

# **Spillemyndighedens krav til akkrediterede testvirksomheder**

Version 1.1.0 af 1. september 2011

## Indhold

1 Indledning .....	3
1.1 Myndighed.....	3
1.2 Formål.....	3
1.3 Målgruppe .....	3
1.4 Version.....	3
1.5 Henvendelser.....	3
2 Certificering .....	4
2.1 Rammer for certificering .....	4
2.2 Ansvar for certificering .....	4
2.3 Certificeringskategorier .....	4
2.4 Certificering og krav til certificering .....	4
3 Spilkonti .....	5
3.1 Styring.....	5
3.1.1 Registrering.....	5
2.4.1 Spilfunktioner ("A") .....	5
2.4.1.1 Krav til procedure .....	5
2.4.1.2 Krav til testvirksomheden.....	5
2.4.1.3 Krav til personale, der superviserer og attesterer certificeringen .....	6
2.4.1.4 Krav til certificeringen .....	6
2.4.1.5 Certificeringens gyldighed .....	6
2.4.2 Forretningsfunktioner ("B").....	6
2.4.2.1 Krav til procedure .....	6
2.4.2.2 Krav til testvirksomheden.....	6
2.4.2.3 Krav til personale, der superviserer og attesterer certificeringen .....	6
2.4.2.4 Krav til certificeringen .....	7
2.4.2.5 Certificeringens gyldighed .....	7
2.4.3 Forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme ("C") .....	7
2.4.3.1 Krav til procedure .....	7
2.4.3.2 Krav til testvirksomheden.....	7
2.4.3.3 Krav til personale, der superviserer og attesterer certificeringen .....	7
2.4.3.4 Krav til certificeringen .....	8
2.4.3.5 Certificeringens gyldighed .....	8
2.4.4 Sårbarheds- og indtrængningsefterprøvning ("D") .....	8
2.4.4.1 Krav til procedure .....	8
2.4.4.2 Krav til testvirksomheden.....	8
2.4.4.3 Krav til personale, der superviserer og attesterer certificeringen .....	8
2.4.4.4 Krav til certificeringen .....	9
2.4.4.5 Certificeringens gyldighed .....	9
2.4.5 Styring af systemændringer ("E") .....	9
2.4.5.1 Krav til procedure .....	9
2.4.5.2 Krav til testvirksomheden.....	9
2.4.5.3 Krav til personale, der superviserer og attesterer certificeringer.....	9
2.4.5.4 Krav til certificeringen .....	10
2.4.5.5 Certificeringens gyldighed .....	10

## **1 Indledning**

### **1.1 Myndighed**

Dette dokument "Spillemyndighedens krav til akkrediterede testvirksomheder" er udstedt af Spillemyndigheden i henhold til spilleloven (nr. 848 af 1. juli 2010 med senere ændringer) og bekendtgørelserne om onlinekasino, online væddemål og landbaserede væddemål, og er en del af det samlede certificeringsprogram, som består af dokumenterne "Spillemyndighedens krav til akkrediterede testvirksomheder", "Spillemyndighedens program til styring af systemændringer" og "Spillemyndighedens tekniske standarder".

### **1.2 Formål**

Dokumentet fastsætter kravene for hvordan testvirksomheder bliver akkrediteret til at foretage certificering af tilladelsesindehaveres spilsystem herunder spilfunktioner og forretningsfunktioner, interne procedurer mv. Denne akkreditering foretages af Den Danske Akkrediterings- og Metrologifond (DANAK) eller et tilsvarende akkrediteringsorgan, som er omfattet af European co-operation for Accreditation's multilaterale aftale om gensidig anerkendelse eller medlem af International Laboratory Accreditation Cooperation.

### **1.3 Målgruppe**

Dokumentet er rettet mod tilladelsesindehaver, leverandører, akkrediteringsorganer og testvirksomheder.

### **1.4 Version**

Dette dokument er version 1.1.0 af 1. september 2011.

Spillemyndigheden vil løbende revidere certificeringsprogrammet og seneste version samt versionshistorik er tilgængelig på spillemyndighedens hjemmeside: <http://spillemyndigheden.dk>.

Ved ændringer i certificeringsprogrammet vil certificeringer som udgangspunkt fortsat være gyldige i den periode, de er udstedt for.

Det skal fremhæves, at det er den danske version, der er bindende og den engelske version udelukkende stilles til rådighed som vejledning.

### **1.5 Henvendelser**

Alle henvendelser, der vedrører dette dokument, bør stilles skriftligt til denne adresse:

[spillemyndigheden@skat.dk](mailto:spillemyndigheden@skat.dk)

eller

Spillemyndigheden  
Helgeshøj Allé 9  
2630 Taastrup

## 2 Certificering

### 2.1 Rammer for certificering

En certificering er baseret på audit og test af procedurer og tekniske standarder i forhold til kriterier fastsat i Spillemyndighedens certificeringsprogram.

Da kravene til certificeringens sikring er varierende, kræver det forskellige ekspertiser, og derfor er den overordnede certificering opdelt i fem kategorier jf. afsnit 2.3 nedenfor. Dette fordrer, at et bredt udvalg af professionelle aktører kan udstede certificeringer indenfor en eller flere kategorier og giver tilladelsesindehavere og leverandører større mulighed for at vælge, hvem der skal forestå udstedelsen af certificeringerne.

### 2.2 Ansvar for certificering

Det er tilladelsesindehavers ansvar at opnå de påkrævede certificeringer og, at disse er udfærdiget af en akkrediteret testvirksomhed i henhold til certificeringsprogrammet ved at tilrettelægge sin virksomhed med udgangspunkt i dette.

Det er testvirksomhedens ansvar at opnå akkreditering.

### 2.3 Certificeringskategorier

Certificeringskategori		Krav	Beskrivelse
A	Spilfunktioner	Spillemyndighedens tekniske standarder	Random Number Generator (RNG), spilleregler, registrering, driftsrapporteringer, kundeoversigt, betingelser og vilkår osv.
B	Forretningsfunktioner	Spillemyndighedens tekniske standarder	Informationssikkerhed osv. (revision)
C	Forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme	Spillemyndighedens tekniske standarder og retningslinjer for kontrolsystem	Registrering, sikkerhed, mistænkelig spilleradfærd
D	Sårbarheds- og indtrængningsefterprøvning	Spillemyndighedens tekniske standarder	Informationssikkerhed (efterprøvning)
E	Styring af systemændringer	Spillemyndighedens program for styring af systemændringer	Standard for godkendte ændringer til spilsystemer

### 2.4 Certificering og krav til certificering

For at sikre, at de nødvendige kvalifikationer er til stede, når en certificering udføres, skal testvirksomheder og deres ansatte leve op til minimumskravene i dette dokument. Dokumentation for at kravene er opfyldt, skal vedlægges alle certificeringerne.

Dokumentet "Spillemyndighedens tekniske standarder" består af en række krav i punktform, hvor hvert krav har en henvisning til hvilken/hvilke certificeringskategori(er), A, B, C og D, de henhører under, og dermed hvilken/hvilke kategori(er) af de akkrediterede testvirksomheder, der kan certificere efterlevelsen af det pågældende krav.

Af eksemplet nedenfor fremgår det, at testvirksomheder akkrediteret i certificeringskategori A, B og/eller C kan certificere efterlevelsen af kravet. Andre krav kan certificeres af forskellige akkrediterede testvirksomheder, som noteret i søjlen til højre for kravene.

<b>3 Spilkonti</b>			
<b>3.1 Styling</b>			
<b>3.1.1 Registrering</b>			
1	Spilsystemet skal kunne gemme dokumentation for kundeidentifikationsprocessen (kundedetaljer).  Vejledning: Efter kunderegistreringen kan systemet oprette en midlertidig spilkonto.	A	B C

Når en akkrediteret testvirksomhed har certificeret et givent krav i én certificeringskategori, og det krav indgår i flere certificeringskategorier, er det ikke nødvendigt at gentage certificeringen af kravet. I sådanne tilfælde skal der i stedet henvises til den ovennævnte certificering.

Hvis en underleverandør har certificeret deres produkter helt eller delvist efter Spillemyndighedens certificeringsprogram, skal den akkrediterede testvirksomhed ved test af tilladelsesindehaverens spilsystem alene teste de dele af spilsystemet, der ikke er certificeret.

Testvirksomheden skal være særligt opmærksom på at selvom underleverandørens produkt allerede er certificeret, kan det være nødvendigt at gentage dele af certificeringen, når produktet integreres i tilladelsesindehaverens samlede spilsystem. Dette vil blandt andet være relevant, når der ved implementeringen sker ændringer i det certificerede produkt.

Det er altid tilladelsesindehavers ansvar at hele certificeringsprogrammet er opfyldt.

Testvirksomheder skal opnå ISO/IEC 17025-akkreditering med udgangspunkt i de kriterier, der er beskrevet i de følgende afsnit, som omhandler de forskellige kategorier af certificering.

### 2.4.1 Spilfunktioner ("A")

#### 2.4.1.1 Krav til procedure

Dokumentet "Spillemyndighedens tekniske standarder" fastlægger, hvilke krav certificeringskategori A (spilfunktioner) indeholder.

#### 2.4.1.2 Krav til testvirksomheden

- have mindst 3 års erfaring med at teste spilfunktioner,
- arbejde med udgangspunkt i ISO/IEC 17025-akkrediteringen, der henviser til kravene i certificeringskategori A i "Spillemyndighedens tekniske standarder" og
- sikre, at tilstrækkeligt kvalificeret personale udfører certificeringen.

### 2.4.1.3 Krav til personale, der superviserer og attesterer certificeringen

Certificeringen skal udføres af personale, der er tilstrækkeligt kvalificeret, jævnfør afsnit 2.4.1.2 ovenfor. Udførelsen skal superviseres, og certificeringserklæringen skal attesteres, af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

- a) ved test af Random Number Generator skal supervisoren have en relevant kandidat- eller PhD-uddannelse, eller på anden måde kunne demonstrere relevante kvalifikationer
- b) ved test af andre spilfunktioner skal supervisoren have en relevant uddannelse eller på anden måde kunne demonstrere relevante kvalifikationer
- c) hvis supervisoren beskrevet i punkt a eller b ovenfor ikke har 5 års erhvervsmæssig erfaring med at teste spilfunktioner for en akkrediteret testvirksomhed, skal certificeringen også superviseres og attesteres af en person, der har 5 års erhvervsmæssig erfaring med at teste spilfunktioner for en akkrediteret testvirksomhed.

### 2.4.1.4 Krav til certificeringen

Testvirksomheden skal attestere, at kravene i certificeringskategori A i "Spillemyndighedens tekniske standarder" efterleves.

Rent undtagelsesvist kan det accepteres, at testvirksomheden attesterer certificeringen på trods af, at alle kravene ikke er opfyldt som beskrevet i "Spillemyndighedens tekniske standarder". Dette skal ske på baggrund af en risikovurdering med udgangspunkt i formålet med spilleloven og tilhørende bekendtgørelser, baseret på "IEC/ISO 31010 Risk management - Risk assessment techniques".

### 2.4.1.5 Certificeringens gyldighed

Certificeringen udstedes med en gyldighed af 12 måneder.

En fornyelse kan være baseret på stikprøver og efterlevelse af kravene i dokumentet "Spillemyndighedens program for styring af systemændringer".

## 2.4.2 Forretningsfunktioner ("B")

### 2.4.2.1 Krav til procedure

Dokumentet "Spillemyndighedens tekniske standarder" fastlægger, hvilke krav certificeringskategori B (forretningsfunktioner) indeholder.

### 2.4.2.2 Krav til testvirksomheden

- a) have mindst 3 års erfaring med at teste forretningsfunktioner,
- b) arbejde med udgangspunkt i ISO/IEC 17025-akkrediteringen, der henviser til kravene i certificeringskategori B i "Spillemyndighedens tekniske standarder" og
- c) sikre, at tilstrækkeligt kvalificeret personale udfører certificeringen.

### 2.4.2.3 Krav til personale, der superviserer og attesterer certificeringen

Certificeringen skal udføres af personale, der er tilstrækkeligt kvalificeret, jævnfør afsnit 2.4.2.2 ovenfor. Udførelsen skal superviseres, og certificeringserklæringen skal attesteres, af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

- a) have en relevant uddannelse eller på anden måde kunne demonstrere relevante kvalifikationer,

- b) være certificeret som International Information Systems Security Certification Consortium (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP), eller Payment Card Industry (PCI) Qualified Security Assessor (QSA), eller Information Systems Audit og Control Association (ISACA) Certified Information Systems Auditor (CISA).
- c) Hvis supervisoren beskrevet i punkt a og b ovenfor ikke har 5 års erhvervsmæssig erfaring med at teste forretningsfunktioner for en akkrediteret testvirksomhed, skal certificeringen også superviseres og attesteres af en person, der har 5 års erhvervsmæssig erfaring med at teste forretningsfunktioner for en akkrediteret testvirksomhed.

### 2.4.2.4 Krav til certificeringen

Testvirksomheden skal attestere, at kravene i certificeringskategori B i "Spillemyndighedens tekniske standarder" efterleves.

Rent undtagelsesvist kan det accepteres, at testvirksomheden attesterer certificeringen på trods af, at alle kravene ikke er opfyldt som beskrevet i "Spillemyndighedens tekniske standarder". Dette skal ske på baggrund af en risikovurdering med udgangspunkt i formålet med spilleloven og tilhørende bekendtgørelser, baseret på "IEC/ISO 31010 Risk management - Risk assessment techniques".

### 2.4.2.5 Certificeringens gyldighed

Certificeringen udstedes med en gyldighed af 12 måneder.

En fornyelse kan være baseret på stikprøver og efterlevelse af kravene i dokumentet "Spillemyndighedens program for styring af systemændringer".

## 2.4.3 Forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme ("C")

### 2.4.3.1 Krav til procedure

Der er *ikke* krav om en certificering i forbindelse med forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme, men testvirksomheder, der har erfaring inden for dette område, kan certificere krav i certificeringskategori C.

Dokumentet "Spillemyndighedens tekniske standarder" fastlægger, hvilke krav certificeringskategori C (forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme) indeholder.

### 2.4.3.2 Krav til testvirksomheden

- a) have mindst 2 års erfaring med forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme
- b) være akkrediteret som Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
- c) arbejde med udgangspunkt i ISO/IEC 17025-akkrediteringen, der henviser til kravene i certificeringskategori C i "Spillemyndighedens tekniske standarder" og
- d) sikre, at tilstrækkeligt kvalificeret personale udfører certificeringen.

### 2.4.3.3 Krav til personale, der superviserer og attesterer certificeringen

Certificeringen skal udføres af personale, der er tilstrækkeligt kvalificeret, jævnfør afsnit 2.4.3.2 ovenfor. Udførslen skal superviseres, og certificeringserklæringen skal attesteres, af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

## Spillemyndighedens krav til akkrediterede testvirksomheder

- a) have en relevant uddannelse eller på anden måde kunne demonstrere relevante kvalifikationer,
- b) være Certified Anti-Money Laundering Specialists (CAMS) Association of Certified Anti-Money Laundering Specialists (ACAMS) -akkrediteret.
- c) Hvis supervisoren beskrevet i punkt a og b ovenfor ikke har 3 års erhvervsmæssig erfaring med forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme i den regulerede onlinespilindustri, skal certificeringen også superviseres og attesteres af en person, der har 3 års erhvervsmæssig erfaring med forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme i den regulerede onlinespilindustri.

### 2.4.3.4 Krav til certificeringen

Testvirksomheden skal attestere, at kravene i certificeringskategori C i "Spillemyndighedens tekniske standarder" efterleves.

Rent undtagelsesvist kan det accepteres, at testvirksomheden attesterer certificeringen på trods af, at alle kravene ikke er opfyldt som beskrevet i "Spillemyndighedens tekniske standarder". Dette skal ske på baggrund af en risikovurdering med udgangspunkt i formålet med spilleloven og tilhørende bekendtgørelser, baseret på "IEC/ISO 31010 Risk management - Risk assessment techniques".

### 2.4.3.5 Certificeringens gyldighed

Certificeringen udstedes med en gyldighed af 12 måneder.

En fornyelse kan være baseret på stikprøver og efterlevelse af kravene i dokumentet "Spillemyndighedens program for styring af systemændringer".

## 2.4.4 Sårbarheds- og indtrængningsefterprøvning ("D")

### 2.4.4.1 Krav til procedure

Dokumentet "Spillemyndighedens tekniske standarder" fastlægger, hvilke krav certificeringskategori D (sårbarheds- og indtrængningsefterprøvning) indeholder.

### 2.4.4.2 Krav til testvirksomheden

- a) have mindst 2 års erfaring med sårbarheds- og indtrængningsefterprøvning af systemer.
- b) være akkrediteret som Payment Card Industry (PCI) Approved Scanning Vendor (ASV)
- c) arbejde med udgangspunkt i ISO/IEC 17025-akkrediteringen, der henviser til kravene i certificeringskategori D i "Spillemyndighedens tekniske standarder" og
- d) sikre, at tilstrækkeligt kvalificeret personale udfører certificeringen.

### 2.4.4.3 Krav til personale, der superviserer og attesterer certificeringen

Certificeringen skal udføres af personale, der er tilstrækkeligt kvalificeret, jævnfør afsnit 2.4.4.2 ovenfor. Udførelsen skal superviseres, og certificeringserklæringen skal attesteres, af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

- a) 5 års erhvervsmæssig erfaring med sårbarheds- og indtrængningsefterprøvning af systemer og
  - have en International Council of E-Commerce (EC-Council) Certified Ethical Hacker (CEH) eller Licensed Penetration Tester (LPT),



## Spillemyndighedens krav til akkrediterede testvirksomheder

- have en Information Assurance Certification Review Board (IACRB) Certified Penetration Tester (CPT) eller
- have en Global Information Assurance Certification (GIAC) Certified Penetration Tester (GPEN).

### 2.4.4.4 Krav til certificeringen

Testvirksomheden skal attestere, at kravene i certificeringskategori D i "Spillemyndighedens tekniske standarder" efterleves.

Rent undtagelsesvist kan det accepteres, at testvirksomheden attesterer certificeringen på trods af, at alle kravene ikke er opfyldt som beskrevet i "Spillemyndighedens tekniske standarder". Dette skal ske på baggrund af en risikovurdering med udgangspunkt i formålet med spilleloven og tilhørende bekendtgørelser, baseret på "IEC/ISO 31010 Risk management - Risk assessment techniques".

### 2.4.4.5 Certificeringens gyldighed

Certificering for indtrængningsefterprøvning udstedes med en gyldighed af 12 måneder, mens certificering for sårbarhedsefterprøvningen udstedes med en gyldighed på 3 måneder.

Det skal fremgå af certificeringen for indtrængningsefterprøvning, at denne bortfalder ved væsentlige opgraderinger eller ændringer i infrastrukturen eller brugen heraf (f.eks. installation af nye systemkomponenter, tilføjelse af et under-netværk eller tilføjelse af en webserver). Hvad der bedømmes som "væsentligt" afhænger i høj grad af opsætningen af et givent miljø, og det kan som sådan ikke foruddefineres af Spillemyndigheden, men hvis opgraderingen eller ændringen kan påvirke eller give adgang til kundedata, spildata, økonomiske data og/eller funktionalitet, skal den altid betragtes som væsentlig.

"Væsentligt" inden for et meget segmenteret netværk, hvor kundedata, spildata, økonomisk data og/eller funktionalitet er tydeligt isoleret fra andre data og funktioner, er meget forskelligt fra "Væsentligt" i fx et fladt netværk, hvor alle personer og systemer har potentiel adgang til kundedata, spildata, økonomisk data og/eller funktionalitet. Det anbefales at indtrængningsefterprøve alle opgraderinger og ændringer, for at sikre, at de eksisterende interne kontroller stadig virker effektivt efter opgradering eller ændringen.

## 2.4.5 Styring af systemændringer ("E")

### 2.4.5.1 Krav til procedure

Dokumentet "Spillemyndighedens program for styring af systemændringer" fastlægger, hvilke krav certificeringskategori E (styring af systemændringer) indeholder.

### 2.4.5.2 Krav til testvirksomheden

Kravene er de samme som for certificeringskategori A (spilfunktioner), jævnfør afsnit 2.4.1.2.

### 2.4.5.3 Krav til personale, der superviserer og attesterer certificeringer

Certificeringen skal udføres af personale, der er tilstrækkeligt kvalificeret, jævnfør afsnit 2.4.5.2 og 2.4.1.2 ovenfor. Udførelsen skal superviseres, og certificeringserklæringen skal attesteres, af én eller flere personer, der indestår for, at arbejdet er udført fagligt forsvarligt. Disse personer skal opfylde følgende krav:

- a) have en relevant uddannelse eller på anden måde kunne demonstrere relevante kvalifikationer,

## Spillemyndighedens krav til akkrediterede testvirksomheder

- b) være certificeret som International Information Systems Security Certification Consortium (ISC)<sup>2</sup> Certified Information Systems Security Professional (CISSP), eller Payment Card Industry (PCI) Qualified Security Assessor (QSA), eller Information Systems Audit og Control Association (ISACA) Certified Information Systems Auditor (CISA).
- c) Hvis supervisoren beskrevet i punkt a og b ovenfor ikke har 5 års erhvervsmæssig erfaring med at teste spil- eller forretningsfunktioner for en akkrediteret testvirksomhed, skal certificeringen også superviseres og attesteres af en person, der har 5 års erhvervsmæssig erfaring med at teste spil- eller forretningsfunktioner for en akkrediteret testvirksomhed.

### 2.4.5.4 Krav til certificeringen

Testvirksomheden skal attestere, at kravene i certificeringskategori E i "Spillemyndighedens program for styring af systemændringer" efterleves.

Rent undtagelsesvist kan det accepteres, at testvirksomheden attesterer certificeringen på trods af, at alle kravene ikke er opfyldt som beskrevet i "Spillemyndighedens program for styring af systemændringer". Dette skal ske på baggrund af en risikovurdering med udgangspunkt i formålet med spilleloven og tilhørende bekendtgørelser, baseret på "IEC/ISO 31010 Risk management - Risk assessment techniques".

### 2.4.5.5 Certificeringens gyldighed

Certificeringen udstedes med en gyldighed af 12 måneder.