De afgelopen jaren zijn veiligheid en privacy van steeds groter belang voor de bedrijfsvoering van een organisatie. U wilt niet alleen dat de juiste gegevens overal en altijd beschikbaar zijn. U wilt ook dat uw gegevens beschermd zijn tegen inbraak, beschadiging en verlies. Daarom maakt EPASS gebruik van een pakket aan beveiligingsmaatregelen waarmee de continuïteit van uw processen en de veiligheid van uw data gewaarborgd blijft.

Einde ondersteuning TLS 1.0 en TLS 1.1 per 1 mei 2020

Vanaf 1 mei 2020 zal EPASS geen ondersteuning meer bieden voor TLS 1.0 en TLS 1.1. Het gebruik deze TLS versies wordt onvoldoende veilig beschouwd. Om deze reden zal vanaf 1 mei 2020 op onze EPASS server allen nog gebruik gemaakt worden van TLS 1.2.

Hiermee sluiten we aan bij de overheid, banken en andere webapplicaties die inmiddels vanuit veiligheidsoogpunt ook alleen nog maar gebruik maken van TLS 1.2.

Wat is TLS?

Transport Layer Security (TLS) is een encryptie-protocol dat de communicatie tussen computers (bijvoorbeeld op het internet) beveiligt. Het doel van TLS is om twee partijen, bijvoorbeeld een webserver en een webbrowser, in staat te stellen om via het internet veilig gegevens uit te wisselen.

De meeste websites en zeker de sites waarop u moet inloggen, zoals de site van uw bank, maar ook EPASS, maken gebruik van TLS. U kunt dit herkennen als u naar een met TLS beveiligde website surft (beginnend met https://...) en links in de adresbalk van uw browser een slotje ziet.

Door op het slotje te klikken kunt u de identiteit van de server zien. U weet dan zeker dat u inlogt bij uw bank of de EPASS server.

TLS zorgt ervoor dat de communicatie tussen uw PC of tablet en de EPASS server veilig wordt versleuteld. Op deze manier kunnen onbevoegden niets met de data die u met de server uitwisselt.

Wat betekent het uitfaseren van TLS 1.0 en 1.1 voor u?

In de meeste gevallen zult u geen gevolgen ondervinden. Wanneer u reeds gebruik maakt van een moderne computer of tablet met de laatste versies van de verschillende besturingssystemen en browsers, dan bent u ongemerkt al overgestapt naar TLS 1.2 en maakt u veilig gebruik van Internet. U zult dan verder niets merken van het beëindigen van de ondersteuning van TLS 1.0 en 1.1.

Wordt er in uw organisatie nog met oudere internetbrowsers gewerkt? Dan kunt u hiermee vanaf 1 mei 2020 niet meer in EPASS inloggen.

Wat verwachten we van u?

Controleer of binnen uw organisatie de beschikbare apparaten en tablets gebruik maken van browsers/besturingssystemen welke TLS 1.2 ondersteund. Gebruik u nog een van de oudere browsers en/of besturingssystemen, dan is het nodig om voor 1 mei 2020 over te stappen naar een nieuwere versie ervan.

Volgens onze gebruiksstatistieken bestaan nagenoeg 100% van alle bezoeken aan de EPASS server uit bezoeken door browsers welke TLS 1.2 ondersteunen. Desondanks vinden we het wel belangrijk om u hierover te informeren, zodat u op de hoogte bent van deze verandering en indien nodig stappen kunt ondernemen.

Voor het testen van uw browser kunt u eventueel gebruik maken van de volgende sites: https://www.howsmyssl.com of https://www.ssllabs.com.

Hieronder een overzicht van browsers en besturingssystemen die TLS 1.2 ondersteunen:

- Internetbrowsers:
  - Apple Safari: vanaf versie 7
  - Google Chrome: vanaf versie 30
  - Mozilla Firefox: vanaf versie 27
  - Microsoft Internet Explorer: vanaf versie 11
  - Microsoft Edge
- Mobiele browsers (smartphones/tablets):
  - Apple Safari: vanaf iOS versie 7
  - Google Chrome: vanaf Android versie 6.0
  - Microsoft Internet Explorer: vanaf Windows Phone 8.1
- Besturingssystemen:
  - Apple OSX/macOS: vanaf versie 10.9
  - Microsoft Windows: vanaf versie 7

Tevens is het mogelijk dat sommige oudere browsers wel TLS 1.2 ondersteunen maar dat de gebruiker eerst een handeling dient uit te voeren om deze ondersteuning te activeren in zijn browser.

In de bijlage vindt u een uitgebreid overzicht van de diverse browsers en de bijbehorende TLS ondersteuning.

Vragen?

Heeft u naar aanleiding van deze informatie vragen? Stuur dan een bericht naar productmanagement@epass.eu.

Bijlage

Hieronder vindt u een overzicht van de diverse internetbrowsers en de compatibiliteit met TLS1.2:

- Voor het testen van uw browser kunt u eventueel gebruik maken van de volgende sites: https://www.howsmyssl.com of https://www.ssllabs.com.
- Meer informatie over de historie van de TLS/SSL ondersteuning, zie de 'Web Browsers' sectie van het Wikipedia artikel 'Transport Layer Security'. https://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers
- '**No**' betekend geen ondersteuning voor TLS1.2, u kunt deze browser niet meer gebruiken om in te loggen bij EPASS.
- '**Disabled by default**' betekend dat de browser de TLS1.2 ondersteuning standaard heeft uitgeschakeld en dan ook niet kunt in loggen bij EPASS. Mogelijk kan de TLS1.2 ondersteuning in deze browser wel ingeschakeld worden. Raadpleeg de Help sectie van de betreffende browser voor instructies hoe u TLS1.2 ondersteuning kunt inschakelen.

Browser	Versie	Platform	TLS 1.2
Google Chrome (Chrome for Android)	21		**No**
	22-29		**No**
	30+		Yes
Mozilla Firefox (Firefox for mobile)	1-22		**No**
	ESR 17		**No**
	23		**No**
	24-26		**Disabled by default**

Browser	Versie	Platform	TLS 1.2
	ESR 24		**Disabled by default**
	27+		Yes
	ESR 31.0+		Yes
Microsoft Internet Explorer	7-9	Windows Vista Server 2008	**No**
	8-10	Windows 7 Server 2008 R2	**Disabled by default**
	10	Windows 8 Server 2012	**Disabled by default**
	11+	Windows 7 Server 2008 R2	Yes
	11+	Windows 8.1 Server 2012 R2	Yes
Microsoft Edge	Edge 12-18 (IE11)	Windows 10 (desktop/mobile)	Yes
Microsoft Internet Explorer Mobile	7, 9	Windows Phone 7, 7.5, 7.8	**No**
	10	Windows Phone 8	**Disabled by default**
	11+	Windows Phone 8.1	Yes

Browser	Versie	Platform	TLS 1.2
Apple Safari	1-6		**No**
	7	OS X 10.9 (Mavericks)	Yes
	8	OS X 10.10 (Yosemite)	Yes
	9-11	OS X 10.11 (El Capitan)	Yes
	10-13	macOS 10.12 (Sierra) macOS 10.13 (High Sierra) macOS 10.14 (Mojave) macOS 10.15 (Catalina)	Yes
Apple Safari (mobile)	3-5	t/m IOS 4	**No**
	5, 6	IOS 5, 6	Yes
	7	IOS 7	Yes
	8	IOS 8	Yes
	9	IOS 9	Yes
	10	IOS 10	Yes
	11	IOS 11	Yes
	12	IOS 12	Yes
	13	IOS 13, iPadOS 13	Yes