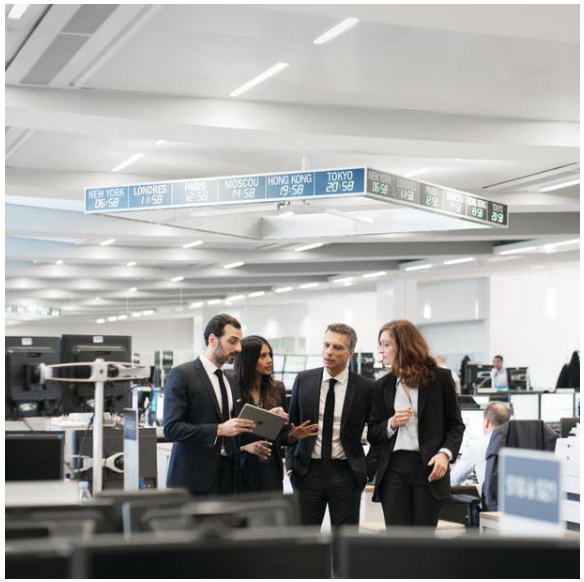


ARRET DES PROTOCOLES TLS 1.0 ET 1.1

Sogenactif

MARS 2018

SOMMAIRE

1.CONTEXTE

A. DEFINITION ET PLANNING

- **Qu'est-ce que le TLS ?**
  - Transport Layer Security (TLS) est un protocole garantissant la confidentialité des communications entre les applications et leurs utilisateurs sur Internet. Lorsqu'un serveur et un client communiquent, TLS veille à ce qu'aucun tiers ne puisse écouter ou modifier les messages. TLS succède au protocole Secure Socket Layer (SSL).
- **Evolution**
  - A partir du 10/04/2018 à 10h, les protocoles TLS 1.0 et 1.1 seront désactivés au sein de la plateforme Sogenactif et toute communication à partir de cette date devra être faite uniquement en TLS 1.2
  - L'obsolescence TLS 1.0 et 1.1 concerne tous les systèmes utilisant une connexion en https, cela ne concerne donc pas que Sogenactif ou le domaine du paiement

Cette mise à jour de protocole TLS concerne l'ensemble des acteurs : e-commerçants et acheteurs

B. PERIMETRE CONCERNE

	Vos clients acheteurs	Vous e-commerçants
Page de paiement	Les internautes devront utiliser un navigateur permettant la navigation en TLS 1.2	Si vous utilisez SOGENACTIF Payment 1.0*, vous n'êtes pas concerné Si vous utilisez SOGENACTIF PayPage 2.0, en utilisant les connecteurs SOAP ou JSON, vous devez migrer votre application afin qu'elle gère le protocole TLS 1.2. Si vous utilisez les connecteurs POST, vous n'êtes pas concernés.
Outils de gestion : ***Portail Sogenactif, Sogenactif Gestion, Sogenactif Téléchargement***	Non concerné	Vous devez utiliser un navigateur internet permettant de naviguer en TLS 1.2 → Une mise à jour de votre navigateur internet sera peut-être nécessaire
Utilisation d'un compte FTP: ***Pour la réception des journaux et/ou l'envoi de fichiers pour automatiser vos opérations (Sogenactif Batch ou Abonnement)***	Non concerné	Vous devez vérifier la configuration du logiciel FTP utilisé pour qu'il accepte le protocole TLS 1.2 → Une mise à jour de votre logiciel sera peut-être nécessaire
Réponses automatiques des tickets de paiement de vos transactions	Non concerné	Si les URL utilisées pour les réponses automatiques sont configurées en https, vous devez migrer vers un serveur d'application compatible TLS 1.2.

* e-commerçants ayant souscrit l'offre Sogenactif avant le 15/09/2016

B. PERIMETRE CONCERNE

- **Cas particulier des e-commerçants utilisant l'offre Sogenactif Office Serveur :**
  - Si vous avez souscrit l'offre SOGENACTIF Office Serveur 1.0* et que vous utilisez le protocole 3D Secure pour vos transactions ou l'option 1clic**, → vous devrez migrer votre application afin qu'elle soit compatible avec le TLS 1.2
  - Si vous utilisez SOGENACTIF Office Serveur 2.0, → vous devez migrer votre application afin qu'elle soit compatible avec le TLS 1.2

* e-commerçants ayant souscrit l'offre Sogenactif avant le 15/09/2016
** L'option 1 clic vous permet de proposer à vos clients d'enregistrer les données de leur carte afin de simplifier le règlement de leurs prochains achats

2. ZOOM SUR LES NAVIGATEURS INTERNET

A. LISTE DES NAVIGATEURS IMPACTES

- **Dès lors que les protocoles TLS 1.0 et 1.1 seront interdits, de nombreuses versions de navigateur ne fonctionneront plus, par exemple :**

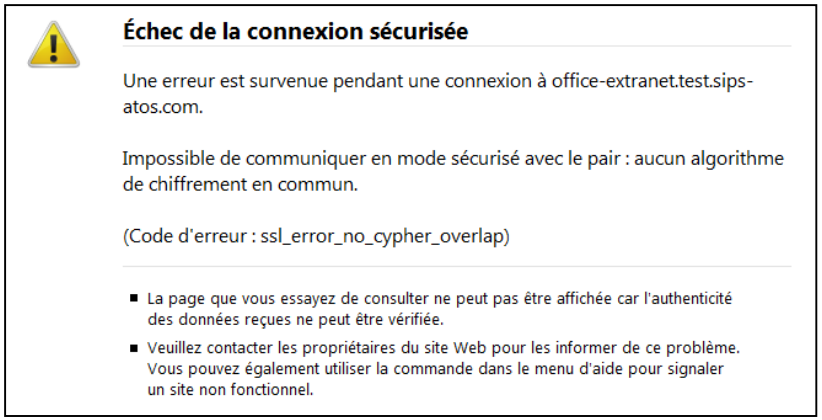
	Versions concernées
Internet Explorer	▪ IE 10 et versions antérieures Il est possible de passer à TLS 1.2 dans les réglages du menu « Outils » : « Options Internet », « Avancé ». ▪ IE Mobile : sous Windows Phone 8.0 et antérieurs
Android OS browser	▪ Sous Android 4.4 KitKat (dernière version : 4.4.4 du 19/06/2014) et antérieurs
Safari	▪ Sous OS X 10.8 Mountain Lion (dernière version : 10.8.5 du 12/09/2013) et antérieurs.
Google Chrome	▪ Sous Windows (7+), OS X (10.9+), Linux, Android (4.1+), iOS (9.0+), Chrome OS version 30-32 et antérieurs
Mozilla Firefox	▪ Mozilla Firefox : sous Windows (7+), OS X (10.9+), Linux, Android (4.0.3+), iOS (9.0+) versions 24 et ESR24.0 et antérieurs ▪ Pour les versions 24, 25.0.0, 25.0.1, 26 ESR24.0-ESR24.1.0, ESR24.1.1, il est possible de passer au protocole TLS v1.2 dans le paramétrage de Mozilla

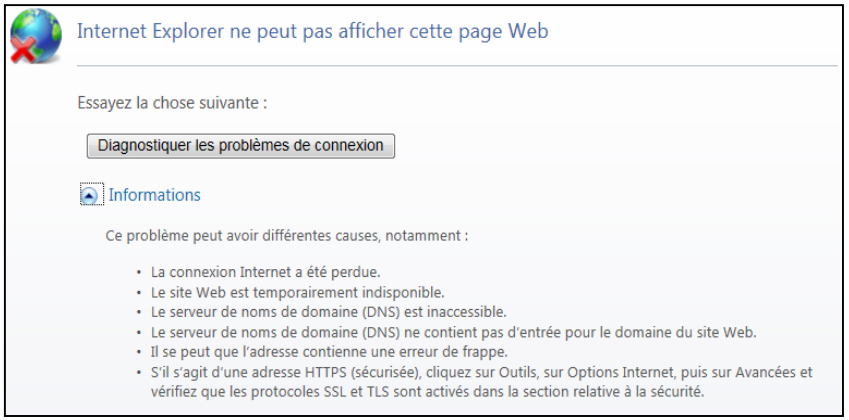
- **L'exhaustivité et la complexité des compatibilités du parc de navigateurs peuvent être consultées à l'adresse suivante : https://en.wikipedia.org/wiki/Transport_Layer_Security#Web_Browsers**

- **Ci-dessous le lien vers la liste exhaustive des navigateurs WEB compatibles/incompatibles : https://caniuse.com/#search=tls1.2**

B. EXEMPLES DE MESSAGES D'ERREURS*

- **Dès lors que le navigateur Internet n'est pas compatible avec le protocole TLS 1.2, voici des exemples de message d'erreurs qui vous seront affichés :**





Ces messages d'erreurs sont générés par les navigateurs (et non par le serveur Sogenactif), ils ne sont donc pas personnalisables. Il est donc important de sensibiliser vos clients pour qu'ils mettent à jour leur navigateur et ne soient pas bloqués lors de leur parcours de paiement

*exemples non-contractuels

FOIRE AUX QUESTIONS

POUR EN SAVOIR PLUS

- **Où puis-je trouver de plus amples informations ?**

Des informations sont disponibles dans les publications officielles suivantes :

- Mise à jour importante du PCI Security Standards Council concernant la prorogation des délais https://www.pcisecuritystandards.org/pdfs/Migrating_from_SSL_and_Early_TLS_-v12.pdf
- PCI DSS version 3.1 - https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
- PCI DSS version 3.1 Résumé des changements https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1_Summary_of_Changes.pdf
- PCI DSS version 3.1 Informations complémentaires https://www.pcisecuritystandards.org/documents/Migrating_from_SSL_Early_TLS_Information_Supplement_v1.pdf
- Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations (National Institute of Standards and Technology) http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295

- **Existe-t-il un outil disponible pour évaluer la mise en œuvre actuelle de TLS ?**
  - Afin de tester la compatibilité de votre navigateur, vous pouvez utiliser des outils externes tels que : https://www.howsmyssl.com.

LES CONSÉQUENCES POUR VOUS

- **Que se passe-t-il si vos protocoles de sécurité ne sont pas à jour ?**
  - Le PCI Council demande aux prestataires de services de paiement comme Sogenactif de refuser les protocoles qui ne sont plus considérés comme sécurisés. Cela signifie que les échanges à l'aide du protocole TLS 1.0 et 1.1 ne seront plus considérés comme sécurisés par nos moteurs de paiement et échoueront.
- **J'utilise Sogenactif Gestion et Sogenactif Téléchargement : suis-je impacté ?**
  - Si vous utilisez Sogenactif Gestion ou Sogenatif Téléchargement, vous devez mettre à jour votre navigateur afin qu'il gère le TLS 1.2 et pouvoir ainsi continuer à vous connecter avec votre USER habituel.
- **J'utilise le Portail Sogenactif *: suis-je impacté ?**
  - Si vous utilisez le Portail Sogenactif, vous devez mettre à jour votre navigateur afin qu'il gère le TLS 1.2 et pouvoir ainsi continuer à vous connecter avec votre USER habituel.
- **J'utilise les réponses automatiques et manuelles : suis-je impacté ?**
  - Si vous utilisez les réponses automatiques sur du https (URL de réponse automatique configurée en https) alors vous devez migrer vers un serveur d'application compatible TLS1.2.
  - Les réponses manuelles ne sont pas concernées car il s'agit d'un flux entre vous et l'internaute.
- **J'utilise un compte FTP : suis-je impacté ?**
  - Selon le protocole de connexion, il existe un impact :
    - Les protocoles concernés sont les connexions en : PeSIT-HS_SSL ; FTP_SSL Serveur ; FTP_SSL Client. Pour ce type de connexion, la configuration du logiciel FTP utilisé devra être modifié pour accepter le protocole TLS 1.2
    - En revanche, il n'existe pas d'impact pour les sFTP (SSH/FTP).

* Uniquement pour les e-commerçants ayant souscrit l'offre Sogenactif après le 15/09/2016 (offre Sogenactif 2.0)

LES CONSÉQUENCES POUR VOS CLIENTS

- **Que se passe-t-il si le navigateur web de votre client utilise encore le protocole TLS 1.0 ou 1.1 ?**
  - Si votre client utilise un navigateur web obsolète, basé sur le protocole TLS 1.0 ou 1.1 , la page de paiement ne sera pas affichée. Il y aura un avertissement généré par le navigateur Web (cf. page 9)
- **Vos clients sont-ils impactés par ce changement ?**
  - Si votre client utilise un navigateur ou un appareil qui ne prend pas en charge le protocole de sécurité TLS 1.2, la page de paiement ne s'affichera pas. Il recevra un avertissement du navigateur Web.
  - En tant que e-commerçant, vous pourriez minimiser le risque de perte de transactions en conseillant à vos utilisateurs de mettre à jour leurs navigateurs.
  - La page Wikipedia sur le protocole TLS fournit un panorama global et complet des protocoles de sécurité pris en charge par les différents appareils et versions de navigateurs. https://en.wikipedia.org/wiki/Transport_Layer_Security

CONTACTS

Pour plus d'informations, vous pouvez contacter le support technique Sogenactif :

0825 090 095
Du lundi au vendredi de 9h à 19h (hors jours fériés)

supportsogenactif@worldline.com

#TEAMSPIRIT