



RAPPORT DU CONSEIL D'ÉTAT AU GRAND CONSEIL

**sur le Postulat Jean-François Chapuisat et consorts au nom du groupe Vert'libéral –
Pour une solution de visioconférence fiable, conviviale, et sécurisée ! (20_POS_220)**

Rappel du postulat

Suite aux différentes mesures de précaution sanitaire prises en lien avec l'épidémie de coronavirus, la Direction générale du numérique et des systèmes d'information (DGNSI) n'a eu que très peu de temps pour préparer toutes les actions qui allaient être mises en place au niveau de ses prérogatives afin d'assurer la continuité des missions de l'État.

Du jour au lendemain, le Conseil d'État a dû décider de mettre une grande partie de l'administration au télétravail. Des milliers de collaborateurs se sont mis à travailler à distance. C'est dans ces conditions que la DGNSI a mis en place l'outil Cisco Webex pour les visioconférences. Des contrats existants avec Cisco pour du matériel informatique englobaient l'utilisation de Webex. C'est donc l'outil que les députés utilisent pour la tenue de commissions en visioconférence.

Cette solution, outre certains aspects d'ergonomie qui s'améliorent avec le temps, n'offre peut-être pas des garanties de sécurités optimales. Même si les serveurs sont désormais en Europe, alors qu'ils étaient situés aux États-Unis au départ, l'entreprise Cisco est américaine et donc soumise au patriot act.

De plus, des sociétés vaudoises ou romandes, telles qu'Infomaniak ou Nimag, ont développé des solutions intéressantes, utilisant des solutions open source et ayant des serveurs basés en Suisse. Même si elles ne sont peut-être pas encore tout à fait équivalentes techniquement, elles méritent d'être prises en compte dans la réflexion, voire, pourquoi pas, soutenues dans leur développement en vue d'une utilisation par le Grand Conseil.

Dans la perspective du dépôt de ma motion « Pérennisation de la tenue de certaines commissions en visioconférence (20_MOT_153) », j'ai le plaisir de faire la demande suivante :

Je demande au Conseil d'État d'étudier la possibilité de mettre en place une solution pour les visioconférences qui soit fiable, conviviale, sécurisée, et si possible locale.

Rapport du Conseil d'Etat

1. RAPPEL DU CONTEXTE ET DES ENJEUX

1.1 Quelques considérations

Avec le postulat « Pour une solution de visioconférence fiable, conviviale et sécurisée » déposée par M. Jean-François Chapuisat et consorts, les députés reconnaissent la nécessité d'une solution de vidéoconférence (« solutions VC ») pour poursuivre le travail à distance tant au sein de l'Administration cantonale vaudoise (ACV) qu'au sein du Parlement. Au début de la crise sanitaire, la Direction générale du numérique et des systèmes d'information (DGNSI) a déployé l'outil Cisco Webex et, dans l'intervalle, d'autres solutions ont rejoint ce marché en plein essor dû à la généralisation du télétravail. Les postulants souhaitent que le Conseil d'Etat (CE) évalue les solutions existantes sous différents angles, puisque l'outil de visioconférence est appelé à être pérennisé.

Le choix d'un outil de vidéoconférence faisait déjà partie d'une réflexion au sein de la DGNSI avant la période de crise. Réflexion qui s'inscrit dans sa stratégie liée à l'environnement de travail des collaboratrices et collaborateurs de l'Administration cantonale. Dès septembre 2019, une première période d'analyse avait permis d'identifier la suite d'outils Webex, développée et supportée par Cisco, comme la solution la plus appropriée pour offrir aux utilisatrices et utilisateurs un environnement de travail mobile et moderne, en phase avec l'évolution technologique et les nouvelles habitudes de travail à distance. En effet, en plus de soutenir un mode de travail collaboratif et de vidéoconférence, cette solution s'intègre aux outils existants et offre une assurance en matière de chiffrement et de sécurité des données.

Aujourd'hui, la période de crise a confronté la DGNSI à une utilisation intensive de l'outil de vidéoconférence. Suite à différents retours d'expérience en interne et en externe, la DGNSI a mené une analyse globale avec une revue des différents acteurs et des outils du domaine, qui permettra de répondre à certains besoins impératifs qui font partie de la stratégie « environnement de travail numérique » : la fonctionnalité, la performance, la sécurité, la maintenabilité, la facilité d'utilisation, la fiabilité, la portabilité et la compatibilité. Le télétravail, qui permet de réduire les déplacements des collaboratrices et collaborateurs et d'améliorer la flexibilisation des espaces de travail, sera favorisé à l'avenir. Ainsi, le périmètre des besoins fonctionnels en matière de vidéoconférence couvre le Conseil d'Etat, le Grand Conseil et ses Commissions, l'Administration cantonale ainsi que des organismes bénéficiant de services informatiques de l'administration et des prestataires externes à l'Etat (fournisseurs, communes, partenaires paraétatiques). Il est important qu'une solution identique soit proposée à l'ensemble de ces acteurs.

1.2 Définitions, principaux acteurs et produits du marché des VC

1.2.1 Définitions, fonctionnalités, appareils et mode d'accès

Les solutions de vidéoconférence (« solutions VC ») proposent comme service de base des transmissions vidéo et audio entre plusieurs participants. On parle d'appel s'il s'agit de deux participants, et de conférence à partir de trois. Une conférence a des exigences technologiques plus importantes qu'un appel, car la synchronisation des pistes audio et vidéo entre tous les participants doit être assurée. Dans la suite de l'analyse, la DGNSI a exclu de fait les solutions de téléphonie simple, les solutions sans vidéo et les solutions propriétaires fermées.

Trois types de conférences sont à prendre en compte : conférences ouvertes/publiques, conférences internes et conférences confidentielles. Dans la pratique, ceci correspond au niveau de protection 1+ de l'ordonnance fédérale sur la protection de l'information. La solution ne doit pas couvrir des informations classées militaires (niveau 2 et 3).

Outre les fonctionnalités de la vidéoconférence de base (vidéo, audio), le champ fonctionnel d'une solution VC est plus large. Elle nécessite des fonctions, telles que la fonction de sourdine et la possibilité d'ajouter des participants dans la conférence. D'autres fonctionnalités sont considérées utiles pour gérer des réunions formelles, telles que le rôle du conférencier/modérateur ou la salle d'attente, ainsi que la messagerie instantanée et le partage de contenu d'écran.

Le besoin d'une solution de vidéoconférence sécurisée est devenu encore plus urgent dans le cadre de la pandémie de COVID-19, et celle-ci doit donc être utilisable non seulement sur le lieu de travail, mais aussi de manière mobile et sur divers points de terminaisons. La DGNSI a identifié quatre classes majeures d'appareils et de terminaux qui peuvent participer à des conférences : ordinateur/PC, téléphone mobile et tablettes, téléphones vidéo ou systèmes vidéo et le serveur central sur lequel est installée une partie de la solution VC. Différents niveaux de sécurité sont donc proposés pour ces produits :

- La sécurité de base : la solution s'appuie sur la sécurité du serveur central et des appareils terminaux, et se fie pour les connexions à la sécurité de l'infrastructure (p. ex. les réseaux). Les conférences ne sont pas cryptées.
- La sécurité augmentée : sécurité informatique de base où les conférences entre le serveur et tous les appareils terminaux sont cryptées par la solution VC.
- Enfin, la sécurité de bout en bout : sécurité informatique de base où les conférences entre les appareils terminaux sont cryptées par la solution VC et le serveur n'a pas accès au contenu, équivalent de la notion de « zero knowledge encryption »

1.2.2 Vue d'ensemble des produits et producteurs majeurs

Il existe deux types d'acteurs importants :

a. Éditeurs

Les éditeurs élaborent l'écosystème (code source compris) composé de l'application, du serveur et des appareils terminaux. Il n'y a pas d'écosystème complet qui soit édité en Suisse. Les éditeurs principaux sont Cisco, Microsoft, Avaya, Huawei, Unify. Il existe un certain nombre d'autres éditeurs dits de deuxième niveau, exclus de cette analyse, qui proposent des écosystèmes limités, p. ex. sans logiciel PC ou sans connexion externe.

Un cas particulier sont les logiciels libres (« Free and Open Source, FOSS »), où il n'y a pas d'éditeur central, mais un collectif qui édite le logiciel. Cependant, vu la complexité très élevée de la visioconférence, il y a dans tous les projets majeurs de VC une entité commerciale qui assure l'évolution de l'écosystème – la VC présente une constellation atypique dans le monde des FOSS.

b. Intégrateurs

Les intégrateurs sont des entreprises qui ne disposent pas elles-mêmes d'un produit, mais qui ont la capacité d'intégrer des solutions existantes et de les adapter. Les intégrateurs assemblent des solutions ou complètent une solution existante pour fournir un produit fonctionnel dans un nouveau contexte global.

Dans le cas présent du postulat, plusieurs sociétés romandes ont été mentionnées. Elles sont considérées comme des intégrateurs. Leurs rôles et offres seront abordés plus loin.

Un tableau récapitulatif des produits et producteurs majeurs est proposé ci-dessous et donne une idée de leur couverture fonctionnelle globale.

Solution	Fournisseur (pays)	Couverture des exigences	Sécurité	Modèle de déploiement
Unified Communications Manager (CUCM)	Cisco (US)	Solution haut de gamme, leader mondial, utilisée par des administrations publiques (CH, Etat de Vaud, autres cantons)	Base, augmentée	Sur site (<i>fin du cycle de vie probable</i> ¹)
Webex	Cisco (US)	Solution haut de gamme, leader mondial, utilisée par des administrations publiques (CH, État de Vaud, autres cantons)	Bout en bout, augmentée	Cloud Sur site (<i>non recommandé</i>)
Skype for Business	Microsoft (US)	Solution haut de gamme, leader mondial, utilisée par des administrations publiques (CH, autres cantons)	Augmentée	Sur site (<i>fin du cycle de vie probable</i>) Cloud (<i>fin du cycle de vie annoncée</i>)
Teams	Microsoft (US)	Solution haut de gamme, leader mondial	Augmentée	Cloud
Zoom	Zoom (US)	Solution Visioconférence	Augmentée	Cloud
Aura	Avaya (US/CA)	Solution haut de gamme utilisée par des administrations publiques (CH, autres cantons)	Base, augmentée	Sur site, Cloud
Poly	Poly (US)	Equipements haut de gamme utilisés par des administrations publiques (CH)	Base, augmentée	Sur site, Cloud
CloudLink Video Conferencing	Huawei (CN)	Solution haut de gamme	Base, augmentée	Cloud
Wire Enterprise	FOSS, Wire (CH/DE)	Solution Open Source, focus maximal sur sécurité, avec sécurité end2end	Bout en bout	Sur site, Cloud
Jitsi	FOSS, 8x8 (US)	Solution Open Source, focus maximal sur convivialité, avec sécurité augmentée, sécurité end2end expérimentale	Augmentée (bout en bout expérimental)	Sur site, Cloud
SIPFoundry, Elastix, Livestorm, Big Blue Button	FOSS, divers	Solutions Open Source	Base	Sur site, Cloud

1.2.3 Solutions commerciales

Les produits commerciaux pour VC ont l'avantage d'être largement utilisés dans diverses industries. La vente, la conception, la mise en œuvre, la maintenance et l'exploitation professionnelles par le fournisseur et ses partenaires sont garanties. Il est également assez facile de développer un savoir-faire interne, qui peut s'appuyer sur des certifications et des formations établies. Presque tous les fournisseurs peuvent assurer ou prendre en charge l'intégration des solutions correspondantes via des architectures « plug-in » ou des interfaces de programmation d'applications, mais l'effort reste du ressort du partenaire de mise en œuvre. Certaines solutions dites COTS (« Commercial Off the Shelf », produit commercial sans adaptation spécifique au client) couvrent une large gamme de produits commerciaux qui, en plus d'un client logiciel, comprennent également des appareils terminaux, tels que des appareils de salle ou des visiophones. Des exemples de fournisseurs de solutions COTS dans le domaine de la VC pertinents sont, par exemple, Cisco (UCM et Webex), Huawei, Avaya et Polycom.

Les deux solutions commerciales installées à l'ACV sont détaillées ci-dessous. Les autres seront décrites dans le chapitre 3.

¹ On peut constater déjà un ralentissement des investissements Cisco dans le produit en faveur de WebEx, cependant Cisco n'a pas une politique de cycle de vie agressive, contrairement à Microsoft.

a. Cisco UCM

Cisco UCM repose sur un déploiement à partir de centres de données centralisés. En règle générale, les gestionnaires d'appels sont déployés sur du matériel propriétaire Cisco. Il s'agit de la ligne de produits traditionnelle de Cisco, comparé à Webex, qui n'est plus considérée comme stratégique pour Cisco.

Dans la ligne de produits Cisco, les serveurs Cisco UCM peuvent servir aussi bien des vidéoconférences que des appels téléphoniques. L'ACV utilise aussi Cisco UCM comme solution téléphonique.

Cisco UCM dispose d'un client logiciel (Jabber), qui se caractérise par une intégration étroite avec divers produits Microsoft, tels qu'Outlook et SharePoint par les API natives de Microsoft. Cisco dispose d'une large gamme de terminaux téléphoniques et est particulièrement performant dans le domaine de la VC.

Cisco UCM est un système complet provenant d'une source unique et hautement éprouvée. Les outils de gestion sont très éprouvés et riches en fonctionnalités. Toutes les fonctionnalités liées au réseau sont l'une des forces de Cisco comme leader mondial des équipements réseaux. L'État de Vaud utilise Cisco UCM dans des environnements sensibles, dans le cas notamment des appels de la Police cantonale (traitements des appels d'urgence, central d'engagement 117, etc.).

b. Cisco Webex

Webex est la deuxième ligne de produits VC de Cisco. Il s'agit d'une solution basée dans le Cloud. Le produit est très mature et utilisé par des millions d'utilisateurs, ce qui a été démontré avec l'échelonnement rapide durant la pandémie. Webex possède un riche ensemble de fonctionnalités, comme un lobby vidéo, de la gestion avancée de réunions et des fonctions de modérateur puissantes. Les salles privées permettent de mener des discussions confidentielles dans un cercle plus restreint. L'authentification à deux facteurs est mise en œuvre et il est possible, par exemple, de stocker un identifiant qui peut être vérifié lors de la participation à une conférence.

Pour les clients gouvernementaux, notamment des parlements et gouvernements, Webex regroupe et augmente ces fonctionnalités dans le cadre de « Legislate for Webex », par exemple une mise en œuvre de processus législatifs à l'aide de rôles intégrés, tels que la fonction de minuteur, une fonction d'ordre du jour et l'attribution de droits de parole.

Parmi les exemples de références pour Webex, citons la Banque Centrale européenne, le Gouvernement des Pays-Bas, où l'ensemble de l'appareil politique est désormais passé à Webex (environ 100 000 personnes), l'Administration fiscale britannique et le National Health Service.

Un audit du code source est possible au Trust Access Point, à Rolle. Des tests d'intrusion sont également possibles.

L'État de Vaud utilise Cisco Webex à large échelle.

1.2.4 Solutions libres (*Free and Open Source Solutions, FOSS*)

Avec les logiciels FOSS, ce n'est pas une entreprise, mais une communauté de développeurs qui les soutient. Le principe fondamental est le caractère volontaire de cette communauté, qui représente un très grand réservoir de ressources et de savoir-faire. Le terme Free and Open Source Software peut être utilisé dans un contexte restreint (se limitant à tous les logiciels sous la licence GPL) ou large, ce qui englobe toutes les licences sur la liste de l'Open Source Initiative. La vérification de la licence Open Source est une activité importante dans un projet informatique, car il existe des licences incompatibles avec une utilisation commerciale ou étatique.

Les produits présentés ci-dessous, les plus pertinents, possèdent de la sécurité augmentée ou end2end. Voici, en bref, le modèle de licence pour chacun d'eux :

a. Wire

Wire se compose de trois services différents dans le domaine du VC sécurisé : Wire Pro (conférences dans l'équipe), Wire Enterprise (conférences dans l'entreprise/institution) et Wire Red (envoi de messages en cas de crise). L'accent est clairement mis sur la sécurité et la transparence. Le siège de la société est situé en Suisse (Wire Swiss GmbH à Zoug). Les références comprennent le Gouvernement fédéral allemand (conforme aux normes BSI), EY (Ernst & Young) et l'UNICEF.

Wire Enterprise permet l'intégration automatisée de Wire dans le paysage informatique de l'entreprise : synchronisation de l'Active Directory (AD), Single Sign-On via SAML 2.0, utilisation des API, etc. Comme avec Wire Pro, toutes les fonctions sont cryptées de bout en bout. En outre, Wire Enterprise est disponible dans le Cloud et sur site. La solution est 100 % open source et conforme aux normes CCPA/DSGVO.

Caractéristiques de la licence Open Source :

- Le produit peut être utilisé à des fins commerciales
- L'utilisation des brevets est incluse
- Le logiciel n'est pas accompagné de garanties ni de prise de responsabilité
- Des changements et la distribution du logiciel sont possibles, mais sous conditions.

La licence est donc compatible avec les cas d'utilisation qui pourraient être envisagés.

b. Jitsi

Jitsi est une collection de projets open source qui fournit des fonctionnalités de VC. L'objectif du projet est de fournir une solution conviviale et facile à héberger soi-même. Les services standards sont hébergés dans le Cloud (Oracle Cloud Infrastructure, OCI). Le cryptage de bout en bout est actuellement à l'état expérimental¹. D'après les indications Jitsi, le cryptage de bout en bout est disponible, mais la documentation cryptographique² n'est pas sur le même niveau que pour Wire et ne permet pas actuellement de vérifier si elle correspond à l'exigence bout en bout, notamment si le serveur est capable d'inspecter le contenu de la communication. Pour une évaluation cryptographique et une revue du code, une documentation du concept cryptographique est indispensable et ne peut pas être remplacée par une pure inspection du code, sans valider le concept de sécurité. En aout 2021, jitsi meet a publié un « document blanc »³ sur la sécurité du produit. Ce document concis et compact montre un notable progrès, mais liste un certain nombre de restrictions de l'implémentation, parmi lesquelles une limite de participants et l'absence de protection contre des attaques d'*Insiders* (menaces internes). Ce constat est partiellement en contradiction avec les éléments⁴ du site web présents actuellement et non référencés sur le site web jitsi.

En 2018, l'équipe de développement et la technologie de Jitsi ont été acquises par 8x8, une firme américaine. Caractéristiques de la licence Open Source :

- Le produit peut être utilisé à des fins commerciales.
- L'utilisation des brevets est incluse.
- Le logiciel n'est pas accompagné de garanties ni de prise de responsabilité.
- La marque Jitsi est réservée.
- Des changements et la distribution du logiciel sont possibles, mais sous conditions.

La licence est donc compatible avec les cas d'utilisation qui pourraient être envisagés.

1.2.5 Intégrateurs

Les intégrateurs sont des entreprises qui ne disposent pas elles-mêmes d'un produit, mais qui ont la capacité d'intégrer des solutions existantes. Ils combinent des solutions ou complètent une solution existante afin de fournir un produit fonctionnel dans un nouveau contexte global. Dans le cas présent, il s'agirait d'entreprises qui ajoutent une composante de sécurité aux solutions de VC existantes (sans modifier la solution elle-même) afin de fournir une solution de VC sécurisée. Il y a un grand nombre d'intégrateurs pour chacun des produits mentionnés dans les chapitres ci-dessus, dont une ou plusieurs firmes suisses. La plupart des éditeurs mettent à disposition des outils de recherche de partenaires en fonction des compétences requises.

Exemples⁵ d'intégrateurs :

- Netcloud, IBM, Bithawk, Swisscom : solution Cisco
- Swisscom, iSolutions, Atos : solution Microsoft
- Infomaniak (sous la marque kMeet), Hostpoint (sous la marque Hostpoint Meet), walkingtowel : solution Jitsi

A noter qu'un intégrateur suisse restera limité par les propriétés du produit choisi. Si le produit possède une faille intentionnelle (backdoor) placée par un organisme étranger, l'intégrateur ne sera pas nécessairement en mesure d'y remédier. Même dans le cas des logiciels FOSS, où le code source est librement disponible, un audit du code est impossible en pratique. Une inspection du code complet est un projet de large envergure qui devrait être répété à chaque nouvelle version.

¹ <https://jitsi.org/e2ee-in-jitsi/>

² La documentation sur le site date de d'avril 2020 et n'a pas connu de mise à jour : <https://jitsi.org/blog/e2ee/>

³ <https://jitsi.org/wp-content/uploads/2021/08/jitsi-e2ee-1.0.pdf>

⁴ <https://jitsi.org/e2ee-in-jitsi/>

⁵ Cette liste n'est pas exhaustive et ne constitue aucune recommandation. Les services d'intégrateurs non mentionnés peuvent être identiques ou supérieurs.

1.3 Modèles d'hébergement

1.3.1 Sur site/On Premise

L'entreprise a la possibilité de mettre en place le système elle-même et de l'exploiter en interne sans l'aide supplémentaire d'autres fournisseurs externes. Il y a également des variantes hybrides, sur le site d'un fournisseur ou sous forme de Managed Service, c'est-à-dire avec la maintenance et les mises à jour gérées et exploitées à distance par un opérateur.

1.3.2 Cloud

Au lieu d'un hébergement sur site, la plateforme est hébergée dans un Cloud, généralement sur une plateforme partagée avec d'autres clients, mais avec une séparation des données. Certains produits permettent également un modèle *zero-knowledge*, où aucune donnée n'est divulguée à la plateforme Cloud, notamment Cisco Webex et Wire.

La solution est soumise à des exigences élevées en matière de cybersécurité. Les fournisseurs de Cloud publics, en particulier, ont un niveau de sécurité très élevé en matière de cybersécurité, car ils sont sous attaque en permanence.

2. CRITÈRES D'ÉVALUATION D'UNE SOLUTION VC

2.1 Critères d'évaluation d'un logiciel

La qualité d'un logiciel peut être estimée avec un modèle de qualité qui détermine ses caractéristiques essentielles. ISO 25010 est le standard le plus utilisé au monde. Les critères d'évaluation selon ISO 25010 sont la fonctionnalité, la performance, la sécurité, la maintenabilité, la facilité d'utilisation, la fiabilité, la portabilité, et la compatibilité.

2.2 Critères d'évaluation dans notre contexte

Dans leur énoncé, les postulants demandent au CE « *d'étudier la possibilité de mettre en place une solution pour les visioconférences qui soit **fiable, conviviale, sécurisée, et si possible locale*** ». Ces critères d'appréciation correspondent en partie aux caractéristiques standards de qualité d'un logiciel. Les caractéristiques de fiabilité, convivialité (facilité d'utilisation) et sécurité se laissent directement aligner à certaines dimensions d'ISO 25010. L'hébergement en Suisse (solution locale) est une dimension à compléter. Il s'agit donc des quatre critères d'évaluation qui appuieront les explications qui vont suivre.

2.2.1 Fiable

La fiabilité est considérée selon l'ISO 25010 comme un système, un produit ou une composante qui remplit des conditions spécifiques pendant une certaine période. L'importance est surtout axée sur la maturité, la disponibilité, la tolérance aux pannes matérielles ou logicielles, et la récupérabilité des données affectées.

2.2.2 Conviviale

Le volet de la convivialité est défini dans l'ISO 25010 sous le point de l'utilisabilité et considère l'atteinte d'objectifs avec efficacité, efficience et satisfaction du degré d'utilisation d'un produit ou système par des utilisateurs spécifiques. L'ISO 25010 valorise surtout les caractéristiques de la reconnaissance appropriée, de l'apprentissage de l'utilisation du produit/système, de l'exploitabilité, de la protection contre les erreurs de l'utilisateur, de l'esthétique de l'interface utilisateur, et de son accessibilité.

2.2.3 Sécurisée

La sécurité est censée protéger les informations et données de façon à ce que toutes les personnes ou tous les produits et systèmes disposent d'un cryptage correspondant à leurs types et niveaux d'autorisations, mais concerne aussi la transmission, le stockage, le traitement des données et des métadonnées. L'ISO 25010 considère surtout comme importantes les sous-caractéristiques de la confidentialité, l'intégrité, la non-répudiation, la responsabilité et l'authenticité de la sécurité des données.

2.2.4 Locale

La localisation n'est pas définie dans la norme ISO et une telle exigence entre en contradiction avec le principe de l'interdiction des discriminations applicable en droit des marchés publics et consacré aux articles 11, alinéa 1, lettre a de l'Accord intercantonal sur les marchés publics (AIMP 1994/2001) et 6, alinéa 1, lettre a de la loi du 24 juin 1996 sur les marchés publics (LMP-VD).

De ce fait, l'État de Vaud ne peut pas exclure d'office des entreprises étrangères d'un marché public. Pour satisfaire aux exigences de la législation sur les marchés publics et au présent postulat, il faut définir une exigence fonctionnelle qui permettrait de satisfaire ce critère, sans exclure d'office les entreprises étrangères.

a. Localisation de l'éditeur

Dans cette dimension, la question sous-jacente est la possibilité de l'intervention d'un État étranger sur l'éditeur relatif au placement d'un *backdoor* dans le code. Il est relativement difficile d'estimer le risque lié chez un éditeur, quel qu'il soit, américain, allemand ou chinois. L'exigence fonctionnelle qui permet de traduire cette dimension est donc d'assurer qu'il n'y a pas de *backdoors* dans le produit.

b. Localisation du serveur/hébergement

Dans cette dimension, il y a surtout la question de l'intervention d'un État étranger sur l'exploitant de la plateforme, notamment l'exigence de fournir les données de l'État de Vaud. L'exigence fonctionnelle qui permet de traduire cette dimension est donc d'assurer qu'une divulgation des données de l'État de Vaud par des tiers est impossible.

3. ADÉQUATION DES SOLUTIONS VC

3.1 Evaluation selon les critères définis

La DGNSI a procédé en détail à la comparaison et propose une synthèse de cette analyse des solutions les plus répandues – Cisco Webex, Zoom, Microsoft Teams, Wire et Jitsi – selon les 4 critères définis. Cette analyse se fait sur les bases de données et d'informations disponibles, mises à disposition, voire des retours d'expérience d'entités comparables à l'État de Vaud sur l'une ou l'autre des solutions.

La solution Cisco Webex a été introduite sous les contrats existants avec Cisco, qui étaient soumis à une procédure de marché public.

3.1.1 Fiable

Depuis 1997 sur le marché, Cisco Webex est un produit leader. Il a montré sa haute disponibilité pendant des années et pendant la pandémie (un fait avéré également au sein de l'État de Vaud), avec plus de 600 millions d'utilisatrices et utilisateurs mensuels. L'ACV organise régulièrement des séances Webex avec plusieurs centaines de participantes et participants. Webex garantit des disponibilités contractuelles par SLA (Service Level Agreement) de 99,99 %.

Microsoft Teams (250 millions d'utilisateurs mensuels, SLA 99,9 %) et Zoom (300 millions, pas de SLA) ont connu un développement massif en 2020 et disposent d'une maturité et de fonctionnalités comparables à Webex.

Jitsi (10 millions d'utilisateurs mensuels, pas de SLA¹) ou Wire (pas de chiffres fournis, pas de SLA) ont une maturité nettement inférieure à Cisco Webex. Des limitations techniques sont constatées chez Jitsi dès que le nombre d'utilisateurs dépasse 75 utilisateurs, chez Wire la limite se situe autour de 35.

3.1.2 Conviviale

Webex, Microsoft Teams et Zoom sont considérés comme des produits simples à utiliser. Jitsi est considéré sur le même niveau, car le produit est fortement ciblé sur la convivialité.

Wire a une priorité sur la sécurité de la communication et accepte des réductions de la convivialité en faveur d'une augmentation de la sécurité. Pour les utilisatrices et utilisateurs, ceci se traduit par des étapes plus complexes que dans d'autres outils.

¹ Un SLA de 99 999 % est possible en contractant les services de 8x8 qui utilisent certains services de Jitsi, mais qui n'est plus FOSS.

Pour les utilisatrices et utilisateurs, l'intégration dans leurs applications de base (bureau et téléphone portable) est un facteur essentiel pour la convivialité, notamment en matière d'intégration de calendriers et de carnets d'adresses. Webex dispose d'une bonne intégration dans les produits Microsoft utilisés à l'État de Vaud et permet une intégration profonde avec les systèmes de gestion des identités et de droits d'accès de l'ACV.

Pour Jitsi, une telle intégration est possible, mais à développer, tandis que Wire a intentionnellement limité certaines intégrations pour une sécurité maximale.

3.1.3 Sécurité

Webex, dans la configuration de base, dispose d'une sécurité avancée. Les communications sont cryptées, mais le serveur accède au contenu des communications pour assurer la qualité audio et vidéo. Cette configuration peut échelonner jusqu'à 1 000, dans certaines configurations jusqu'à 3 000, connexions par conférence. Il existe une configuration plus sûre qui implémente le cryptage de bout en bout, qui protège le contenu des communications même dans le cas d'un serveur compromis. Un récent test montre que dans cette configuration, la performance se dégrade à partir de 50 utilisateurs, vu que le serveur ne peut pas amener des améliorations de qualité.

Zoom dispose de la sécurité avancée et, depuis 2021, d'une configuration avec cryptage de bout en bout, cependant limitée à quelques types d'appareils terminaux. Depuis 2017, Zoom promettait du cryptage de bout en bout, mais l'implémentation n'a pas été conforme avec les standards. D'après un accord entre Zoom et la *Federal Trade Commission* (FTC) américaine (commission fédérale du commerce), Zoom restait en possession des clés cryptographiques. Un audit en 2020 a également révélé que, contrairement à la documentation, AES-128 était implémenté au lieu de AES-256. L'implémentation 2021 serait conforme, mais ne peut pas être vérifiée pour l'instant.

Microsoft Teams dispose de la sécurité avancée. Une option avec cryptage de bout en bout a été annoncée, mais seulement pour les appels (donc limitée à deux utilisateurs).

Wire dispose exclusivement du cryptage de bout en bout. En plus de Cisco, les clés cryptographiques sont individualisées, ce qui donne un avantage théorique en cas d'attaques par des utilisateurs exclus de la même conférence. Un récent test montre que la performance se dégrade à partir de 35 utilisateurs.

La cryptographie de Jitsi ne peut pas être validée, car la documentation est actuellement insuffisante. Il n'y a qu'un document simplifié qui affirme que Jitsi dispose de cryptage de bout en bout, mais l'explication fournie ne décrit que des fonctionnalités de sécurité avancée.

Comme la récente attaque « Pegasus » l'a rappelé, toute mesure de sécurité de la plateforme centrale ou de cryptage bout en bout ne protégera pas contre des appareils terminaux compromis par un logiciel malicieux. Ceci concerne tous les produits de façon identique.

3.1.4 Localisation – localisation du service produit

L'éditeur de Webex est Cisco, une entreprise américaine, représentée en Suisse par Cisco Systems (Switzerland) GmbH avec un office à Rolle. L'implantation de Cisco dans le Canton de Vaud a représenté un succès majeur pour la promotion économique cantonale et sa collaboration dans le numérique avec l'EPFL. Le code source de Webex est fermé, mais Cisco permet, sous certaines conditions, de procéder à des audits du code source. L'ACV a reçu l'autorisation de faire un tel audit.

Zoom et Microsoft sont des entreprises américaines. Microsoft est représenté en Suisse par Microsoft Schweiz GmbH, à Wallisellen (ZH). Le code source de produits Microsoft peut être analysé par des organismes gouvernementaux par le Government Security Program, mais sous des contraintes lourdes.

Zoom permet des audits par des tiers sous certaines conditions. Un tel audit a révélé en 2020 que le cryptage de bout en bout n'était pas fiable et que les serveurs étaient configurés avec un algorithme de cryptage plus faible que publié.

Wire et Jitsi sont des produits FOSS, il n'y a donc pas d'éditeur centralisé, mais une communauté éditrice. Cependant, dans les deux cas, une entreprise joue un rôle fort dans l'écosystème. Les employés de ces entreprises émettent la majorité des changements dans le code source, d'après le portail Github, où le code est géré. Jitsi, 8x8 est une entreprise américaine et Wire est soutenu par Wire Swiss GmbH, qui appartient à une firme allemande. Le code source des produits peut être inspecté sur GitHub, cependant un audit public n'a jamais été effectué. Le code source de Wire est nettement plus compact et plus facile à inspecter, celui de Jitsi demanderait un effort massif.

Dans tous les produits, le code source peut donc être soumis à un audit, mais le risque de *backdoors* ne peut pas être exclu complètement au vu de la complexité et de l'ampleur du code.

Les solutions Cloud de Webex, Zoom, Wire et Jitsi sont actuellement hébergées en Europe, dans un pays avec une législation équivalente à la LPD. Microsoft Teams est hébergé en Suisse.

Webex, Zoom, Wire et Jitsi peuvent également être déployés sur site. Ce scénario entraîne des coûts additionnels et des contraintes, telles que des fonctionnalités plus limitées. Microsoft Teams n'est pas proposé en variante sur site.

3.2 Situation en Suisse et à l'international

Cisco Webex est utilisé par un grand nombre d'organisations gouvernementales et étatiques, y inclus l'Administration des Pays-Bas, la Banque Centrale européenne ainsi que des administrations américaines. Dans le cadre de la pandémie du COVID-19, la Confédération a mis un service Webex à disposition de certains employés. Certains Cantons utilisent Webex depuis des années, notamment en Suisse romande.

Microsoft Teams est utilisé comme solution principale par des administrations publiques au Royaume-Uni, en Nouvelle-Zélande, en Pologne et à Hong Kong. Des milliers d'organisations du secteur public l'utilisent comme application complémentaire.

Dans sa note du 28 avril 2020, la Conférence suisse sur l'informatique (CSI) préconise, pour l'ensemble de ses partenaires, l'utilisation des solutions Cisco Webex et Microsoft Teams. Sur la base de cette recommandation, les deux clients seront mis à disposition des collaboratrices et collaborateurs de l'ACV afin qu'ils puissent participer à des séances intercantionales, avec la Confédération et avec les communes.

Zoom est utilisé par des administrations publiques américaines, auxquelles Zoom propose une version spéciale ZoomGov avec toutes les données aux États-Unis. Au début de la pandémie, l'utilisation de Zoom par des organisations gouvernementales – notamment dans l'éducation – a fortement augmenté. La DGNSI n'a pas actuellement connaissance d'organisations gouvernementales européennes qui utilisent Zoom comme solution principale.

Wire est utilisé par certains offices du Gouvernement fédéral allemand, notamment la Chancellerie fédérale allemande et l'Office pour la Sécurité de l'Information (BSI) – éditeur d'un standard reconnu en sécurité des visioconférences (*Kompendium Videokonferenzsysteme*) – ainsi que le ministère de l'Intérieur. Cependant, dans tous ces cas, il s'agit d'une utilisation complémentaire au système de communication principal.

Jitsi est fortement utilisé dans les écoles et universités, mais la DGNSI n'a pas connaissance de références gouvernementales ou étatiques. L'Office pour la Sécurité de l'Information allemande (BSI) a émis un guide spécifique pour la sécurisation de Jitsi dans le contexte écolier.

3.3 Règlementation légale sur les solutions VC

La Suisse n'a pas de réglementation spécifique pour les vidéoconférences, mais c'est la loi fédérale sur la surveillance de la correspondance par poste et télécommunication (LSCPT) qui s'applique, notamment sur le secret des communications à distance. En cas de transmission de données sensibles personnelles, la loi sur la protection fédérale (LPD) ou cantonale (LPrD) des données s'applique. Dans ce contexte, le principe d'équivalence du niveau de protection des données est le facteur essentiel qui détermine si des données peuvent être hébergées dans le Cloud.

Comme mentionné plus haut, les plateformes de Webex, Zoom, Wire et Jitsi se trouvent en Europe (dans la plupart des cas, en Allemagne), et Microsoft Teams peut être hébergé, au choix, en Suisse ou en Europe. Pour la LPD et la LPrD, toutes ces options sont conformes.

Une question fréquemment soulevée est celle du Cloud Act américain, respectivement du Foreign Intelligence Surveillance Act. Notons que la loi fédérale sur la surveillance de la correspondance par poste et télécommunication confère beaucoup plus de droits aux autorités suisses que le CLOUD Act et FISA n'en donnent aux autorités américaines, et qu'une obtention des données hébergées en Suisse par les autorités américaines se ferait plus facilement par la voie de l'Art. 18 para. 1 de la Cybercrime Convention. Sous cette convention, les autorités vaudoises sont même tenues de fournir des données hébergées dans leurs propres bâtiments dans le cadre d'une procédure officielle. Finalement, rappelons les restrictions imposées par la législation sur les marchés publics. En effet, l'ACV ne peut exiger un produit spécifique dans le cadre d'un marché ouvert à la concurrence internationale. Une telle procédure ne pourra pas non plus imposer un choix de fournisseur ou fermer le marché aux entreprises hébergées hors de Suisse en exigeant un produit local en raison du principe de l'interdiction des discriminations. Les équivalences garanties par des protections légales doivent être respectées, par exemple en matière de protection des données. Dans le contexte de la législation sur les marchés publics, il est possible de formuler des exigences fonctionnelles qui excluent certaines firmes.

3.4 Étude d'alternatives à la solution en place

L'ACV dispose déjà d'une solution hébergée dans ses propres locaux. Le central téléphonique de l'ACV est une solution Cisco UCM (utilisé par la police pour la centrale d'appels d'urgence) qui, grâce au logiciel Jabber, permet aussi aux utilisatrices et utilisateurs de tenir des conférences audio et vidéo sur l'infrastructure de l'ACV. Webex est intégré à cette solution et est utilisé sur des machines qui n'appartiennent pas à l'ACV. Stratégiquement, comme tous les fournisseurs, Cisco pousse la solution VC vers le Cloud, de même que la plateforme Webex. Actuellement, Cisco Webex a été mis en place avec toutes les intégrations nécessaires pour une solution conviviale. La DGNSI dispose des compétences nécessaires pour exploiter les produits Cisco et intégrer de nouveaux composants dans le futur. Il y a de fortes synergies entre les différents produits Cisco.

Microsoft Teams peut être mis en place avec le même degré d'intégration que Cisco Webex. La DGNSI dispose des compétences nécessaires pour exploiter les produits Microsoft et intégrer de nouveaux composants dans le futur. Il y a de fortes synergies entre les différents produits Microsoft.

L'ACV ne dispose actuellement pas de compétences sur Zoom, Wire et Jitsi, notamment en matière d'intégration. Des recrutements ou de l'expertise externe sont donc inévitables, et il n'y a pas de synergies avec d'autres produits dans le portefeuille de l'ACV.

Il est fort probable que le niveau d'intégration de Cisco Webex peut être atteint pour Jitsi et Zoom, mais avec un investissement conséquent : il s'agit d'une estimation entre CHF 100 KF et CHF 300 KF en fonction des travaux d'intégration qui seront nécessaires et 2 ETP de ressources pérennes. Dans le cas de Wire, certaines intégrations ne seront pas possibles au vu des restrictions de sécurité imposées.

Toutefois, une procédure de marché public est à prévoir impérativement dans tous les cas de figure. Il est donc probable qu'une bascule vers un autre produit nécessitera au moins deux ans.

3.5 Analyse financière

Avec Cisco et Microsoft, l'ACV a des contrats d'entreprise en place qui couvrent un vaste inventaire de produits. Le contrat Cisco contient des licences Webex (cependant, la licence Microsoft actuelle de l'ACV ne contient pas Microsoft Teams). Ce contrat a été utilisé pour la mise en place de Webex avec la rapidité exigée dans la situation pandémique tout en restant conforme au cadre légal des marchés publics. L'analyse avait été initiée avant la pandémie dans le cadre de la stratégie d'évolution de l'environnement de travail numérique.

La mise en place rapide a été facilitée par le savoir-faire Cisco existant à l'interne et les intégrations déjà en place avec les infrastructures de l'ACV. Pour tous les autres produits, une montée en compétences et un effort massif d'intégration (poste de travail, calendriers, répertoires, téléphonie) seraient nécessaires.

Une discussion approfondie des coûts se ferait dans le contexte d'une procédure de marché public, avec les limitations d'une telle procédure. Même une comparaison des prix de liste est peu indicative à cause du large choix d'options possibles.

Pour les solutions FOSS, il n'y a pas de coûts de licence. Toutes les autres dimensions de coûts, comme le support, l'effort en personnel interne et la connectivité, s'appliquent de la même façon que pour les solutions commerciales. En plus, il est fortement conseillé dans les projets FOSS d'être présent avec ses propres développeurs dans la communauté éditrice pour bénéficier du meilleur niveau de support. Cette expertise peut être acquise à l'externe. Avec la taille et la complexité de l'ACV, il est peu réaliste qu'une solution FOSS puisse être introduite sans ressources supplémentaires, sans présumer de toutes les questions d'interopérabilité entre les différents systèmes existants (téléphonie, réseau, etc.) et de la procédure de marché public à envisager.

4. RÉPONSE AU POSTULAT

Poussé par la pandémie du COVID-19 et les mesures sanitaires mises en place en mars 2020, en particulier le télétravail, l'intérêt pour des solutions de vidéoconférence a fortement augmenté, et les éditeurs ont rapidement étendu leur couverture en fonctionnalités. Le Conseil d'État a su très rapidement développer une stratégie qui assure l'importance de la communication riche à distance et, même aujourd'hui au-delà du contexte pandémique, avec une volonté de moderniser les conditions de travail du personnel de l'ACV, en particulier en autorisant une augmentation de la part du télétravail.

Le rapport présente différentes solutions de vidéoconférences libres et commerciales avec des analyses en relation avec les quatre exigences selon les critères du postulat : fiabilité, convivialité, sécurité et ancrage local. Trois de ces exigences ont été analysées selon les standards du domaine, la norme ISO 25010, la quatrième a nécessité une interprétation pour respecter la législation applicable en matière de marchés publics.

Deux produits libres majeurs (FOSS) font partie des solutions analysées : Wire, qui obtient le meilleur niveau en sécurité, au prix d'une convivialité réduite, et Jitsi, qui reçoit des appréciations inférieures en sécurité à cause de l'impossibilité de vérifier l'implémentation technique de la cryptographie, mais qui dispose d'une convivialité plus haute. Les deux produits peuvent être installés sur des serveurs en Suisse ou sur un Cloud en Europe, répondant partiellement au critère de l'ancrage local. Des solutions suisses existent, dont celle d'Infomaniak Meet qui se base sur le logiciel OpenSource Jitsi Meet. Ces solutions ne permettent cependant pas à ce jour une intégration avec les éléments internes de l'ACV, tels que les carnets d'adresses, la messagerie, les agendas, le système de téléphonie, les systèmes de gestion documentaire et le système d'archivage probatoire. Il existe une forte communauté de développeurs derrière les deux produits, mais, dans les deux cas, la majorité des contributions au code source proviennent des employés d'une seule firme : dans le cas de Jitsi, il s'agit d'une firme américaine ; pour Wire une firme suisse et allemande. Pour le Conseil d'État, les deux produits, même représentés par des intégrateurs suisses, ne satisfont pas toutes les exigences. Au demeurant, une discrimination explicite et absolue des entreprises extraromanandes serait incompatible avec les dispositions légales régissant les marchés publics.

A la suite de cette analyse, le Conseil d'État constate que la solution Webex, produit de l'entreprise Cisco, actuellement utilisée par l'ACV est évaluée de manière très satisfaisante en termes de fiabilité, de convivialité et de sécurité. Bien que Cisco soit une entreprise américaine, le Conseil d'État note toutefois qu'elle est implantée localement avec une succursale sur sol vaudois (Rolle), où elle emploie une centaine de personnes. Cisco Webex étant un produit Cloud, la localisation des serveurs est également un facteur important. Dans le cas d'espèce, ils sont situés en Europe, dans un pays (Allemagne) considéré comme garantissant un niveau de protection des données équivalent à la LPD et LPrD. Avec cette solution, les communications et les informations sont chiffrées de bout en bout. Les experts de la DGNSI ont à leur disposition tous les éléments nécessaires qui leur permettent d'intervenir en cas d'incident majeur à résoudre pour l'État de Vaud. Sur ce point, le Comité d'experts du numérique (CEDN) regroupant des représentants de plusieurs départements de l'ACV a procédé à une analyse également en lien avec le secret de fonction. Dans sa conclusion, il est unanime quant à l'importance de mettre à disposition un environnement de travail numérique moderne et des outils collaboratifs permettant de nouveaux modes de travail et d'organisation à l'ACV. Ainsi les écueils potentiels en matière de protection des données de la solution Webex, mise en place de manière plus rapide que prévue, sont identifiés et des solutions contractuelles et techniques (serveurs rapatriés en Europe) permettent de les prévenir. De plus, ils sont à mettre au regard d'une part de l'importance stratégique d'une politique RH moderne, et d'autre part des risques qu'entraînerait la prolifération d'outils plus problématiques.

L'introduction très rapide, en mars 2020, de la solution Webex a permis à l'Administration cantonale de continuer son travail malgré les restrictions liées à la situation sanitaire. La DGNSI a constaté un bon niveau de satisfaction des collaboratrices et collaborateurs de l'ACV quant à l'utilisation de cette solution.

A ce jour, Cisco Webex reste la solution privilégiée, car elle s'intègre parfaitement à la plateforme de téléphonie du même fournisseur déployée à l'ACV. Le Conseil d'État rappelle qu'elle est l'une des solutions recommandées par la Conférence suisse sur l'informatique (CSI). Sur la base de cette recommandation, la DGNSI a mis à disposition des collaboratrices et collaborateurs de l'ACV l'autre solution recommandée (Microsoft Teams) afin qu'ils puissent participer à des séances avec d'autres acteurs institutionnels (communes, cantons, Confédération).

Par ailleurs, le Conseil d'État note qu'un changement de la solution Webex vers un autre produit commercial ne présente aucun avantage sous l'angle du postulat et devrait se faire dans le cadre d'une procédure de marché public, qui ne permet pas d'exiger un produit ou un vendeur spécifique.

En résumé, le Conseil d'État considère que la solution actuelle répond aux exigences formulées dans le postulat et qu'elle a fait ses preuves auprès des collaborateurs et collaboratrices de l'ACV. Il n'estime pas nécessaire aujourd'hui de changer sa stratégie en matière de vidéoconférence ni de changer de solution. Toutefois, il a chargé la DGNSI d'observer continuellement le marché et, en fonction des évolutions technologiques, d'évaluer son portefeuille de solutions du domaine.

Ainsi adopté, en séance du Conseil d'Etat, à Lausanne, le 1^{er} juin 2022.

La présidente :

N. Gorrite

Le chancelier :

A. Buffat

5. GLOSSAIRE

Abréviation/Terme	Description
ACV	Administration cantonale vaudoise
AD	<i>Active Directory</i>
AES	<i>Advanced Encryption Standard</i> (AES-128, AES-256)
API	<i>Application Programming Interface</i> – Une interface qui permet à des solutions de communiquer entre elles
Appel	Transmission vidéo et audio entre deux participants
Backdoor	En français porte dérobée, une backdoor est une caractéristique ou un défaut d'un système informatique qui permet un accès subreptice et non autorisé aux données.
BSI	<i>Bundesamt für Sicherheit in der Informationstechnik</i> - l'Office pour la Sécurité de l'Information allemand
CA	Canada
CCPA	<i>California Consumer Privacy Act</i> . Pour plus d'informations, se référer à https://oag.ca.gov/privacy/ccpa
Cloud	Ensemble de serveurs accessibles via Internet, y compris les logiciels et bases de données qui fonctionnent sur ces serveurs
Cloud Act	<i>Clarifying Lawful Overseas Use of Data (Cloud) Act</i> : se référer à https://www.justice.gov/dag/cloudact pour plus d'informations
Commercial Off the Shelf (COTS)	Produit commercial ne comprenant pas d'adaptation spécifique au client
Conférence	Transmission vidéo et audio entre trois ou plus participants
COTS	Commercial Off the Shelf
CN	Chine
DE	Allemagne
DGNSI	Direction générale du numérique et des systèmes d'information
Editeur	Un éditeur élabore l'écosystème composé de l'application, du serveur et des appareils terminaux. Il écrit le code source.
end2end (E2E)	De bout en bout – se réfère à une implémentation de cryptographie, où la technologie assure qu'aucun intermédiaire n'a accès aux communications
Foreign Intelligence Surveillance Act (FISA)	Se référer à https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286 pour plus d'informations
Free and Open Source Software (FOSS)	Logiciels libres où il n'y a pas d'éditeur central, un collectif (une communauté de développeurs) édite le logiciel
FTC	<i>Federal Trade Commission</i> (US), en français la commission fédérale du commerce
GATT	<i>General Agreement on Tariffs and Trade</i> , en français « Accord général sur les tarifs douaniers et le commerce (GATT) » (https://www.fedlex.admin.ch/eli/cc/1959/1745_1807_1812/fr)
GPL	<i>General Public License</i> – licence Free and Open Source très répandue
Intégrateur	Un intégrateur est une entreprise qui ne dispose pas elle-même d'un produit, mais qui a la capacité d'intégrer des solutions existantes et de les adapter. Il assemble des solutions ou complète une solution existante pour fournir un produit fonctionnel dans un nouveau contexte global.
ISO 25010	Standard de qualité de logiciel
LMP	Loi fédérale sur les marchés publics (https://www.fedlex.admin.ch/eli/cc/2020/126/fr)
LMP-VD	Loi sur les marchés publics (https://prestations.vd.ch/pub/blv-publication/actes/consolide/726.01?key=1544080192149&id=38a6a8fa-d455-4218-8cd3-32510a097fb5)
LPD	Loi fédérale sur la protection des données (https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/fr)
LPrD	Loi sur la protection des données personnelles du canton de Vaud (https://prestations.vd.ch/pub/blv-publication/actes/consolide/172.65?key=1543934892528&id=cf9df545-13f7-4106-a95b-9b3ab8fa8b01)
Managed Service	Services comprenant la maintenance et les mises à jour, qui sont gérées et exploitées à distance par un opérateur.

Abréviation/Terme	Description
Modèle <i>zero-knowledge</i>	Modèle où aucune donnée n'est divulguée à la plateforme Cloud
RGPD	Règlement général sur la protection des données (européen). Plus d'informations sous https://www.edoeb.admin.ch/edoeb/fr/home/documentation/datenschutz/Datenschutz%20-%20International/DSGVO.html
SAML	<i>Security Assertion Markup Language</i>
Single Sign-On	Méthode d'authentification qui permet à un utilisateur de s'authentifier dans différents systèmes à l'aide d'un identifiant et d'un mot de passe unique
SLA	<i>Service level agreement</i> , accord de niveau de service est un contrat où la partie d'un contrat par lequel un prestataire informatique s'engage à fournir un ensemble de services à un ou plusieurs clients et leur garantit certains niveaux de service
Solutions VC	Solutions de vidéoconférence
US	États-Unis
VC	Vidéoconférence