

29. juni 2020

# Sikkerhedsopgradering af anvendelsessystemer

## Indhold

1. Baggrund .....	1
1.1 Kontakt.....	2
2. Omfanget af ændringer.....	2
2.1 Skift til TLS 1.2.....	2
3. Konsekvenser ved skift til TLS 1.2 .....	2
3.1 Windows XP og IE8.....	2
3.2 Windows Server 2012 R2 eller tidligere .....	2
3.3 Java .....	2
3.4 .Net .....	3
3.5 Understøttede browsere .....	3
4. Referencer .....	3

## 1. Baggrund

KOMBIT ønsker at understøtte højeste generelle sikkerhedsniveauer på alle services der udstilles.

Derfor varsler KOMBIT at der skiftes til et højere sikkerhedsniveau fra august 2020, og det kan have konsekvenser for nogle anvendelsessystemer hos kommunerne og ældre Internet browsere, der tilgår brugervendte systemer hos KOMBIT. Bemærk denne ændring er gennemført i maj 2019 på Serviceplatformens eksterne testmiljø.

Formålet med dette dokument er at beskrive omfanget at de eventuelle ændringer de enkelte anvendelsessystemer kan blive ramt af.

Målgruppen er kommunernes IT-ansvarlige, IT-arkitekter og anvendelsessystemer.

## 1.1 Kontakt

- Kontakt [helpdesk@serviceplatformen.dk](mailto:helpdesk@serviceplatformen.dk) for spørgsmål vedrørende Serviceplatformen
- Kontakt [sts-support@kmd.dk](mailto:sts-support@kmd.dk) for spørgsmål vedrørende Støttesystemerne
- Kontakt [kdi@kombit.dk](mailto:kdi@kombit.dk) for generelle og forretningsmæssige spørgsmål.

## 2. Omfanget af ændringer

Der er således planlagt følgende ændringer:

### 2.1 Skift til TLS 1.2

Understøttelse af TLS versioner 1.0 og 1.1 samt krypteringsnøgler markeret som usikre ophører. Dette gælder for alle systemer der kalder element af KOMBIT fælles infrastruktur, herunder specielt

- Serviceplatformen
- Serviceplatformen Administration
- STS Administrationsmodul
- Adgangsstyring for Systemer; Security Token Service
- Beskedfordeler

## 3. Konsekvenser ved skift til TLS 1.2

De fleste moderne systemer og browsere er uden videre i stand til at benytte TLS 1.2, og vil ikke opleve en ændring. [Læs evt. anbefaling fra Microsoft om emnet.](#)

Følgende restriktioner for systemer der tilgår TLS 1.2 services er kendt:

### 3.1 Windows XP og IE8

Klienter der benytter ældre Windows, som eksempelvis Windows XP og Internet Explorer 8 eller tidligere, vil ikke kunne benyttes.

Udfør testen beskrevet i [TLS TEST](#) for at afgøre om en browser understøtter TLS 1.2

### 3.2 Windows Server 2012 R2 eller tidligere

Systemer der benytter Windows Server 2012 R2 eller tidligere understøtter ikke umiddelbart TLS 1.2 uden at udføre en justering som vist i **[Windows]**<sup>1</sup>.

Bemærk at dette betyder at kommuner der anvender AD FS 3.0, skal udføre disse justeringer, før deres AD FS server kan hente metadata fra Context Handleren.

### 3.3 Java

Systemer der benytter Java tidligere end 1.6 Update 111, kan ikke benytte TLS 1.2, og skal opdatere Java versionen til update 111 eller senere.

Systemer der benytter Java 1.7 eller 1.6 Update 111 eller senere kan anvende en property som

```
-Dhttps.protocols=TLSv1.2
```

---

<sup>1</sup> Link under referencer

Se den relevante produktdokumentation for nærmere oplysninger.

Senere version af Java (1.8 og frem) understøtter TLS 1.2 uden videre.

Se [Java](#)

### 3.4 .Net

Systemer der benytter .Net anbefales at benytte .Net 4.6 eller senere og benytte en indstilling som

```
System.Net.ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
```

### 3.5 Understøttede browsere

Følgende browsere og nyere kan anvende TLS 1.2:

- Google Chrome version 38 eller nyere
- Firefox version 27 eller nyere
- Internet Explorer 11 i Windows 7
- Microsoft Edge alle versioner
- Apple Safari version 7 (iOS X 10.9)
- Apple Safari Mobile version 6 (iOS 6)

## 4. Referencer

<b>[Anbefaling]</b>	<a href="https://docs.microsoft.com/en-us/security/engineering/solving-tls1-problem">https://docs.microsoft.com/en-us/security/engineering/solving-tls1-problem</a>
<b>[Java]</b>	<a href="https://blogs.oracle.com/java-platform-group/jdk-8-will-use-tls-1-2-as-default">https://blogs.oracle.com/java-platform-group/jdk-8-will-use-tls-1-2-as-default</a>
<b>[TLS TEST]</b>	<a href="https://www.ssllabs.com/ssltest/viewMyClient.html">https://www.ssllabs.com/ssltest/viewMyClient.html</a>
<b>[Windows]</b>	<a href="https://support.microsoft.com/en-in/help/3140245/updateto-enable-tls-1-1-and-tls-1-2-as-default-secure-protocolsin-wi">https://support.microsoft.com/en-in/help/3140245/updateto-enable-tls-1-1-and-tls-1-2-as-default-secure-protocolsin-wi</a> <a href="https://www.admin-enclave.com/en/articles/windows/305enable-tls-1-2-on-windows-2012-r2.html">https://www.admin-enclave.com/en/articles/windows/305enable-tls-1-2-on-windows-2012-r2.html</a>