Deprecating support for unsecure TLS 1.2 ciphers

We are announcing the deprecation of the unsecure Transport Layer Security (TLS) Cipher Suites that support CBC-Mode since Thursday, the **15th of September 2022 (on Production)**.

This step was done already on Tuesday **19th of July 2022** on our DEMO environments https://demo.esignanywhere.net/ and https://demo-lts.esignanywhere.net/, so that you can then check if your integrations code supports already TLS 1.2 GCM algorithms by using that environments for your tests.

We will then only support TLS 1.2 with algorithms supporting Perfect Forward Secrecy (PFS) and GCM-Mode! Here you can find a list:

~~ECDHE-ECDSA-AES128-GCM-SHA256~~
ECDHE-RSA-AES128-GCM-SHA256
~~ECDHE-ECDSA-AES256-GCM-SHA384~~
ECDHE-RSA-AES256-GCM-SHA384

This has an impact of the list of supported Software versions:

Minimum supported server version: Windows Server 2016 or newer
Minimum client version: iOS 9, Android 4.4, Mac OS X 10.11, Windows 10
Minimum Java integration version: Java 8

which means, if your API integration runs on the following Software versions you will be unable to establish a secure TLS connection with our services:

Windows 7 / 8.1 or older
Windows Server 2012 R2 or older
Java 7 or older