In the past years safety and privacy have become of greater importance to businesses and organizations. You don't just want to have access to the right data from everywhere and at any time. You also want your data to be safe from theft, damage and loss. For this reason EPASS takes safety precautions which guarantee the continuity of your processes and the safety of your data.

End of support for TLS 1.0 and TLS 1.1 starting May 1st 2020

Starting May 1st 2020 EPASS will no longer support TLS 1.0 en TLS 1.1. Using these TLS versions is considered unsafe. For this reason starting May 1st 2020, our EPASS server will only support TLS 1.2.

With this decision we align with the government, banks and other web applications who have already ended support for TLS 1.0 and TLS 1.1 due to safety concerns.

What is TLS?

Transport Layer Security (TLS) is an encryption-protocol that secures the communication between computers. The purpose of TLS is to provide a safe means of exchanging information over the internet between two entities, for example a webserver and a webbrowser.

Most websites where you have to log in, like your bank website, but also EPASS, make use of TLS. U can recognize this when you navigate to a TLS secured website (starting with https://...) and you will see a lock sign on the left of the address bar of your webbrowser.

By clicking on the lock sign you can see the identity of the server. U will be able to tell that you are logging in with your bank or the EPASS server.

TLS ensures that the communication between your PC or Tablet and the EPASS server is encrypted safely. This also ensures that unauthorized persons cannot access the data your exchange with the server.

What does phasing out TLS 1.0 and 1.1 mean for you?

In most cases you won't notice any changes. If you are already using a recent computer, smartphone or tablet with up-to-date versions of their respective operating systems and webbrowsers, then you have unknowingly already updated to TLS 1.2 and you are already navigating the internet safely. You will not notice any change when the support of TLS 1.0 and TLS 1.1 will be discontinued.

Does your organization still use older versions of webbrowsers? In that case you might not be able to access EPASS starting May 1st 2020.

What do we expect from you?

Check if within your organization the available devices like PC's, smartphones and tablets make use of webbrowsers and operating systems that support TLS 1.2. If you are still using older browsers or operating systems, you will have to upgrade to recent versions before May 1st 2020.

According to our usage statistics, almost 100% of the visits to the EPASS server consist of visits from webbrowsers which support TLS 1.2. Nonetheless we think it's important to inform you of these changes so that you are aware of what will change and which steps you can take if necessary.

To test your browser you can make use of the following websites:

https://www.howsmyssl.com or https://www.ssllabs.com.

The following list shows which webbrowsers and operating systems that support TLS 1.2:

- Webrowsers:
  - Apple Safari: version 7 and up
  - Google Chrome: version 30 and up
  - Mozilla Firefox: version 27 and up
  - Microsoft Internet Explorer: version 11 and up
  - Microsoft Edge: all versions
- Mobile webbrowsers (smartphones/tablets):
  - Apple Safari: iOS version 7 and up
  - Google Chrome: Android version 6.0 and up
  - Microsoft Internet Explorer: Windows Phone 8.1 and up
- Operating systems:
  - Apple OSX/macOS: version 10.9 and up
  - Microsoft Windows: version 7 and up

Some older webbrowsers do support TLS 1.2 but in that case the user has to manually activate support in the webbrowser.

In the appendix you can find an extensive overview of different types of webrowsers and the respective support of TLS 1.2.

Questions?

Do you have any questions in relation to this information? Please send an email to productmanagement@epass.eu.

Appendix

The following overview shows a list of all the different webbrowsers and their TLS 1.2 compatibility:

- To test your browser you can make use of the following websites: https://www.howsmyssl.com or https://www.ssllabs.com.
- For more information about the history of TLS/SSL support, please refer to the 'Webbrowsers' section of the Wikipedia article 'Transport Layer Security': https://en.wikipedia.org/wiki/Transport_Layer_Security#Web_browsers
- '**No**' means that there is no support for TLS 1.2. You can't use this webbrowser to log in to EPASS anymore.
- '**Disabled by default**' means that the browser support TLS 1.2, but that this support is turned off by default and you won't be able to log in to EPASS. Possibly you can activate the TLS 1.2 support in this webbrowser. Please consult the help section for the respective for instructions on how to activate TLS 1.2 support

Browser	Version	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	Version	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	Version	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