PREREQUIS TECHNIQUES

Cegid RHP

SaaS

Version 1.01 du 08/07/2020
Document Public

cegid

SOMMAIRE

1. PREAMBULE 2
2. ACCES TELECOM SUPPORTES 2
3. DIMENSIONNEMENT DE VOS ACCES 5
4. PREREQUIS POUR LES POSTES DE TRAVAIL 6
5. PROTOCOLES TLS SUPPORTES 7

1. PREAMBULE

Ce document décrit les prérequis techniques associés à la solution Cegid RHP en mode SaaS (Software as a Service) éditée, hébergée et exploitée par Cegid.

Ce document couvre les prérequis techniques relatifs aux aspects réseau et Télécom, aux postes de travail, et aux périphériques. Le respect de ces prérequis techniques est essentiel au bon fonctionnement de la solution Cegid RHP. La responsabilité de Cegid ne pourra être engagée en cas de dysfonctionnement de la solution lié à leur non-respect.

Dans le cas d'une utilisation d'autres solutions Cegid, le Client doit s'assurer de respecter les recommandations communes à l'ensemble de l'offre proposée. Pour un conseil personnalisé, contactez votre Ingénieur Commercial.

Les Clients accèdent à leur solution Cegid RHP au travers d'une infrastructure Télécom mise en place par leurs soins en adéquation avec les recommandations techniques de Cegid décrites dans les paragraphes suivants.

Les modes de connexion possibles et les accès Télécom supportés en standard sont fonction de chaque solution Cegid RHP. Il convient néanmoins de noter les points suivants :

- La mise en place de certains accès Télécom pourra être sujette à devis et nécessiter une pré-étude technique.
- Toute demande de connexion et d'accès à la plateforme d'hébergement non standard devra être transmise à Cegid pour étude et validation. Cegid se réserve le droit de refuser la demande ou de la soumettre à devis.

2. ACCES TELECOM SUPPORTES

Le service Cegid RHP est accessible par l'ensemble des utilisateurs via un accès de type :

- Internet
- VPN

Les accès au Cloud Cegid peuvent être « mixés » avec une liaison VPN Orange Galerie et des accès en Internet Sécurisé.

Accès Internet Sécurisé

Le Client peut utiliser une ligne Internet grand public pour l'accès et l'utilisation de sa solution Cegid RHP.

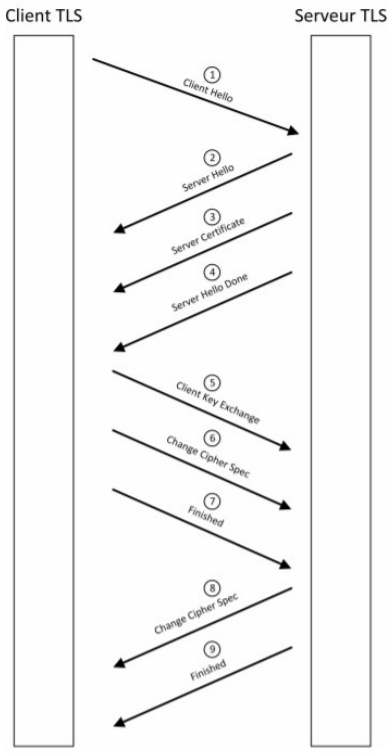
L'accès via Internet constitue le moyen le plus simple et le plus rapide à mettre en œuvre pour accéder à la plateforme SaaS. L'ensemble des données sont chiffrées lors des transferts avec des protocoles sécurisés. La plateforme SaaS utilise les protocoles suivants :

- HTTPS (TLS)
- SFTP (SSH)

Le protocole HTTPS correspond à la déclinaison sécurisée de HTTP encapsulé à l'aide d'un protocole de niveau inférieur nommé TLS. Ce protocole est conçu pour protéger en confidentialité et en intégrité des communications de bout en bout (entre un client et un serveur). Il apporte également des fonctions d'authentification du serveur.

La ligne Internet pourra être de type ADSL ou SDSL en accord avec les prérequis définis dans le paragraphe « dimensionnement de vos accès ». Ce paragraphe fourni également les débits minimums recommandés par Cegid.
Le Client pourra, s'il le désire, ou si le profile d'utilisation de sa ligne en dehors des flux interactifs avec la solution Cegid RHP le justifie, dédier une signe Internet pour l'utilisation exclusive de sa solution Cegid RHP et répondant aux prérequis techniques fournis dans ce document.
Dans ce cas Cegid recommande, lorsque c'est possible, d'opter pour un accès de type VPN avec la solution Orange VPN Galerie proposée par Cegid.
Le Client doit disposer d'un accès Internet répondant aux prérequis techniques décrit dans le paragraphe suivant et autoriser les connexions HTTPS (port tcp 443) à destination de la plateforme d'hébergement de Cegid.

Le schéma ci-dessous illustre le cas classique d'établissement d'une session TLS :



Dans l'optique de garantir le meilleur niveau de sécurité, les certificats HTTPS utilisés par Cegid proviennent d'autorités de certifications publiques et reconnues. Les certificats mis en place utilisent des clés de 2048bits et une signature en SHA256 conformément aux bonnes pratiques actuelles.

Les règles concernant la longueur des clés de chiffrement sont :
•Chiffrement asymétrique : supérieure ou égale à 2048bits
•Chiffrement symétrique : supérieure ou égale à 128bits mais 256bits conseillée si les systèmes l'acceptent.

La Production SaaS Cegid utilise un logiciel de chiffrement s'appuyant sur l'AES256 pour créer des archives sécurisées.

Cegid possède ses propres adresses IP publiques ainsi que plusieurs accès internet auprès de fournisseurs différents pour palier toute défaillance d'un fournisseur et ainsi fournir à ses clients le niveau de service attendu.

Accès VPN

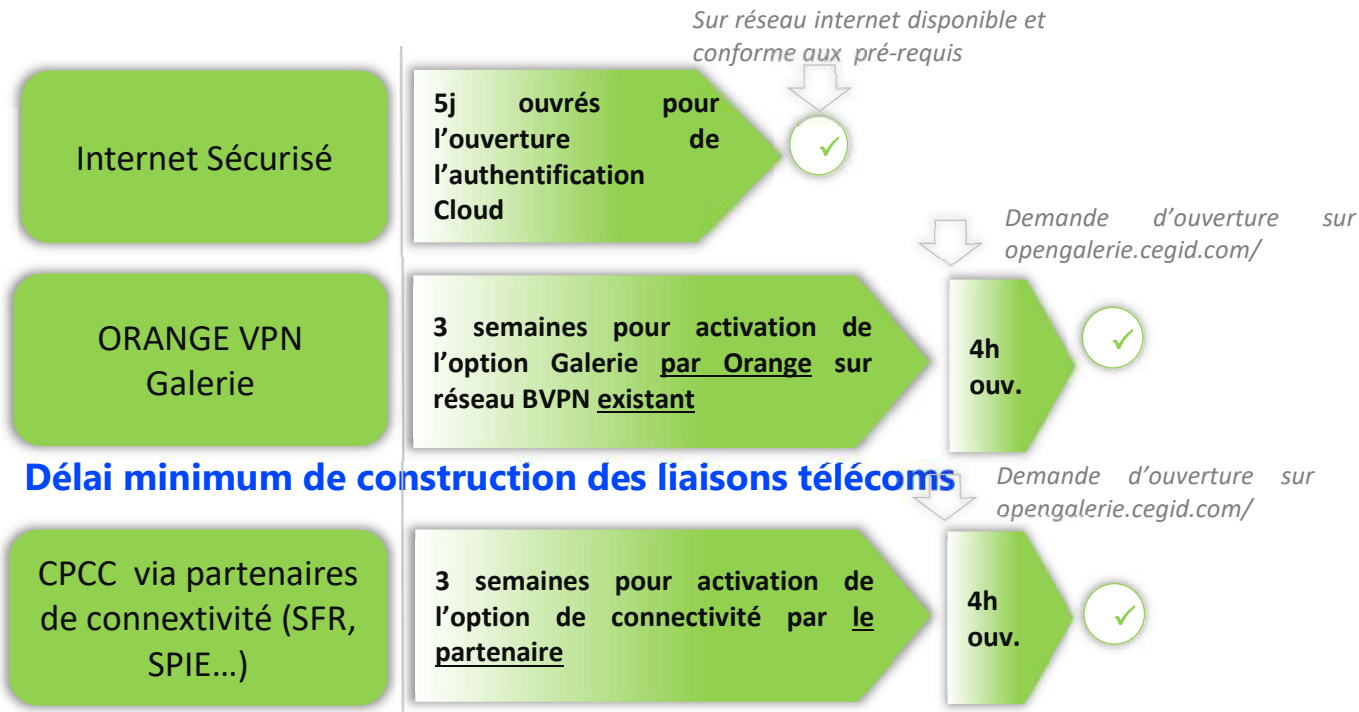
Cet accès permet aux Clients d'étendre facilement leur réseau VPN Orange vers la plateforme d'hébergement de Cegid elle-même raccordée au Backbone d'Orange. Les centres d'hébergement Cegid sont en effet déjà intégrés au réseau Orange BVPN Galerie. Les Clients disposants d'une infrastructure BVPN contractualisée auprès d'Orange peuvent donc souscrire à l'option Galerie et étendre ainsi leur réseau privé aux data centers Cegid.
Toute demande de raccordement VPN, en dehors de la solution standard proposée par Cegid en partenariat avec Orange, sera traitée comme une demande spécifique et sera soumise à devis et acceptation par Cegid (cf. Délai minimum de construction des liaisons télécoms).
S'il le désire le Client peut renforcer la qualité de service de son accès à sa solution Cegid RHP en implémentant les options de backup proposées par Orange et décrites ci-dessous :

Backup option 1	Backup option 2
Redondance niveau 1 – Always On Ligne de secours bas débit permettant de prendre le relai et d'assurer la continuité du service en cas de problème sur la liaison VPN principale.	Redondance niveau 1 – Dual Backup Ligne de secours identique à la liaison VPN principale permettant de prendre le relai de manière transparente et d'assurer la continuité du service en cas de problème sur la liaison VPN principale

D'autres options de backup peuvent être étudiées sur demande. Veuillez-vous rapprocher de votre Ingénieur Commercial.

Schéma Solution Télécom recommandée et délais minimum de construction des liaisons :

Standard



Délai minimum de construction des liaisons télécoms

3. DIMENSIONNEMENT DE VOS ACCES

Le dimensionnement de vos accès à votre solution Cegid RHP dépend de plusieurs critères :

- Les préconisations spécifiques à chaque solution et fournies par Cegid
- L'utilisation de votre solution Cegid RHP
- Les utilisations annexes de votre accès Internet en dehors de votre solution Cegid RHP (surf, messagerie etc…)

Les préconisations techniques pour l'accès à votre solution Cegid RHP sont résumées ci-dessous :

Nombre d'utilisateurs simultanés	Débit minimum de ligne recommandé	Latence
Moins de 3	1Mb/s	100ms maximum
De 3 à 10	2Mb/s	
De 10 à 50	4Mb/s	
De 50 à 150	6Mb/s	
De 150 à 300	8Mb/s	
Plus de 60	Étude spécifique	

* En ADSL, des coupures et des ralentissements liés à cette technologie pourront être observés

Notes importantes :

- Les préconisations sont valides uniquement dans le cadre de sessions interactives avec l'application en ligne Cegid RHP.
- Ces préconisations ne prennent pas en compte les besoins en bande passante nécessaires à l'exécution d'autres applications que Cegid RHP, à l'échange d'information avec d'autres applications du Système d'Information ou avec la plateforme (type échange de fichiers ou téléchargement de documents) et au support des autres types de flux Internet du Client comme la navigation Internet ou la messagerie …
- En cas de flux annexes significatifs, Cegid préconise l'utilisation d'un accès dédié aux flux applicatifs de la solution Cegid RHP et notamment l'utilisation d'Orange VPN Galerie lorsque c'est possible.
- La responsabilité de Cegid ne pourra être engagée en cas de non-respect par le Client des prérequis techniques fournis dans ce document.

4. PREREQUIS POUR LES POSTES DE TRAVAIL

Ces préconisations sont liées au bon fonctionnement de la solution Cegid RHP.
Attention, l'utilisateur faisant l'installation et les mises à jour doit obligatoirement être de niveau Administrateur sur le poste.

Prérequis hardware et système

Architecture	Système	Mise à jour	Mémoire minimale	Mémoire conseillée	Processeur Intel	Carte vidéo
64 bits (x64)	Windows 8.1 Professionnel	Min SP1	2 Go	4 Go	2 GHz - 64bits (x64)	16 millions de couleurs en 1024x768
64 bits (x64)	Windows 10 Professionnel		3 Go	4 Go	2 GHz - 64bits (x64)	16 millions de couleurs en 1024x768

- 1 Go de disque disponible en prévision du stockage local des fichiers « utilisateur » pour les postes ayant un disque dur. Si non prévoir un stockage réseau.
- Carte vidéo configurée en « taille normale ou petite police ».

Autres prérequis pour le poste de travail

Type	Produit et version requis	Utilisation	Informations complémentaires
Navigateur	Chrome 59 minimum Firefox 54 minimum Internet Explorer 11 minimum	- URL d'accès à l'application du Client - Accès au site : https://www.cegidlife.com - Navigateurs compatibles HTML5 et CSS3	L'url du site d'accès à l'application doit être ajoutée au « paramètre d'affichage de compatibilité », aux sites de confiance et bloqueur de fenêtre Windows
Utilitaire	Adobe Acrobat Reader version 11 minimum	Lecture document PDF générés par l'application	
Utilitaire	Client Citrix Ica Web V14.x minimum	Accès à l'application Cegid RHP	Fourni par Cegid selon les modalités décrites dans le document d'installation
Utilitaire	Client Thinprint V10.x minimum	Pour la gestion des tâches d'impression avec l'application Cegid RHP	

Bureautique	Suite bureautique*	Lecture locale des fichiers générés par l'application Cegid RHP.	*.doc, *.docx, *.xls, *.xlsx
Disque local	Accès aux ressources local du poste utilisateur	La connexion au Cloud Cegid « remappe » automatiquement le disque c : local du Client en v : au moment de l'accès. La lettre w : est également nécessaire au moment de la connexion.	Les lettres v : et w : doivent donc être libérées sur le poste utilisateur

Attention :

- Un antivirus à jour est obligatoire sur chaque poste avec mise à jour régulière des signatures.

Dans le cas d'une connexion intermittente via Internet de type « ADSL » : le navigateur « Web » doit disposer de l'option « cryptage 128 bits ».

* Cegid RHP est compatible avec Office 2016 et Office 365

5. PROTOCOLES TLS SUPPORTES

Définition : TLS (Transport Layer Security - anciennement SSL)

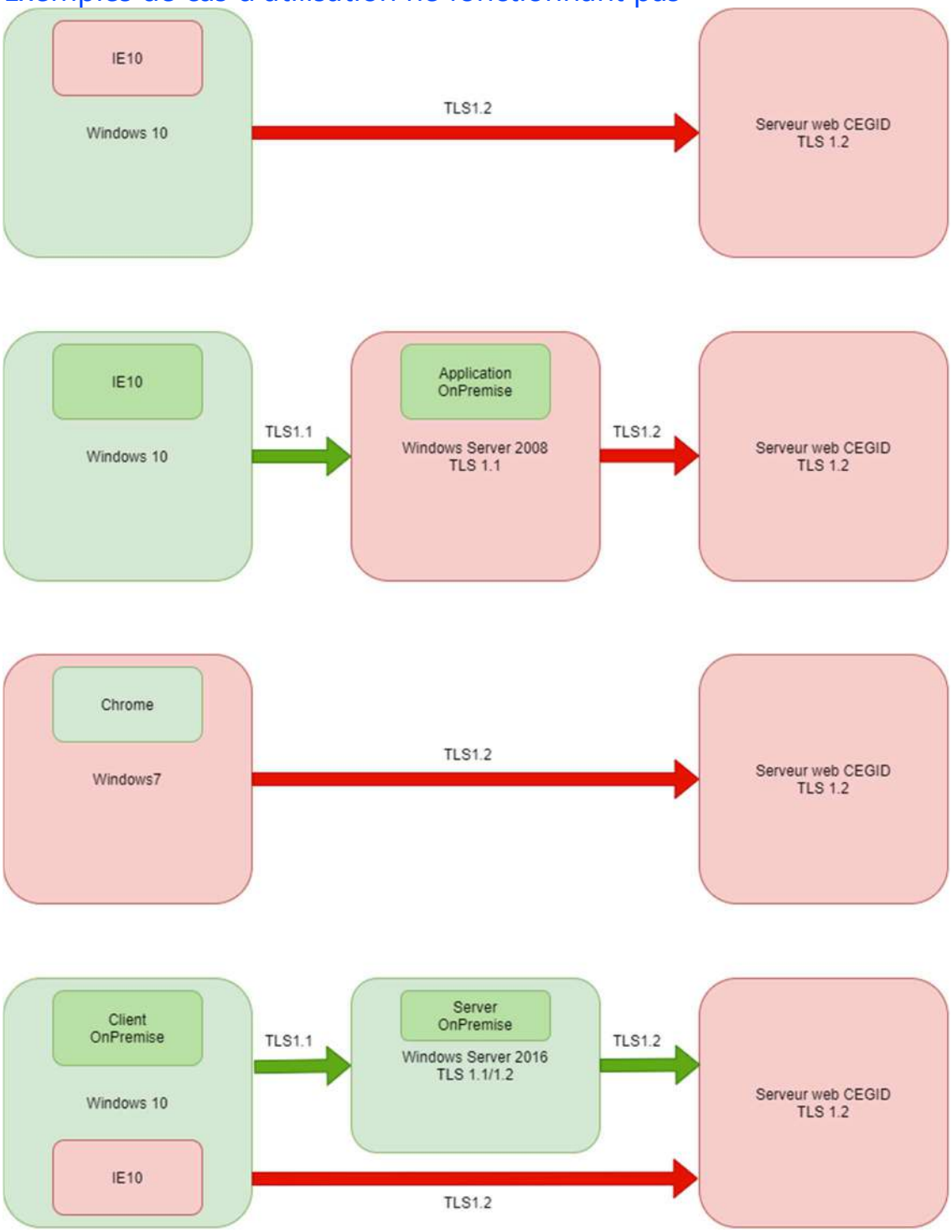
TLS est un protocole qui assure la confidentialité des échanges entre les applications de communication et les utilisateurs sur Internet. TLS s'assure qu'aucun tiers ne peut intercepter ni falsifier une communication. C'est ce protocole qui est mis en œuvre lors de la connexion à un site web en https par exemple.
Celui-ci se décline en plusieurs versions évoluant au fil du temps en fonction des avancées technologiques avec comme but de renforcer la solidité et la confidentialité des échanges.

Cegid n'assurant plus la compatibilité de ses solutions avec les versions TLS 1.0 et TLS 1.1 (celles-ci présentant des failles potentielles de sécurité) , certains sites web ou applications ne sont plus accessible à partir d'anciens navigateurs ou systèmes d'exploitation. La tentative se solde par une erreur de connexion.

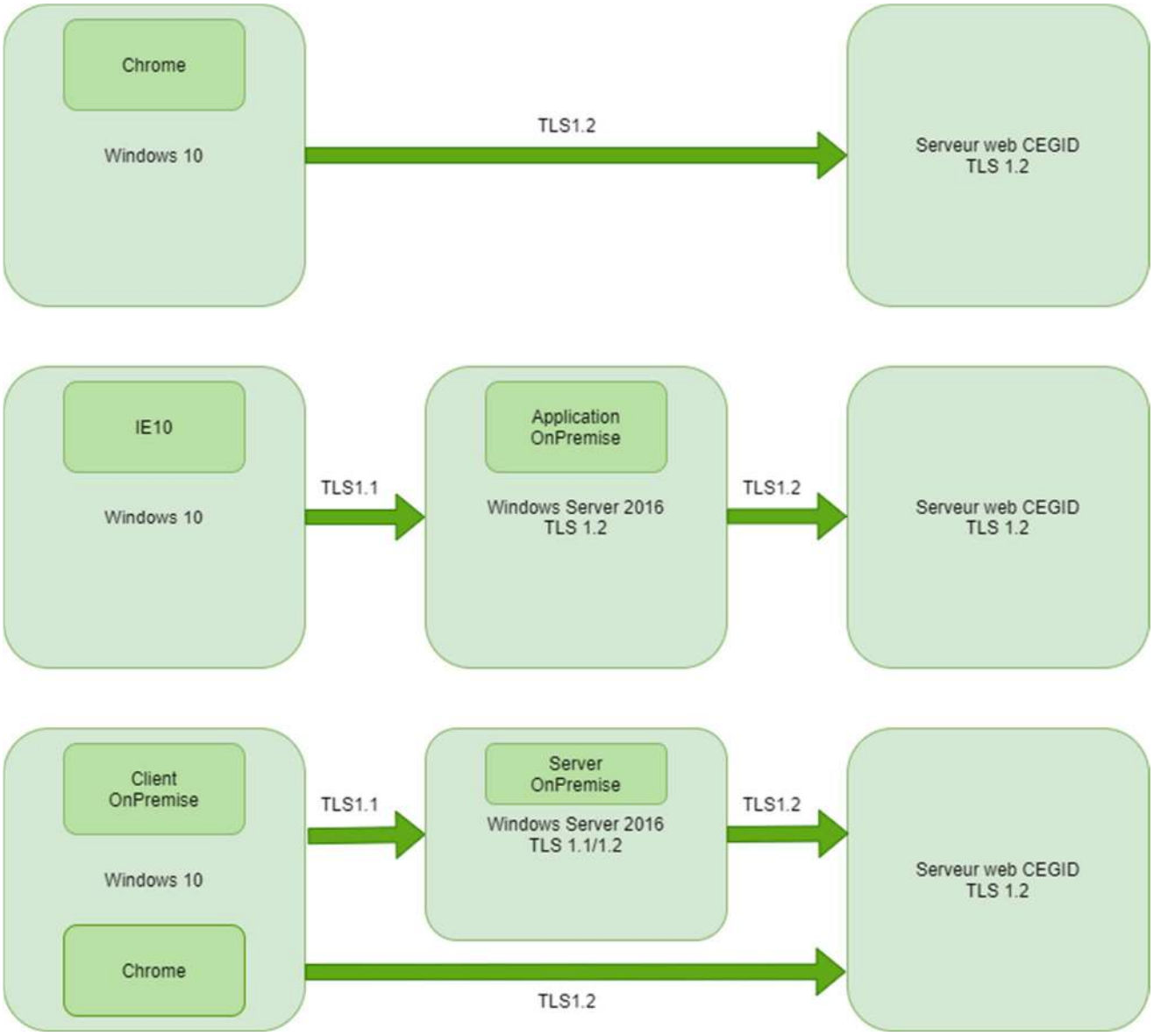
Seul le protocole TLS 1.2,, permet de consommer un service Cegid, il faut donc avoir un navigateur ET un système d'exploitation le supportant.

Se référer aux prérequis système et poste de travail du chapitre 4 pour les version compatibles TLS 1.2

Exemples de cas d'utilisation ne fonctionnant pas



Exemples de cas d'utilisation fonctionnant



Pour aller plus loin

Une liste plus complète des navigateurs et OS supportant TLS1.2
https://caniuse.com/#feat=tls1-2
https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility

Pour plus d'information sur la Transport Layer Security
https://fr.wikipedia.org/wiki/Transport_Layer_Security
https://openweb.eu.org/articles/https-de-ssl-a-tls-1-3