

Opgradering til ny krypteringsalgoritme

eSkatDatas krypteringsalgoritme opgraderes fra TripleDesRsa15 til Basic256Sha256Rsa15. eSkatData har altid benyttet en sikker kryptering og høj sikkerhed i øvrigt. Timing af opgraderingen handler således om rettidig omhu og ikke om at lukke et sikkerhedshul.

eSkatData anvender en lagdelt sikkerhedsarkitektur, der beskytter borgerdata gennem uafhængige tekniske, kryptografiske og applikationslogiske lag. Krypteringsalgoritmen bruges ikke til nøgleudveksling, hvilket mitigerer en lang række sårbarheder, der ellers kunne være forbundet med Rsa15.

Basic256Sha256Rsa15 er valgt, da eSkatData skal være tilgængeligt for alle anvendere. Derfor kan der ikke vælges en nyere krypteringsalgoritme. Opgraderingen fra TripleDES15 til Basic256Sha256Rsa15 er derfor det bedst mulige valg inden for de tilgængelige og understøttede standarder.

Nuværende og kommende sikkerhedsarkitektur

Opgraderingen eliminerer de algoritmiske svagheder, der kunne være, hvis ikke det var for de øvrige sikkerhedslag, i den nuværende konfiguration. Ændringerne fra den gamle til den nye krypteringsalgoritme er defineret i [WS-SecurityPolicy 1.2](#) og omfatter:

Dansk:

XML-element	WS-SecurityPolicy 1.2-spec	TripleDesRsa15	Basic256Sha256Rsa15	Ændring
EncryptionMethod i EncryptedKey (nøgleindpakning)	Asym KW	rsa-1_5	rsa-1_5	Nej - uændret
EncryptionMethod i EncryptedData (data-kryptering)	Enc	tripleDES-cbc	aes256-cbc	Ja - opgraderet
DigestMethod	Dig	sha1	sha256	Ja - opgraderet
SignatureMethod	Asym Sig	rsa-sha1	rsa-sha1	Nej - uændret

Engelsk:

XML element	WS-SecurityPolicy 1.2-spec	TripleDesRsa15	Basic256Sha256Rsa15	Change
EncryptionMethod in EncryptedKey (key wrap)	Asym KW	rsa-1_5	rsa-1_5	No - unchanged
EncryptionMethod in EncryptedData (data encryption)	Enc	tripleDES-cbc	aes256-cbc	Yes - upgraded
DigestMethod	Dig	sha1	sha256	Yes - upgraded
SignatureMethod	Asym Sig	rsa-sha1	rsa-sha1	No - unchanged

Tidsplan og paralleldrift

Deployment tidsplan

De eksisterende PROD-endpoints skifter til at anvende den nye krypteringsalgoritme d. 1. oktober 2026.

Frem til den 30. november 2026 vil det være muligt at anvende PROD-OLD-endpoints, hvis man som anvender, ikke er klar til at bruge den nye krypteringsalgoritme d. 1. oktober. Af hensyn til anvendernes planlægning er det dog allerede nu muligt at skifte til PROD-OLD-endpoints, så man ikke behøver gøre det den 1. oktober. Det er dog stadig et krav, at anvenderen er klar til at bruge den nye krypteringsalgoritme den 30. november 2026. OLD-endpoints afvikles den 30. november 2026 i både DEMO og PROD.

Tidsplanen ser dermed sådan ud:

Datoer (2026)	Miljø	Eksisterende URL'er	Fallback -old URL'er
Er oprettet	PROD		UFST laver deployment med kopi af eksisterende apps med et "-old" endpoint (til anvendere der ikke kan køre med den nye algoritme).
01-okt	PROD	Anvendere tilgår med den nye algoritme.	
30-nov	PROD		UFST nedlægger apps med "-old" endpoint.

Paralleldrift

eSkatData tilbyder paralleldrift i PROD i forbindelse med opgraderingen af krypteringsalgoritmen. Det betyder, at hvis man ikke kan nå at være klar til at bruge den nye krypteringsalgoritme d. 1. oktober 2026, kan man skifte over til OLD-løsningen (den sorte linje), indtil den lukkes. Se nedenstående illustration:

Tidslinje for kryptering



Som det fremgår af illustrationen, er det allerede nu muligt at skifte til OLD-endpoints, hvis det ikke er muligt for anvenderen at foretage ændringen d. 1. oktober 2026. OLD-endpoints vil være tilgængelige frem til d. 30. november 2026.

Applikationer og endpoints

Opdatering af krypteringsalgoritmen i eSkatData PROD omfatter følgende applikationer:

Applikationer
HentSelvSendDataWS
Samtykke

OLD-endpoints

UFST har lavet en kopi af de eksisterende applikationer med et "-old" endpoint i PROD til anvendere, der ikke kan køre med den nye krypteringsalgoritme.

App	OLD-Endpoint
HentSelvSendDataWSOld	/hentselv-old/services/HentSelvSendDataService
SamtykkeOld	/samtykke-old/anmodadgang.do /samtykke-old/safari.do
WSDL filer Old	/hentselv-old/services/HentSelvSendDataService.wsdl

Der er kun ændringer til xpath på de eksisterende endpoints, så det kræver som udgangspunkt ikke ændringerne til firewall eller i anvenderens eSkatData-løsning – medmindre endpoints er hardcodet i løsningen. For anvendere, hvis løsninger kræver flere ændringer eller hvis planlægning ikke tillader et skifte d. 1. oktober 2026, er det

dermed muligt at køre videre med den gamle krypteringsalgoritme på OLD-endpoints, indtil anvenderen er klar.

Eksisterende endpoints

UFST opgraderer eksisterende applikationer og endpoints til den nye krypteringsalgoritme.

App	Endpoint (uændret)
HentSelvSendDataWS	/hentselv/services/HentSelvSendDataService
samtykke	/samtykke/anmodadgang.do /samtykke/safari.do
WSDL-filer	/hentselv/services/HentSelvSendDataService.wsdl

Bemærk, xpath er uændret og ændres altså ikke til new.

Anvenderens opgaver

Opgraderingen af krypteringsalgoritmen indebærer følgende opgaver og aktiviteter for anvendere af eSkatData:

- **Opdatering af kryptografiske konfigurationer**
Anvenderne skal sikre, at deres systemer understøtter den nye krypteringsalgoritme, herunder opdatere relevante biblioteker og konfigurationsindstillinger.
- **Test og validering**
Anvenderne bør gennemføre test for at sikre, at data fortsat kan krypteres/dekrypteres korrekt, og at integrationer fungerer som forventet efter ændringen.

Test af ny krypteringsalgoritme

Den nemmeste måde at teste Samtykkekomponenten på, er at anvende eSkatDatas Samtykke Request Test Driver: [HentSelv - Samtykke Parameter Generator Driver](#)

Vælg ”XML – med signering + kryptering”, Tryk på ”Generate Parm”:

HentSelv - Samtykke Request Test Driver

Generate SamtykkeParm Request:

- ☐ XML - uden indpakning
- ☐ XML - med signering
- ☒ XML - med signering + kryptering
- ☐ XML - med signering + kryptering + base64

```
<urn:PersonSamtykkeOpret_I xmlns:urn="urn:oio:skat:hentselv:ws:1.0.1"><xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Type="http://www.w3.org/2001/04/xmlenc#Content"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
><xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/><xenc:CipherData>
<xenc:CipherValue>3Xk5h1p7Mw9MZe2nePhIsr73WuU0L3cG6lmi1R/cbc71A0Sp1FW0Qt2FTfZkPUSCEr6y568I
s+z2jd6L7CGdy2lhrBv614Adu8R8Aw5Kr+Tf0ngnPuYufryIeAu5d1ZCHGwOftht93Q6hnb0
+Clv61ZDKUJW9XraUtttUPLX9erK+LzAGJyq/p1Thcsyer2qmhhxN0Nb+Oaql6Yz6hJ00B6CA
7pTjbK01qz0dt5gmYoss3hm2H8Cxr1P/DMe4mBx7dq4rrknROEwEiSR0LU3cuGq1k2XhJb
ZAoAsETBheOnu/X7Kup0JqctqrEPsF8zXlmgZUfeoEzciae1UjMEPlty8BVtP/tUthT3IyKY3/Ig
8v15NVY20zysYFPtCTbnEQpynIUs3EPMSmtQV/6jftxM2tmbutLw+Lu8waw5bky3xbMMF06YX
saKI75jnXugwHhnhYYIJEKK/syCGGhOpq65nEMV3VgLvAb81yghPeQB0/<xenc:CipherValue/><xenc:EncryptedKey/><ds:KeyInfo>
<xenc:CipherData><xenc:CipherValue>Dn/5mPzcndFgicnOE8Hh601LU6dvr7Z131zslxj/dE3YDch5mILND0Gxm5ubh75pR91/y
Rndk4QcZf5pY7efdf+hG0XrQ+ONS8gMIV571+3t62dH9P+qVfDh/1VsAUvdZLSybIA0hberh3Q11
vgAA1FQ6FCOCyBjXbsc8D63d0tsf2pmQTnosMhyLeNeS3+hckjR0k7nU8mlmPrYLuJ24UKjMhX9d
DQ6yICRYTqgMj+3j615akfta+u7XUIb267zwTA3Vo+alNW8oZUFAtIDCDoBrje5TNKJ2Luh3L/8
Pv+7B7l0Q1J1618Ag51x3Up1PPHzpVCLLeOPWm1d49a871InoeYQKFRQWqZ5X8K03DH/L1
sP5MFxE18hxYZ811G1K4C1DIsanPlyunkB83Jat380rMhBytapJw6d97Q0nyK9tjG6A42Z
Vn3e35/e37G0G4U7h2p21yPCSSYXD4QeN1L0gAnJp8eXZUBMq0181Pwb5XpU0j1eh5i0VgZoot3
0PytxTYEvsQU5FB8ZgsRPHV7z5537GEo78jquy3Ddr1XJdZ1680oL6hXQ128xlmhRgG/63pJdH
1o027WtGurMSY4Y9mgRkvKk0Wov/Ie+EOY7K8hPfuUctHvpI0pxitUpzLa10zCSBE/gB1cqX8g
01d0pEXzVeOBmVz1PPmMmDN65r15wkmukqE8H5rREpOK86HC1oBv2e2JkdYp9Z15XFhUDnZh
uY0Y681U7MhPj17HwH82X1ehEps5R1F1ENbYbYz/uHMR0Fz11v7JueIV+C6GalyhZTF+PmU9e
s195URKRphA9F19Jz1V588BDY1Hun503vZDws0ZHPV5261uI+43aX03GnT8z2F2AwK3M/Kz0EU
pWvo71v1+11Kw1Cy0rDvTu0/rUFgeanB0AYKPBvErsVfagq2AyzUw9Qt9zX7Xwty2CylhTcxp
BQ2R0sGkr6QCR51MZRsvPYJ3p1b305+m3E1Kbfrrer+XkMcVDERk4kqtackDUIGQweD1ENC68
J98CeosQwVLQonsEHC/Fh0ub03b/vQ0HBB/NRLduTcTvJ3Cuk1YHSMIF+24ayY0ezSHU5ImZV8
k5DnWkgCtEw0h8ecr7ZcBCarC21C9c9uLQ0f1qh10Tn53JavGtSulBf+v0GhMd+qht/bz1bym
MUCeqv/mvdv8B0/0P5ozZrsuf8w/XvG1Z1V6dAmk+039y/jyQgAUGtGZy6vcrK13MCCp1AH96
1Yo5+DYGC1H6M4Nr1+cGy5FXBx3BwXCLRgprv1KmmU08EwBhThosDX7usfb81DL00BUEZDF62X
BhsK7P61NDwEVTdc9H4VcoJ6o/2WgV009co/1zQGHIx291A15ndQH0D1JHqzN21BQxXCJpLS5v1p
```

Samtykke response kan ses ved at trykke ”Validate Parm” og se indholdet af ”Resultat”:

HentSelv - Samtykke Request Test Driver

Indtast Samtykke Request:

- ☐ XML - uden indpakning
- ☐ XML - med signering
- ☒ XML - med signering + kryptering
- ☐ XML - med signering + kryptering + base64

```
<urn:PersonSamtykkeOpret_I xmlns:urn="urn:oio:skat:hentselv:ws:1.0.1"><xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
><xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/><xenc:CipherData>
<xenc:CipherValue>ps+71/NYQPHdosFX1SYtuBaQTvniExnex+SvD9w/SbUGG1j71ymhTaNK9uGay1h9vWpIDrplSoxy
gf46rLYMB5VeavA11U8Yvly6+2Fx60jM4+dBthR00+xlX6Z4CI+2VXLUy+mvdBUwIKCXG1o/ZaT
1hcEOXs1HwV18hV9SL6GKDF8pR2GRqI4xZaFCUUE+mIplqLJnT2y1ZfGwygCugyBPqy11m6bZefn
krWp8FPFP7CppyHffvsLKwyg1uBUGVAM35MTt+5YI77zxMEdouhpi650GZRI0F8PqPDbwLRIdO
xbkeZw0d0r4kgHqotm+Is1o9Qk1KYb3YVcw5JtqEkdCOCqts1WzLSBKsPh41s6Y9V419eZqBfrO
pcr+MbKU9ueLx0/R56VYjotq1Yt+54qZ616GGEF5fgLtd25+nC68nbK9LUJJpcGeRzErxFzY2+H
1PBV7LMjenBRM052ADFV2b0poxEnep66352K3dHw1h8k1geiHwGRMSdce6errWcelFQ/JuZKaDV
```

Send Request

Meddelelse

Validering af SamtykkeRequestParm gennemført uden fej1

Resultat

```
<urn:PersonSamtykkeOpret_0 xmlns:urn="urn:oio:skat:hentselv:ws:1.0.1"><xenc:EncryptedData
xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
><xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"><xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/><xenc:CipherData>
<xenc:CipherValue>ps+71/NYQPHdosFX1SYtuBaQTvniExnex+SvD9w/SbUGG1j71ymhTaNK9uGay1h9vWpIDrplSoxy
gf46rLYMB5VeavA11U8Yvly6+2Fx60jM4+dBthR00+xlX6Z4CI+2VXLUy+mvdBUwIKCXG1o/ZaT
1hcEOXs1HwV18hV9SL6GKDF8pR2GRqI4xZaFCUUE+mIplqLJnT2y1ZfGwygCugyBPqy11m6bZefn
krWp8FPFP7CppyHffvsLKwyg1uBUGVAM35MTt+5YI77zxMEdouhpi650GZRI0F8PqPDbwLRIdO
xbkeZw0d0r4kgHqotm+Is1o9Qk1KYb3YVcw5JtqEkdCOCqts1WzLSBKsPh41s6Y9V419eZqBfrO
pcr+MbKU9ueLx0/R56VYjotq1Yt+54qZ616GGEF5fgLtd25+nC68nbK9LUJJpcGeRzErxFzY2+H
```

XML Resultat

```
<urn:PersonSamtykkeOpret_0 xmlns:urn="urn:oio:skat:hentselv:ws:1.0.1"
xmlns:ns="http://rep.oio.dk/skat.dk/basis/kontekst/xml/schemas/2006/09/01/"
xmlns:urn1="urn:oio:skat:hentselv:1.0.0"
xmlns:ns1="http://rep.oio.dk/cpr.dk/xml/schemas/core/2005/03/18/">
<ns:HovedOplysningerSvar>
<ns:TransaktionIdentifikator>c36784e8-3423-46d7-8e21-df231ef7bdf0</ns:TransaktionIdentifikator>
<ns:ServiceIdentifikator>SKAT-HentSelv</ns:ServiceIdentifikator>
<ns:TransaktionId>2026-06-24T14:41:55.938+02:00</ns:TransaktionId>
<ns:SvarStruktur/>
</ns:HovedOplysningerSvar>
```

I Test Driveren kan anvenderen også teste sit eget request med forskellige sikkerhedsniveauer.

Dokumentation og samples

I dokumentet [eSkatData Samtykke v2.1](#) er der i afsnit 3.4 XML Security Sample et Java-eksempel (Apache Santaurio). Der er følgende ændringer til eksemplet i forbindelse med opgraderingen af krypteringsalgoritmen:

```
XMLCipher_dataCipher = XMLCipher.getInstance(XMLCipher.AES_256);  
...  
  
String jceAlgorithmName = "AES";  
KeyGenerator keyGenerator = KeyGenerator.getInstance(jceAlgorithmName);  
keyGenerator.init(256);  
return keyGenerator.generateKey();
```

Den downloadede zip-fil, indeholdende denne vejledning, indeholder desuden eksempler på et request til og et response fra Dataservicen.