



Tekniske krav til spilleautomater

Beskrivelse af tekniske krav til serversupporterede spilleautomater og spilleautomater i landbaserede kasinoer.

Version	Dato	Kort beskrivelse af ændring
1.0	09.05.2019	Første officielle version
1.1	03.07.2019	Ændring i punkt 1.1 Lovgrundlag
1.2	17.01.2020	Ændring i punkt 1.1 Lovgrundlag og ændring af illustration af mappestruktur under punkt 3.3 Krav til mappestrukturen på SAFE
1.3	08.04.2021	Ændring af tekst om CPR-numre i punkt 5.5 Servicekald og CPR-numre

Indhold

1. Indledning.....	4
1.1 Lovgrundlag	4
2. Overordnet beskrivelse af det tekniske setup	5
2.1 Visuel fremstilling	5
3. SAFE	6
3.1 Krav til tilgængelighed og forbindelse til SAFE	6
3.2 Krav til opbevaring og backup af data	6
3.3 Krav til mappestrukturen på SAFE	7
3.4 Navngivning af standard records og zip filer	7
3.5 Krav til pakning af data på SAFE	8
3.6 Valg af dato folder for zip fil	9
3.7 Størrelse på zip filer og antal standard records	9
3.8 Krav til rapportering af spildata	10
3.9 Spillemyndighedens proces til at hente data.....	10
3.10 SAFE i ansøgningsprocessen	11
3.11 Ændringer eller udskiftning af SAFE.....	11
4. TamperToken.....	13
4.1 Tekniske krav i forhold til TamperToken	13
4.2 Vejledning og eksempler på brug af services.....	13
4.3 Fejlhåndtering for TamperToken services	16
4.4 Håndtering af ubrugte tokens	17
4.5 Mekanisme til generering af MAC	17
4.6 MAC API.....	18
4.7 Eksempel på beregning af MAC.....	19
5. ROFUS – Register overfrivilligt udelukkede spillere.....	20
5.1 Tekniske krav i forhold til ROFUS.....	20
5.2 Forespørgsel i ROFUS ved spillerregistrering.....	21
5.3 "Nej tak til spilreklamer" i ROFUS.....	22
5.4 Vejledning til masseforespørgsel i ROFUS (Nej tak til spilreklamer).....	22
5.5 Servicekald og CPR-numre	23
6. Adgang til TamperToken og ROFUS	25
6.1 Ansøgers test af TamperToken og ROFUS	25
6.2 End-points til services på testmiljø	25
6.3 Ansøgers connectivity-test	26
6.4 Spillemyndighedens vurdering af testen	26
6.5 Adgang til testmiljø efter tilladelse er udstedt	26
7. Tilføjelse eller skift af spilsystem	27

8. Tilladelsesindehavers underretningspligt	28
8.1 Nye spil og ændringer i eksisterende udbud af spil	28
8.2 Implementering af nye spil	28
8.3 Ændringer i eksisterende udbud af spil	28
8.4 Situationer, hvor Spillemyndighedens Standard Records ikke kan anvendes	28
8.5 Øvrig underretningspligt.....	29
Bilag 1	30



1. Indledning

Formålet med dette dokument er at beskrive de tekniske krav, der bliver stillet til spiludbydere, som ønsker tilladelse til at udbyde eller som allerede har tilladelse til at udbyde spil i landbaserede kasinoer og på serversupporterede spilleautomater. Kravene er beskrevet i forhold til de systemer, der skal anvendes i forbindelse med Spillemyndighedens tilsyn med tilladelsesindehaver. Dvs. tilladelsesindehavers datalager (SAFE), sikkerhedssystemet TamperToken og Register Over Frivilligt Udelukkede Spillere (ROFUS). Kravene omkring ROFUS gælder ikke for tilladelsesindehavere, der har eller søger tilladelse til at udbyde spil på serversupporterede spilleautomater.

Tilladelsesindehavere skal således 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 spil i landbaserede kasinoer og på serversupporterede spilleautomater 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 har eller søger om tilladelse til at udbyde spil i landbaserede kasinoer leve op til Spillemyndighedens certificeringsprogram, mens spiludbydere, der har eller søger om tilladelse til at udbyde spil på serversupporterede spilleautomater i Danmark skal leve op til Bilag 3 i dokumentet "Godkendelse af testvirksomheder" og dele af Spillemyndighedens certificeringsprogram som findes på spillemyndigheden.dk.

1.1 Lovgrundlag

Lovgrundlaget for denne vejledning er bekendtgørelse om landbaserede kasinoer og bekendtgørelse om gevinstgivende spilleautomater i spillehaller og restaurationer.

Ifølge § 44 i Bekendtgørelse om landbaserede kasinoer, nr. 1290 af 29. november 2019, skal tilladelsesindehaver overholde de tekniske krav, som fremgår af bilag 1 til bekendtgørelsen.

Ifølge § 3 i Bekendtgørelse om gevinstgivende spilleautomater i spillehaller og restaurationer, nr. 1289 af 29. november 2019, skal tilladelsesindehaver mindst en gang i døgnet sende fornøden information om de afviklede spil på spilleautomaten til overvågningssystemet hos Spillemyndigheden.

Bekendtgørelserne inklusive bilag findes på spillemyndigheden.dk under fanen "Virksomheder og Foreninger" og derefter under "Kasinoer", henholdsvis "Spilleautomater".

Manglende overholdelse af kravet er strafbelagt.

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 "Vejledning til rapportering af spil".

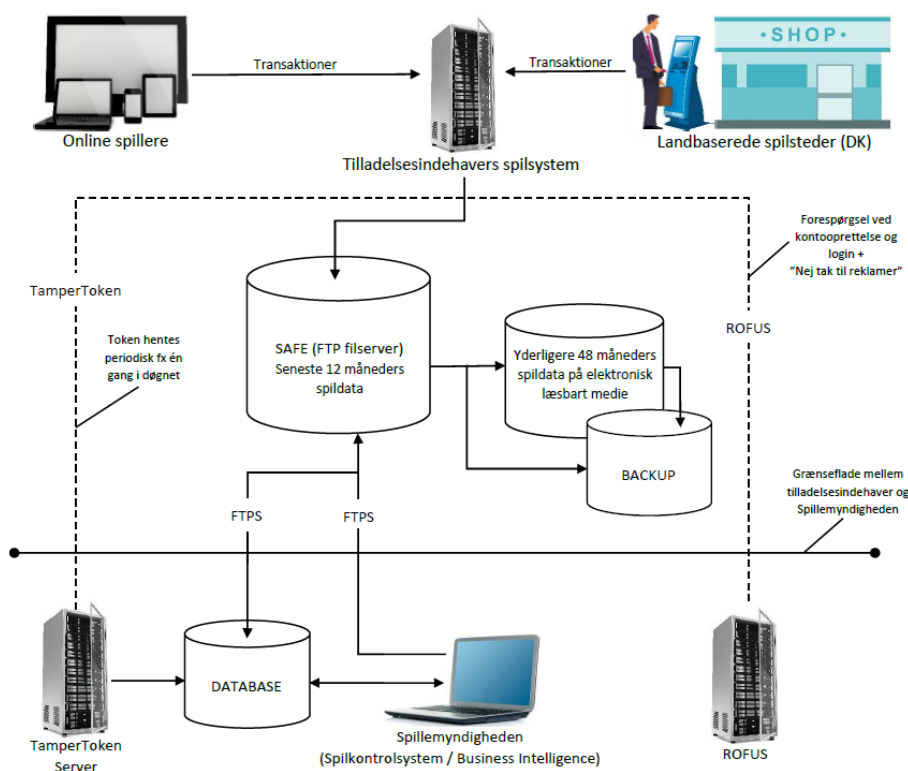
TamperToken er et sikkerhedssystem, der har til formål at sikre at de data, som tilladelsesindehaver lægger i deres SAFE ikke ændres mens de opbevares hos tilladelsesindehaver.

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 til brug for spilkontrol kan illustreres på denne måde:



3. SAFE

I forbindelse med opnåelse af tilladelse til at udbyde spil i landbaserede kasinoer og på server-supporterede spilleautomater 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 tilladelsesindehavers spil-system. 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 opetid på minimum 98,5 % målt pr. måned.
4. SAFE skal være konfigureret i UTC tid, således at tidsstempeller på filer¹ og mapper er angivet i UTC tid.
5. Dataoverførsel skal ske over internettet med FTPS/Implicit SSL i passiv mode på port 990. 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.

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.

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.

¹ Se desuden specifikke krav i "Vejledning til rapportering af spil", som kan findes på spillemyndigheden.dk

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:

Niveau 1: Den yderste mappe navngives "folderstruktur-spilssystem".

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

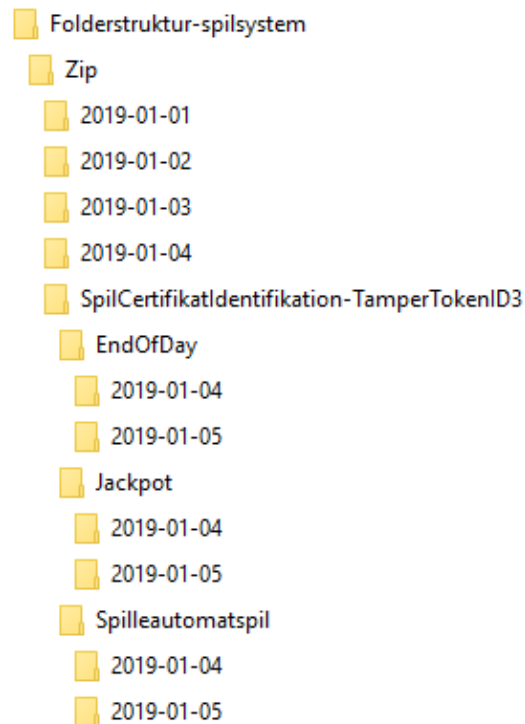
Niveau 3: Her er mapper for hver dag, navngivet efter datoen i formatet YYYY-MM-DD.

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 SpilCertifikatIdentifikation-TamperTokenID.zip.

Niveau 5: Her er de mapper som hver enkelt zip-fil indeholder. De navngives: "EndOfDay", "Jackpot" og "Spilleautomatspil".

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.

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



3.4 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 leveres som xml-fil)

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 = SpilApS

TamperTokenID = 1234567

SequenceInToken = 3

Standard record filen skal have følgende navn SpilApS-1234567-3.xml.

Zip-filen som indeholder denne standard record skal have filnavnet SpilApS-1234567.zip.

Se eksempel på zip fil med tre fastodds standard records på spillemyndigheden.dk

3.5 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 zippes. Zip-filerne skal pakkes på følgende måde:

Når standard record filerne for en token løbende ankommer, 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 tilladelsesindehavers 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 SpilCertifikatIdentifikation-TamperTokenID3.zip.

Det ses at SpilCertifikatIdentifikation-TamperTokenID3.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 SpilCertifikatIdentifikation-TamperTokenID3 og tilknyttes SpilCertifikatIdentifikation-TamperTokenID3.zip. Når token 3 lukkes og alle standard records er tilføjet zip filen, slettes mappen SpilCertifikatIdentifikation-TamperTokenID3.

3.6 Valg af dato folder 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-spilssystem/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>
```

3.7 Størrelse på zip filer og antal standard records

Spillemyndigheden har som udgangspunkt ikke sat begrænsninger på størrelsen af zip filer og antallet af standard records i en enkelt zip fil. For at sikre en smidig indlæsning af rapporteret data fra tilladelsesindehaverne i Spillemyndighedens database anbefales det dog at zip filer ikke overstiger en størrelse på 100 MB i pakket tilstand.

For at lette indlæsningsprocessen anbefaler Spillemyndigheden desuden, at der pakkes flere standard records i hver enkelt xml fil fremfor kun én standard record pr. xml fil.

Hvis Spillemyndigheden oplever problemer med indlæsning af data pga. størrelsen af zip filer, kan Spillemyndigheden vælge at ændre på tokenfrekvensen. Dette vil blive oplyst til tilladelsesindehaver.

3.8 Krav til rapportering af spildata

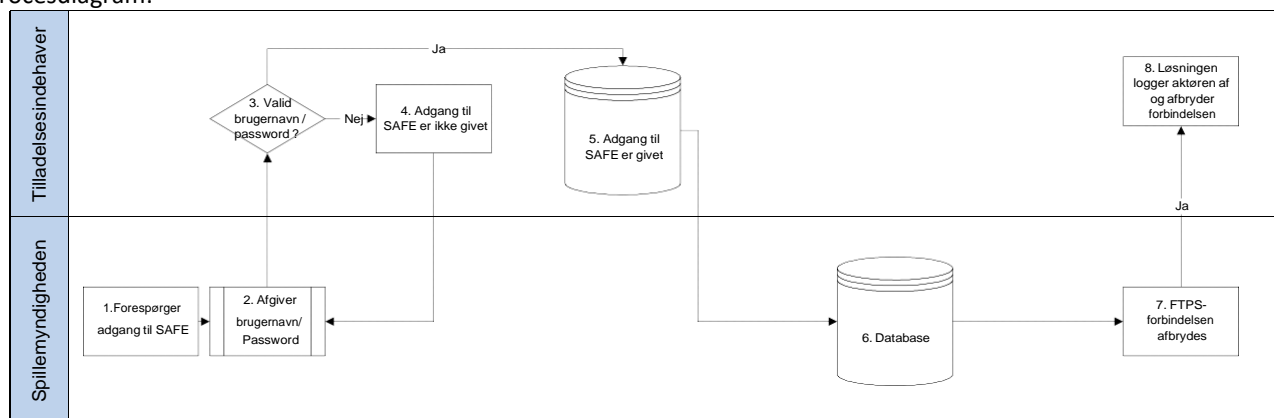
For at Spillemyndigheden kan indlæse data, som rapporteres af tilladelsesindehaverne, skal rapportering af spildata foretages ved brug af datastrukturer, som er udviklet af Spillemyndigheden.

Kravene til datastrukturerne er beskrevet i "Vejledning til rapportering af spil", som kan findes på spillemyndigheden.dk.

3.9 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 tilladelsesindehavers 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 database
7	Spillemyndigheden logger af SAFE
8	SAFE logger Spillemyndigheden af

3.10 SAFE i ansøgningsprocessen

I forbindelse med Spillemyndighedens behandling af en ansøgning om tilladelse til at udbyde spil på serversupporterede spilleautomater skal følgende trin gennemføres:

1. Ansøgeren udfylder punkter vedr. SAFE i Tillæg B til ansøgningen. Punkterne indeholder oplysninger som Spillemyndigheden skal bruge 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 fremgår af bilag 1 til denne vejledning. Testdata kan leveres i forbindelse med ansøgerens gennemførelse 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 hver enkelt dataelement, som indgår i de datastrukturer, som skal anvendes til rapportering af spil data. Dokumentet sendes til spiludbyder i forbindelse med ansøgningen.

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

3.11 Ændringer eller udskiftning af SAFE

Hvis en tilladelsesindehaver ønsker at foretage ændringer til deres eksisterende SAFE, eller de ønsker at udskifte deres eksisterende SAFE skal Spillemyndigheden underrettes.

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 URL og IP adresse til SAFE og det brugernavn og password, 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

4.1 Tekniske krav i forhold til TamperToken

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

Se afsnit 7 for oplysninger om adgang til TamperToken testmiljø.

4.2 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 Authentication 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.

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.

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.

Følgende hovedoplysninger skal angives i service-kald fra tilladelsesindehaver:

- **TransaktionsID:**
Tilladelsesindehaver skal generere et unikt transaktions id 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.

Følgende hovedoplysninger returneres altid i service-svar:

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

Følgende hovedoplysninger returneres også i service-svar, 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.

Eksempler

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 i tekstform 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 tilladel-

sesindehavers forståelse af de servicekaldene, men det er ikke hensigten at tilladelsesindehaver skal bygge 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:TamperTokenAnvend_I>
  </soapenv:Body>
</soapenv:Envelope>
```



```
</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>
```

4.3 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.

vis 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.

4.4 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>
```

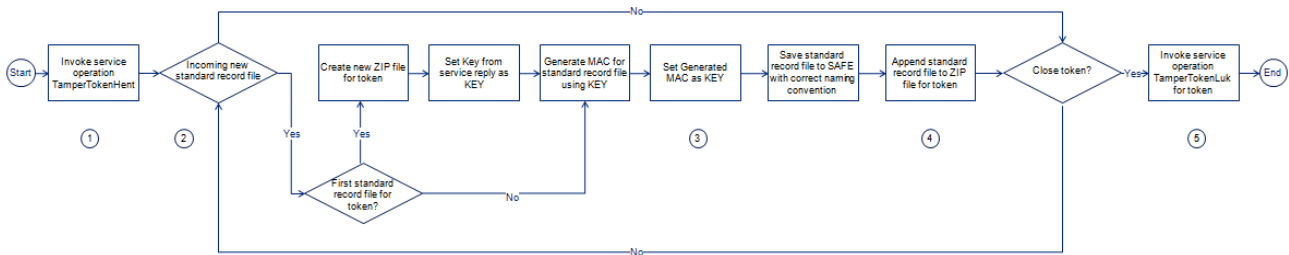
4.5 Mekanisme til generering af MAC

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.

Processen for den mekanisme som skal generere MAC for en token kan illustreres på følgende

måde:



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 umiddelbart efter en MAC af denne record.
3	Den genererede MAC bliver nu den nye Key for 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, typisk efter det tidsinterval som er angivet i svaret fra service operationen TamperTokenHent, aktiveres serviceoperationen TamperTokenLuk med ID for den token, der skal lukkes, den senest genererede MAC samt identifikation af tilladelsesindehaveren.

4.6 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".

Argumentet key er nøglen og InputStream indeholder det data fra den standard record, der skal genereres en MAC ud fra.

Eksempel:

```

public String getMAC(String key, InputStream input) throws
TamperTokenException {
    try {
        Mac mac = Mac.getInstance("HmacSHA256");
        byte[] byteKey = ByteArray-
            handler.parseString(key);
        SecretKeySpec keySpec = new Secret-
            KeySpec(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) ;  
    }  
}
```

4.7 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 overfrivilligt udelukkede spillere

Ifølge Bekendtgørelse om landbaserede kasinoer § 9, er der lovkrav om, at det skal være muligt for en spiller at udelukke sig fra at kunne spille på landbaserede kasinoer i Danmark. Denne udelukkelse kan være af midlertidig karakter, hvor spilleren udelukker sig for en vis periode, og den kan være endelig.

Spillemyndigheden er ansvarlig for dette register over udelukkede spillere. Spillere skal kunne registrere sig i registret både via Spillemyndighedens hjemmeside og via ROFUS fra tilladelsesindehavers hjemmeside.

Registret skal indeholde oplysninger om alle spillere i Danmark, der ønsker at udelukke sig fra at kunne foretage online væddemål, spille online spil samt spille på landbaserede kasinoer i Danmark.

Oplysningerne i registret er som følger:

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

En spiller, der er optaget i registret som endeligt udelukket kan til enhver tid, dog 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 stiller til rådighed for spilleren. Tilladelsesindehaver skal:

- Informere om muligheden for at registrere sig i ROFUS og formidle adgang til registret fra tilladelsesindehavers 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

Spillemyndigheden stiller følgende services til rådighed, der skal anvendes i forhold til ROFUS:

- **GamblerCSRValidation**
En service der skal anvendes til at tjekke en spillers alder forud for adgang til et landbaseret kasino. 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 GamblerCSRValidationRequest.xsd og GamblerCSRValidationResponse.xsd på spillemyndigheden.dk for indhold af servicekaldet.

- **GamblerCheck**
En service der skal anvendes, når en spiller ønsker at få adgang til et landbaseret kasino. 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.

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.

5.2 Forespørgsel i ROFUS ved spillerregistrering

I dette afsnit vil processen for en forespørgsel i ROFUS ved ønsket adgang til et landbaseret kasino 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.

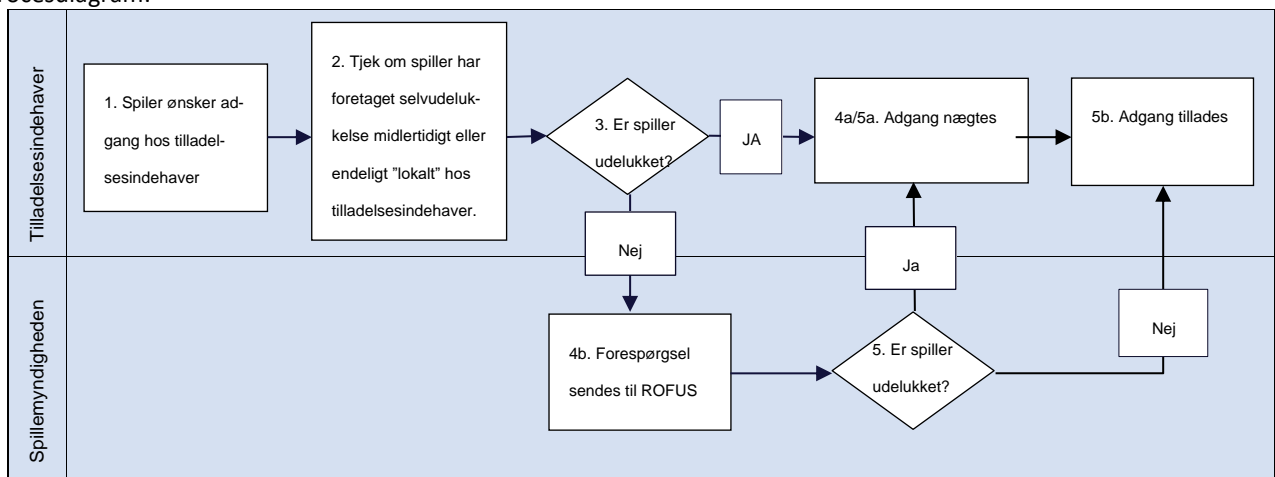
En spiller, der ønsker at spille på et landbaseret kasino, må ikke være registreret i ROFUS.

Når en spiller ønsker adgang til et landbaseret kasino, skal tilladelsesindehaveren, inden adgang, kontrollere om spilleren er registreret i ROFUS. Hvis spilleren er registreret, afvises adgang.

Ved midlertidig og endelig udelukkelse i ROFUS afvises spillerens adgang til kasinoet.

Processen ved forespørgsel i ROFUS ved adgang til kasinoer 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 ønsker adgang til et landbaseret kasino. Hvis spilleren er registreret i ROFUS, skal spilleren nægtes adgang til kasinoet.

	Processen skal anvendes hver gang en spiller ønsker adgang hos tilladelsesindehaver.
Input (start)	Processen starter med at en spiller ønsker adgang hos tilladelsesindehaver.
Output (slut)	Hvis spilleren ikke er registreret i ROFUS, afsluttes processen med at spiller får adgang til kasinoet. Hvis spilleren er registreret afvises adgang til kasinoet. Ved midlertidig udelukkelse i ROFUS nægtes spilleren adgang til kasinoet. Ved endelig udelukkelse i ROFUS nægtes spilleren adgang til kasinoet.

Beskrivelse af procesflow:

Nummer	Beskrivelse
1	Spilleren ønsker adgang hos tilladelsesindehaver.
2	Tilladelsesindehaver kontrollerer i eget system om spilleren er udelukket midlertidigt eller endeligt.
3	Tilladelsesindehavers system behandler forespørgslen.
4a	Hvis spilleren er udelukket "lokalt" hos den pågældende tilladelsesindehaver, afvises adgang til kasinoet.
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, nægtes spilleren adgang til kasinoet. Hvis spilleren er endeligt udelukket, skal spilleren nægtes adgang til kasinoet.
5b	Hvis spilleren ikke er udelukket, tillades spillerens adgang i kasinoet.

5.3 "Nej tak til spilreklamer" i ROFUS

Spillemyndigheden stiller en service til rådighed, der gør det muligt for tilladelsesindehavere at undgå at sende spilreklamer til selvudelukkede personer. Denne service kan til enhver tid tilvælges.

Med "spilreklamer" menes enhver form for salgskontakt via telefonnumre, mailadresser, postadresser eller andre informationer, som tilladelsesindehaveren har om brugeren. Adresseløse husstandsdelte reklamer og internetreklamer er ikke omfattet.

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

Tilladelsesindehavere kan foretage serviceopkald i ROFUS, før der udsendes kampagne- eller reklamemails til deres kunder eller distributører.

Når en bruger siger "Nej tak til spilreklamer" i ROFUS, er dette "nej tak" gældende for alle spilreklamer fra alle spiludbydere. Det er derfor underordnet, hvad brugeren har af indstillinger på sin spilkonto, hvad angår modtagelse af mails. Hvis brugeren gerne vil have reklamer igen, kan vedkommende altid fjerne sit "Nej tak til spilreklamer" i ROFUS.

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

Hvis ROFUS ikke svarer, skal tilladelsesindehaveren undersøge, om fejlen ligger i egne systemer. Hvis ikke det er tilfældet, bedes de underrette Spillemyndigheden om forholdet.

5.5 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: (((([1-9] 1[0-9] 2[0-9] 3[0-1]) (01 03 05 07 08 10 12)) ([1-9] 1[0-9] 2[0-9] 30) (04 06 09 11)) (([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.

Der kan højst spørges på 1.000 personer ad gangen. Det betyder, at hvis tilladelsesindehaver vil sende markedsføringsmateriale til 20.000 personer, skal servicekaldet foretages 20 gange. Ifølge Spillemyndighedens tests, tager et kald på 1.000 personer ca. 2 sekunder.

Servicekaldet kan testes i Spillemyndighedens ROFUS testmiljø. Hvis tilladelsesindehaver ikke har en eksisterende testbrugerkonto, beder vi jer om at rekvirere en ny. Hvis I har en inaktiv testbrugerkonto, skal I anmode om at få genåbnet denne.

Følgende test CPR-numre kan anvendes til testen (indtastes som ti sammenhængende tal):

- 121180 0050
- 121180 0085
- 121180 0107
- 121180 0093

6. Adgang til TamperToken og ROFUS

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

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

6.1 Ansøgers test af TamperToken og ROFUS

Ansøger skal gennemføre de tests som er angivet i test casen og foretage rapportering af modtagne svar og eventuelle bemærkninger i forbindelse med testen i skemaet. 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 skærbilleder eller logfiludtræk 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. Såfremt der opstår fejl i forbindelse med testen, skal disse søges løst hos enten ansøger eller Spillemyndigheden og ny fejlfri test skal gennemføres, før endelig tilladelse kan gives. Dette forløb aftales individuelt mellem ansøger og Spillemyndigheden.

For at få forståelse af hvordan TamperToken og ROFUS fungerer, kan ansøger prøve testcasene af i SoapUI eller lignende værktøj.

6.2 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>

6.3 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 (tilsvarende hvis testen skal gennemføres på end-points uden certifikat):
 - a. <https://rofusdemo.spillemyndigheden.dk/TamperTokenAnvend/TamperTokenAnvendService>
 - b. <https://rofusdemo.spillemyndigheden.dk/GamblerProject/GamblerService>Der åbnes en login-skærm i browseren og ansøger indtaster det af Spillemyndigheden udleverede brugernavn og password
- 2) Såfremt connectivity-testen er succesfuld, vil wsdl-filen ses i browseren.

6.4 Spillemyndighedens vurdering af testen

Spillemyndigheden vurderer ansøgers test ud fra den udfyldte test case og den tilsendte dokumentation. Desuden skal ansøger på dette tidspunkt have bestået Spillemyndighedens forbindelsestest til ansøgers SAFE for at ansøgers anvendelse af TamperToken kan testes af Spillemyndigheden.

Såfremt ansøgers test vurderes korrekt gennemført med tilfredsstillende resultat godkendes ansøgers test af TamperToken og ROFUS.

Hvis ikke ansøgers test vurderes korrekt gennemført eller resultatet ikke er tilfredsstillende, vil Spillemyndigheden give besked til ansøger med årsag til afvisning. Herefter kan ansøger forbedre sine tests og Spillemyndigheden vil på ny gennemgå ansøgerens test og foretage vurdering af resultatet.

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

Umiddelbart inden Spillemyndigheden udsteder en tilladelse oprettes ansøger i produktionsmiljøet for TamperToken og ROFUS og der gives besked til ansøger om, at det tekniske tilslutningsforløb er gennemført.

6.5 Adgang til testmiljø efter tilladelse er udstedt

Såfremt tilladelsesindehaveren på et senere tidspunkt får behov for at have adgang til testmiljøet, skal Spillemyndigheden kontaktes med anførsel af følgende oplysninger:

- Tilladelsesindehaverens brugernavn (det samme som blev brugt i ansøgningsprocessen)
- Hvad der skal testes
- Hvor længe tilladelsesindehaveren forventer at testen vil vare.

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 et nyt tillæg B med tilhørende dokumentation, herunder certificeringsrapporter. Spillemyndigheden vil desuden stille krav om gennemførsel af test case vedrørende TamperToken og ROFUS, såfremt der også anvendes en ny SAFE. Hvis der også foretages skift af SAFE henvises til afsnit 3.8. Tilladelsesindehaveren skal desuden sende nye testdata, så Spillemyndigheden kan se, at der kan rapporteres korrekt spildata fra den nye spilplatform.

8. Tilladelsesindehavers underretningspligt

8.1 Nye spil og ændringer i eksisterende udbud af spil

Dette afsnit indeholder kravene til, hvornår en tilladelsesindehaver skal underrette Spillemyndigheden i forbindelse med ændringer i deres spiludbud.

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

8.2 Implementering af nye spil

Implementering af nye spil, der ikke påvirker tilladelsesindehavers 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.

8.3 Ændringer i eksisterende udbud af spil

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

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

8.4 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 tilladelsesindehavers 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.

8.5 Øvrig underretningspligt

Af afsnit F i bilag 1 til bekendtgørelse om landbaserede kasinoer fremgår det at tilladelsesindehaver skal underrette Spillemyndigheden øjeblikkeligt når der opstår mistanke om eller konstateres fejl hos tilladelsesindehaveren og/eller hos denne samarbejdspartnere fx spilleleverandører.

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. Spillemyndigheden skal desuden underrettes, hvis tilladelsesindehaver får en ny spilleleverandør, ændrer deres procedurer for spillerregistrering 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.

Bilag 1

I forbindelse med ansøgning om tilladelse eller i forbindelse med skift af spilsystem stiller Spillemyndigheden krav om levering af testdata. Alt testdata skal være pakket med TamperToken, være placeret på SAFE og rapporteret til Spillemyndighedens testmiljø. Det er beskrevet under hvert punkt, hvilke strukturer der skal leveres og hvor mange af hver filtype, der forventes.

- Puljespil: Mindst ét helt puljespil.
 - PuljespilStartStruktur (én fil pr puljespil)
 - PuljespilTransaktionStruktur (almindeligvis flere filer pr puljespil)
 - PuljespilEndOfGameStruktur (én fil pr puljespil)
 - PuljespilSlutStruktur (én fil pr puljespil)
- PokerTurnering: Mindst én hel pokerturnering.
 - PokerTurneringStartStruktur (én fil pr pokerturnering)
 - PokerTurneringTransaktionStruktur (almindeligvis flere filer pr pokerturnering)
 - PokerTurneringSlutStruktur (én fil pr pokerturnering)
- PokerCash: Mindst 20 sessioner.
 - PokerCashGamePrSessionStruktur (kan rapporteres i én xml-fil)
- Managerspil: Mindst ét helt managerspil.
 - ManagerspilStartStruktur (én fil pr managerspil)
 - ManagerspilTransaktionStruktur (almindeligvis flere filer pr managerspil)
 - ManagerspilSlutStruktur (én fil pr managerspil)
- FastOdds: Mindst 50 fastoddsspil med transaktioner og gevinster.
 - FastOddsTransaktionStruktur (almindeligvis flere spil pr fil)
 - FastOddsSlutStruktur (almindeligvis flere gevinster pr fil)
- Betexchange: Mindst 10 eksempler på betexchange.
 - FastOddsTransaktionStruktur (almindeligvis flere odds pr fil)
 - FastOddsSlutStruktur (almindeligvis flere gevinster pr fil)
- KasinoSinglePlayer: Mindst 20 sessioner.
 - KasinoPrSessionStruktur (kan rapporteres i én fil)
- KasinoMultiPlayer: Mindst 20 sessioner.
 - KasinoPrSessionStruktur (kan rapporteres i én fil)
- End Of Day: Mindst én hel dags blandede data med tilhørende End Of Day rapport.
 - Blandede standard records fra en typisk dag. (alle relevante strukturer – antallet kan ses ovenfor under hver spilkategori)
 - EndOfDayRapportStruktur (én fil pr spilkategori pr valuta spillet af danske spillere i løbet af dagen)

Ansøgeren skal ved indsendelse af testdata dække alle scenarier, som deres spiludbud dækker. Dvs. hvis der udbydes flere typer for kasinospil fx roulette, black jack og spilleautomater, skal der rapporteres testdata som dækker alle spil typer. Det betyder desuden, at hvis der både udbydes spil via computer, smartphone og landbaseret skal testdata dække alle de anvendte salgskanaler.

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 fastoddsvæddemål eller en kasinosession og erstatte fx en enkelt End Of Day rapport.

