemførte testcase, vedhæfte dokumentation for de gennemførte tests, der viser de krævede servicekald og –svar. Dette kan fx være i form af skærmbilleder eller logfilsudtræk fra ansøgers spilsystem (evt. testmiljø).

Eventuelle fejl ved testen rapporteres også i skemaet ud for den test hvor fejlen opstod. Den test der fejler, bør gentestes tre gange for at se om fejlen er generel eller sporadisk. Dette noteres i bemærkningsfeltet.

Efter testen skal skemaet returneres i udfyldt og underskrevet stand til Spillemyndigheden til godkendelse. Hvis der opstår fejl i forbindelse med testen, skal disse søges løst hos enten ansøger eller Spillemyndigheden, og ny fejlfri test skal gennemføres, før testen kan godkendes. Testforløbet aftales individuelt mellem ansøger og Spillemyndigheden.

6.1.1 End-points til services på testmiljø

Nedenfor findes end-points til de services på Spillemyndigheden testmiljø for TamperToken og ROFUS inkl. test af funktionen "nej tak til reklamer", der skal anvendes til ansøgers test af de to systemer. Der er for begge systemer tale om web-services som tilgås via internettet.

Såfremt ansøgeren gennemfører det tekniske og juridiske tilslutningsforløb og opnår tilladelse til at udbyde spil i Danmark, kommunikerer Spillemyndigheden end-points til produktionsmiljøet.

TamperToken services på TEST-miljøet:
Uden certifikat: http://rofusdemo.spillemyndigheden.dk/TamperTokenAnvend/TamperTokenAnvendService

Med certifikat: https://rofusdemo.spillemyndigheden.dk/TamperTokenAnvend/TamperTokenAnvendService

ROFUS services på TEST-miljøet:
Uden certifikat: http://rofusdemo.spillemyndigheden.dk/GamblerProject/GamblerService

Med certifikat: https://rofusdemo.spillemyndigheden.dk/GamblerProject/GamblerService

ROFUS – Nej tak til reklamer services på TEST-miljøet:
Uden certifikat:
http://rofusdemo.spillemyndigheden.dk/GamblerReklameProject/GamblerReklameService

Med certifikat:
https://rofusdemo.spillemyndigheden.dk/GamblerReklameProject/GamblerReklameService

6.1.2 Ansøgers connectivity-test

Ansøger kan gennemføre connectivity-test på følgende måde:

1) End-point indtastes i en browser på følgende måde for hhv. TamperToken og ROFUS:
   a. https://rofusdemo.spillemyndigheden.dk/TamperTokenAnvend/TamperTokenAnvendService
   b. https://rofusdemo.spillemyndigheden.dk/GamblerProject/GamblerService
2) Der åbnes en loginskærm i browseren og ansøger indtaster det af Spillemyndigheden udleverede brugernavn og password
3) Hvis connectivity-testen er succesfuld, vil WSDL-filen ses i browseren.

6.2 Spillemyndighedens vurdering af testen

Spillemyndigheden vurderer ansøgers test ud fra den udfyldte test case og den tilsendte dokumentation.

Såfremt ansøgers test vurderes korrekt gennemført, og dokumentationen er tilstrækkelig, godkendes ansøgers test af TamperToken og ROFUS.

Hvis ikke ansøgers test vurderes korrekt gennemført og/eller dokumentationen ikke er tilstrækkelig, vil Spillemyndigheden give besked til ansøger med årsag til afvisning. Herefter kan ansøger forbedre sine tests og Spillemyndigheden vil på ny gennemgå og vurdere ansøgerens test.

Når ansøger har fået godkendt alle tests gennemfører Spillemyndigheden en afsluttende vurdering. Spillemyndigheden forbeholder sig ret til at efterspørge yderligere tests og/eller dokumentation.

Spillemyndigheden giver ansøgeren besked, når gennemgangen af ansøgerens test, i forhold til de tekniske krav, er gennemført.

Umiddelbart inden Spillemyndigheden udsteder en tilladelse oprettes ansøger i produktionsmiljøet for TamperToken og ROFUS. Brugernavn og password sendes til ansøgeren sammen med end-points til produktionsmiljøet.

6.3 Adgang til testmiljø efter tilladelse er udstedt

Spillemyndigheden tillader ikke en general åbenstående adgang til testmiljøet. Adgang kan gives efter anmodning, når der er et specifikt behov for at teste.

Hvis tilladelsesindehaveren får behov for at have adgang til testmiljøet, skal Spillemyndigheden kontaktes med anførsel af følgende oplysninger:

- Tilladelsesindehaverens brugernavn til testmiljøet (det samme som blev brugt i ansøgningsprocessen).
- Information om, hvad tilladelsesindehaver skal teste.

- Information om hvor længe tilladelsesindehaveren forventer at testen vil vare.

I denne forbindelse har tilladelsesindehaver mulighed for at få tilsendt testcases, som også er anvendt i forbindelse med ansøgning om tilladelse. ROFUS testcasen indeholder CPR-numre som kan anvendes til test af ROFUS-funktionalitet.

7. Tilføjelse eller skift af spilsystem

I situationer hvor tilladelsesindehaver ønsker at tilføje et ekstra spilsystem eller flytte deres eksisterende udbud af spil helt eller delvist fra ét spilsystem til et nyt, skal Spillemyndigheden underrettes.

Når tilladelsesindehaver vil foretage en af de ovennævnte handlinger, svarer det for Spillemyndigheden som udgangspunkt til behandling af en ny ansøgning. Der er i disse tilfælde tale om nye spilsystemer, hvis sammensætning Spillemyndigheden ikke har et forudgående kendskab til.

Spillemyndigheden skal i disse situationer have informationer, svarende til tillæg B (Tillæg til ansøgning om tilladelse til at udbyde væddemål og onlinekasino) med tilhørende dokumentation, herunder certificeringsrapporter. Spillemyndigheden vil desuden stille krav om gennemførsel af test case vedrørende ROFUS og TamperToken, såfremt der også anvendes en ny SAFE. Hvis der også foretages skift af SAFE se afsnit 3.8. Tilladelsesindehaveren skal desuden sende nye testdata, så Spillemyndigheden kan se, at der kan rapporteres korrekt spildata fra den nye spilplatform.

8 Tilladelsesindehaverens underretningspligt

8.1 Nye spil og ændringer i eksisterende udbud af spil

Dette afsnit indeholder en beskrivelse af situationer vedrørende ændringer i spiludbuddet, hvor tilladelsesindehaver er forpligtet til at underrette Spillemyndigheden.

Kravene fremgår også af afsnit 6 i "Program for styring af systemændringer", som er en del af Spillemyndighedens certificeringsprogram.

8.1.1 Implementering af nye spil

Implementering af nye spil, der ikke påvirker tilladelsesindehaverens anvendelse af Spillemyndighedens Standard Records, kan gennemføres uden forudgående meddelelse til Spillemyndigheden.

Udbud af nye spil, der anvender Spillemyndighedens Standard Records, som ikke tidligere er blevet benyttet af tilladelsesindehaver, skal være meddelt Spillemyndigheden mindst fem hverdage, før udbuddet påbegyndes og samtidigt skal der indsendes eksempler på Standard Records.

8.1.2 Ændringer i eksisterende udbud af spil

Ændringer i eksisterende udbud af spil, der ikke påvirker tilladelsesindehaverens anvendelse af Spillemyndighedens Standard Records, kan gennemføres uden forudgående meddelelse til Spillemyndigheden.

Ændringer i tilladelsesindehaverens eksisterende udbud af spil, der vil påvirke tilladelsesindehaverens anvendelse af Spillemyndighedens Standard Records, skal være meddelt Spillemyndigheden mindst fem hverdage, før udbuddet ændres og samtidigt skal der indsendes eksempler på Standard Records.

8.1.3 Situationer, hvor Spillemyndighedens Standard Records ikke kan anvendes

Hvis tilladelsesindehaver vil udbyde nye spil, der ikke kan anvende Spillemyndighedens eksisterende Standard Records, skal dette være meddelt Spillemyndigheden mindst 60 dage, før udbuddet påbegyndes og kan ikke finde sted uden forudgående godkendelse fra Spillemyndigheden.

Ændringer i tilladelsesindehaverens eksisterende udbud af spil, der vil betyde, at udbuddet ikke længere kan anvende Spillemyndighedens eksisterende Standard Records, skal være meddelt Spillemyndigheden mindst 60 dage, før udbuddet ændres og kan ikke finde sted uden forudgående godkendelse fra Spillemyndigheden.

8.2 Øvrig underretningspligt

Af tilladelsen og bilag til tilladelsen fremgår det, at tilladelsesindehaver skal underrette Spillemyndigheden øjeblikkeligt når der opstår mistanke om eller konstateres fejl hos tilladelsesindehaveren og/eller hos dennes samarbejdspartnere fx spilleverandører.

Dette betyder blandt andet, at når der sker fejl på et spil, som udbydes af tilladelsesindehaveren, så skal Spillemyndigheden underrettes.

Tilladelsesindehavere har desuden pligt til at underrette Spillemyndigheden når der sker væsentlige ændringer af de forudsætninger, hvorpå tilladelsen er opnået.

I forhold til de tekniske krav, så omfatter denne underretningspligt ændring af forhold, svarende til indholdet af tillæg B (Tillæg til ansøgning om tilladelse til at udbyde væddemål og onlinekasino). Dette betyder, at Spillemyndigheden skal underrettes, hvis tilladelsesindehaver får en ny spilleverandør, ændrer deres procedurer for kundelogin eller kunderegistrering eller flytter spilsystemet til en ny fysisk placering mv.

Hvis tilladelsesindehaver foretager ændringer til deres SAFE skal Spillemyndigheden ligeledes underrettes jf. afsnit 3.8 i denne vejledning.

Spillemyndigheden

Bilag 1

I forbindelse med ansøgning om tilladelse eller i forbindelse med skift af spilsystem (bemærk at dette også gælder, hvis en tilladelsesindehaver får en ny spilleverandør, eller der lanceres et helt nyt spil med nye Standard Records) stiller Spillemyndigheden krav om levering af testdata.

Alt testdata skal være baseret på udtræk fra spilsystemet, være pakket med TamperToken, være placeret på SAFE og rapporteret til Spillemyndighedens testmiljø. Indholdet af testdata skal være i overensstemmelse med kravene i "Spillemyndighedens krav til rapportering af spildata på monopolspil", som findes på Spillemyndighedens hjemmeside.

Ansøgeren skal ved indsendelse af testdata dække alle scenarier, som deres spiludbud dækker. Hvis ansøgeren fx anvender en eller flere spilleverandører, så skal testdata dække spil fra alle leverandører, hvis der udbydes flere typer monopolspil, skal der rapporteres testdata som dækker alle spiltyper og hvis der både udbydes spil via computer, smartphone og landbaseret skal testdata dække alle de anvendte salgskanaler mv.

Ansøgere skal desuden demonstrere at de kan håndtere proceduren for annullering af transaktioner og rapportering af erstatningsdata, hvilket betyder at ansøger skal annullere minimum én fremsendt test transaktion fx et talspil eller et Netskrab og erstatte fx en enkelt End Of Day rapport.

Det er beskrevet i Spillemyndigheden krav til rapportering af spildata på monopolspil, hvilke strukturer der skal leveres til de enkelte typer af spil. Det aftales individuelt med Spillemyndigheden, hvor mange af hver filtype, der forventes.