CYBER | MANUEL D'INTEGRATION D'UNE PRESTATION AU PORTAIL SECURISE DES PRESTATIONS EN LIGNE

HISTORIQUE DE REVISION	Version	Date	Qui	Description
	1.0	17.10.2017		Initialisation
	1.1	11.02.2019	PCA	Ajout d'information sur Cyread
	1.2	19.02.2019	RGL	Changement du nom de SDK Cyber vers PrestaKit. Actualisation des services transversaux, gestionnaires de demandes et information utilisateur.
	1.3	20.02.2019	SBA	Changement du processus projet et mises à jour des screenshots

TABLE DES MATIERES

1 INTRODUCTION

Ce document est à destination :

- des services métier
- des équipes de pôles métier de la DSI
- des personnes intervenant dans les projets du programme de cyberadministration.

Il décrit et spécifie les besoins métier liés à la dématérialisation de prestations. Il reprend les terminologies relatives aux normes en cyberadministration eCH.

1.1 ABRÉVIATIONS, GLOSSAIRE, DÉFINITIONS

Annonce de mise en ligne de prestation	Annonce d'un projet de réalisation et déploiement d'une prestation sous sa forme électronique.
BIC	Bureau d'information et de communication
COPIL	Comité de pilotage
ROP	Répondant en optimisation des processus
UCA	Unité de conseil et d'appui
DSI	Direction des systèmes d'information
eCH	Standards et normes de cyberadministration Suisse
EMPD	Exposé des motifs et projet de décret
EMS	Elaborer et Maintenir les solutions
IDM	Identity Manager
RSI	Responsable de système d'information
Mise en ligne d'une prestation	Réalisation et déploiement de la prestation sous sa forme électronique.
Prestation en ligne	Prestation partiellement ou totalement dématérialisée.
PSPL	Portail sécurisé des prestations en-ligne

2 DEFINITIONS

2.1 PRESTATION

Comme il est décrit dans la norme eCH0073, le terme prestation désigne le résultat (produit) d'un processus. Une prestation est délivrée par un service prestataire pour accomplir les besoins des usagers (bénéficiaires de prestation).

2.1.1 PRESTATIONS PUBLIQUES

Les prestations que délivrent les unités administratives dans le cadre de leurs missions prescrites par la loi sont décrites comme étant des prestations publiques. Les prestations publiques concernent en particulier : les prestations d'information, les décisions administratives et les prestations en lien avec la tenue des registres officiels.

Exemples de prestations :

- Autorisation de vente à l'emporter de boissons alcooliques
- Autorisation d'exercer la profession de médecin à titre indépendant
- Inscription au chômage
- Inscription à l'examen de chasseur
- Autorisation d'exercer la profession de pêcheur professionnel
- Déclaration d'assujettissement à la TVA
- Déclaration d'impôt

2.1.2 PRESTATIONS RELATIVES AUX TACHES DE DIRECTION ET DE SOUTIEN

Les prestations relatives aux tâches de direction et de pilotage consistent en la coordination, la planification et la description stratégique des activités principales d'une unité administrative.

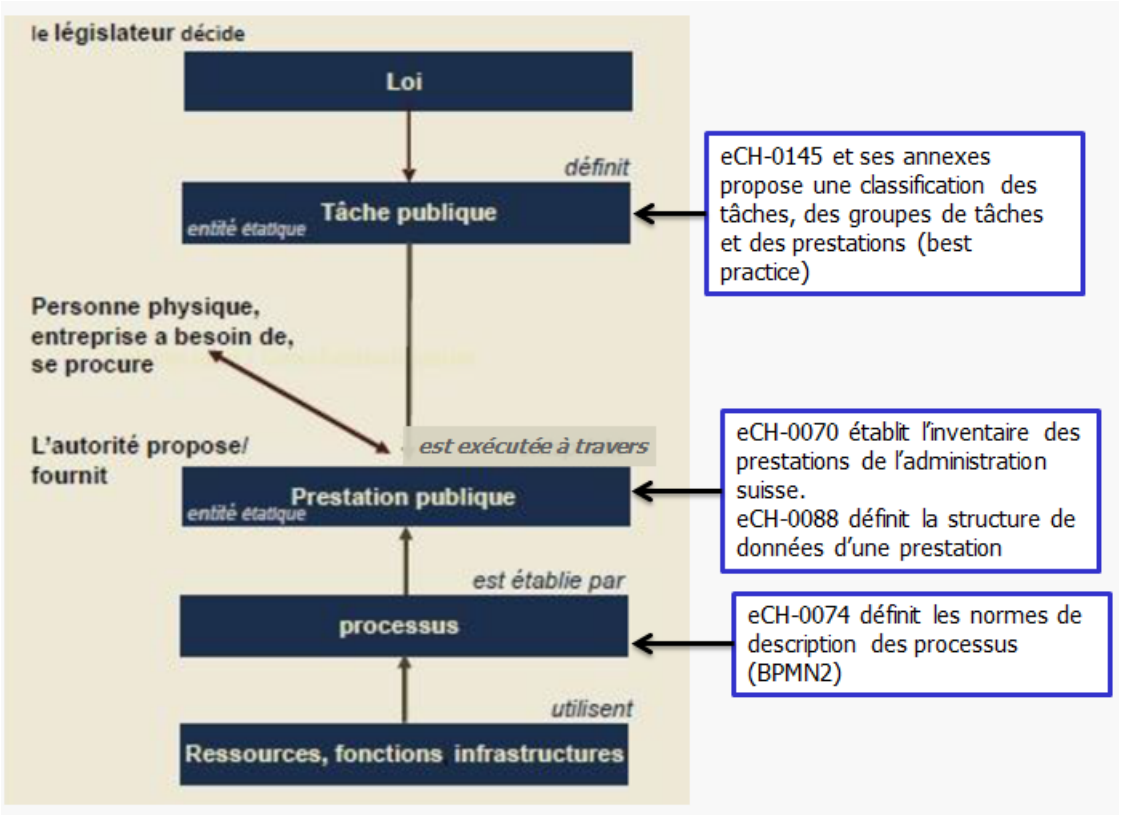
Les prestations relatives aux tâches de soutien décrivent les ressources telles que les personnes, les moyens matériels et les moyens budgétaires nécessaires à l'accomplissent des activités principales.

2.1.3 PRESTATIONS EN LIGNE

Il s'agit des prestations métier ou relatives aux tâches de direction et de soutien totalement ou partiellement dématérialisées.

Ces prestations sont délivrées aux usagers (Particuliers, Entreprises, Communes) sous leur format électronique et mises à disposition via des guichets ou des portails électroniques.

2.1.4 NOTIONS FONDAMENTALES RELATIVES A LA DELIVRANCE DE PRESTATION



3 CATALOGUE DE PRESTATIONS

3.1 CONTEXTE ET OBJECTIF

L'EMPD cyberadministration prévoit de mettre en ligne une douzaine de prestations en moyenne chaque année. Il prévoit aussi le financement de la mise œuvre du projet « Déployer et gérer le catalogue de prestations ». Ce projet permet de faciliter et de supporter la gestion des prestations.

Ainsi, le projet vise à combler les besoins :

- d'annoncer qu'un projet de dématérialisation de prestation est pris en charge par la plateforme eVD (en l'état seule cette phase est opérationnelle). Il s'agit donc de faire évoluer la plateforme d'annonce en ajoutant des fonctionnalités de gestion et d'exploitation d'un catalogue de prestations mises à dispositions par l'Etat. Ces fonctionnalités permettront de faciliter le suivi des travaux de dématérialisation des prestations.
- de se conformer aux règles relatives à la description des prestations décrites dans les normes et standards eCH.

Le catalogue de prestations constitue le référentiel des prestations internes du système d'information de cyberadministration de l'Etat de Vaud.

Il a pour objectifs principaux de :

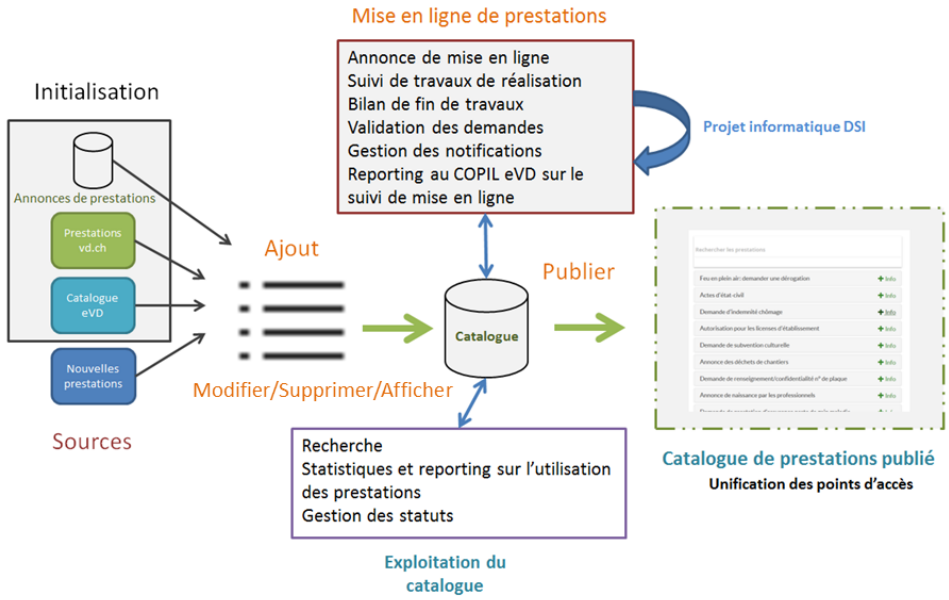
- identifier, pour les services métier de l'ACV, les prestations délivrées aux usagers
- publier les prestations dans le catalogue

3.2 ACCÈS ET PUBLIC CIBLE

Le catalogue de prestations est accessible depuis le portail IAM intranet. Les parties prenantes sont les suivantes :

- Les Répondants à l'Optimisation des Processus (ROP) des services métier pour l'identification et l'ajout des prestations
- Systèmes abonnés à la notification de publication de prestation
- Gestionnaire du catalogue : utilisateur d'administration du catalogue
- Les responsables de systèmes d'informations (RSI) : pour la saisies des informations de mise en ligne

3.3 FONCTIONNALITES



3.3.1 AJOUTER UNE PRESTATION

L'ajout d'une prestation est une fonctionnalité permettant aux utilisateurs (principalement les ROPs) d'identifier et de décrire les prestations que leur service délivre aux usagers. L'ajout d'une prestation est la fonctionnalité principale du catalogue de prestations.

L'ajout d'une prestation s'articule particulièrement sur le remplissage d'un formulaire depuis l'application « Catalogue de prestations ».

3.3.2 PUBLIER UNE PRESTATION

L'objectif de la publication de prestation consiste à permettre aux services métier (représentés par le ROP ou le contributeur) de mettre à disposition les informations descriptives d'une prestation aux usagers. Les prestations sont publiées et mises à disposition via des API.

La prestation avec une modalité d'accès en ligne est publiée dans le gestionnaire de demande. Ce qui permet d'utiliser les informations telles que :

- le titre des étapes
- le niveau de sécurité
- les liens d'accès
- la durée de conservations des données

4 UNIFICATION DES POINTS D'ACCES

4.1 CONTEXTE

L'unification des points d'accès consiste à :

- offrir aux usagers une expérience utilisateur conforme et uniforme
- permettre une navigation simple et unique entre l'espace public et les espaces sécurisés (Particuliers, Professionnels)
- mettre en conformité les échanges des demandes des usagers au sein du système d'information de cyberadministration
- appliquer les normes et standards de cyberadministration

4.2 UN SITE VD.CH ORIENTE PRESTATIONS

Selon l'analyse statistique de l'utilisation du site officiel de l'Etat de Vaud, 75% des usagers consultent le site pour obtenir une et une seule prestation.

De ce fait, le site met en avant et facilite l'accès aux prestations délivrées par l'Etat. Les prestations sont accessible depuis les pages thématiques, les pages d'autorités ainsi que dans l'espace sécurisé.

Page thématique : Poursuites et faillites

Listes des prestations dans l'espace sécurisé

5 PROCESSUS DE PROJET DE MISE EN LIGNE D'UNE PRESTATION

Le processus standard de projet informatique DSI doit être utilisé pour la réalisation d'une prestation. Le projet doit être initialisé dans le programme de gestion de projet à la DSI et un mandat de projet doit être rédigé pour commencer le projet.

6 ARCHITECTURE, NORMES ET STANDARDS

6.1 DESCRIPTION DE L'ARCHITECTURE DU PSPL

L'architecture du Portail sécurisé de prestations en ligne (PSPL) est le résultat d'un compromis entre les exigences de la stratégie e-VD et la nécessité de maintenir une flexibilité pour les services métiers dans l'implémentation de leurs prestations. Les deux projets phares qui apportent des exigences en termes de normalisation des prestations sont les suivants :

- **L'unification des points d'accès.** (chapitre 4) Offre au citoyen une interface unique pour interagir avec l'Etat de Vaud et accéder à l'ensemble de ses prestations (PSPL).
- **Le catalogue des prestations.** (chapitre 3) Ce projet exprime le besoin de normaliser toutes les prestations fournis par l'Etat aux citoyens, avec des attributs et des données cohérentes avec les normes fédérales.

Pour maintenir une flexibilité des services métiers dans l'implémentation de leurs prestations, le PSPL introduit le concept de « Prestation Cyber » qui représente la prestation devant le guichet, par opposition à la prestation derrière le guichet, normalement implémentée par des systèmes applicatifs métier pour le traitement de demandes ou le stockage de données métier.

Cette séparation entre la « Prestation Cyber », partie « front-office » devant le guichet, et la partie « back-office » derrière le guichet, permet de standardiser les interactions avec les usagers du portail, en introduisant des normes graphiques et d'UX tout en laissant la flexibilité des services métier pour implémenter les processus dans leurs applications métier.

L'autre avantage de cette séparation entre la « Prestation Cyber » et les applications métier est de permettre aux services métier de réutiliser les services applicatifs transversaux sans à avoir à les redévelopper eux-mêmes, comme par exemple les services d'autorisation et authentification, les services de gestion de demande, de notifications de documents, etc.

La flexibilité pour les services métier est aussi garantie par le déploiement indépendant de la « Prestation Cyber ». Ce composant est une application web sous la maîtrise du service métier ; il peut donc être déployé de manière autonome et suivre l'évolution fonctionnelle de la prestation.

Nous présentons ci-dessous un schéma de la solution Portail de l'Etat de Vaud. Les composants en rose sont des services transversaux offerts par le PSPL que les prestations peuvent réutiliser. Les composants en orange sont des services applicatifs que les services métiers doivent fournir ou implémenter.

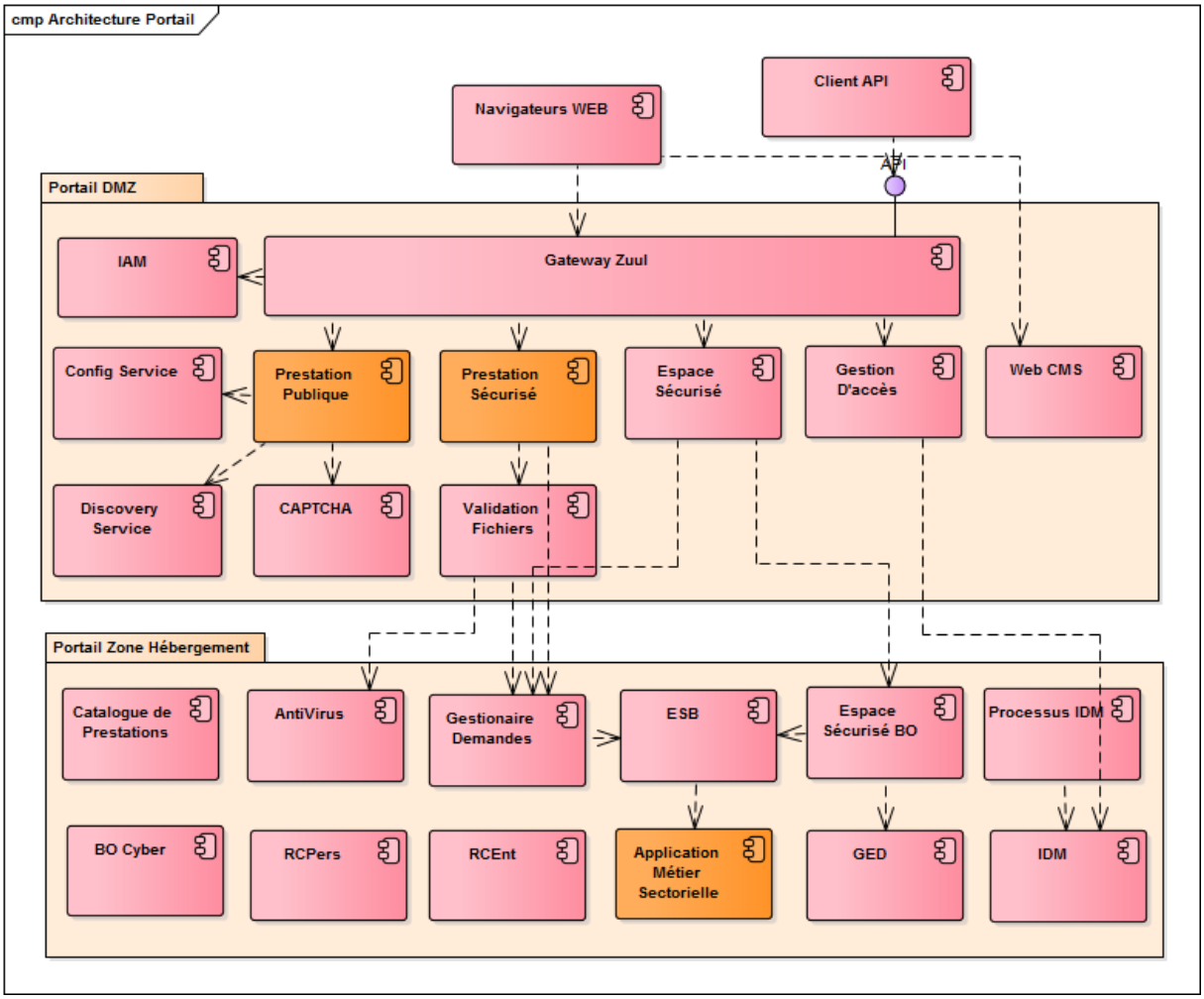


Figure 1 Architecture Logique PSPL

6.2 DESCRIPTION PRESTATION CYBER

La prestation Cyber implémente la partie devant le guichet pour l'usager du PSPL. Comme décrit dans le chapitre antérieur, les objectifs de ce composant sont les suivants:

- Unifier les points d'accès et offrir à l'usager une expérience cohérente dans ses interactions avec les prestations.
- Normaliser les attributs des prestations dans le catalogue (accès sécurisé, url, topologie, etc.).
- Flexibiliser les déploiements du composant « front-office » pour respecter les contraintes du service métier en termes de cycle budgétaire, juridique, calendrier, etc.
- Réutilisation des services transversaux du PSPL, pour rationaliser les développements et normaliser les procédures et méthodes (création de compte, gestion d'accès, gestion demandes, etc.).
- Découpler l'évolution des applications métier de la partie « front-office », pour garantir les attributs non-fonctionnels de performance, disponibilité, évolutivité, « scalabilité », sécurité des données, etc.

Ce composant « front-office » est une application web indépendante (Java, Angular, HTML). La construction de

ce composant est de la responsabilité du projet.

Pour faciliter la construction de ce composant, un SDK (*Software Development Kit*) avec le nom PrestaKit, est fourni à l'équipe projet qui contient une collection d'éléments graphiques et d'appels API vers les services transversaux du PSPL. (Chapitre **Erreur ! Source du renvoi introuvable.**). Le projet doit utiliser PrestaKit pour construire la partie « front-office » de la prestation Cyber.

Le rôle applicatif de ce composant est de faire l'interaction avec l'usager dans le cadre de la prestation en exposant des formulaires ou des informations pertinentes. Ce composant n'a pas l'objectif de faire du traitement métier, mais seulement de la validation de données. La fonction de traitement de données de la prestation est réservée aux applications back-office. Ce composant n'a pas de base de données associée.

6.2.1 PERIMETRE FONCTIONNEL

Il est possible d'avoir plusieurs prestations (ex : plusieurs formulaires) dans le même composant, tant qu'elles respectent toutes le même périmètre fonctionnel.
Exemple : Les prestations des actes de mariage ou de décès peuvent faire partie d'un composant qui agrège tous les actes civils.

Néanmoins, toutes les prestations dématérialisées doivent être individuellement adressables dans le composant « front-office », avec l'attribut « Lien d'accès » (URL) dans le catalogue des prestations. Le périmètre fonctionnel est le même que celui décrit dans MEGA dans le cadre de la cartographie du système d'information métier.

L'objectif est de garantir qu'il est possible de faire évoluer la prestation avec des déploiements indépendants récurrents sans impacter plusieurs services métiers ou parties prenantes a là fois.

Dans le cas limite, il serait possible d'avoir un composant « front-office » par service métier, mais en pratique la granularité est plus fine parce que les prestations n'ont pas toutes les mêmes attributs non-fonctionnels.

6.2.2 ATTRIBUTS NON-FONCTIONNELS

Les attributs non-fonctionnels les plus importants d'une prestation cyber sont les suivants :

- **Performance** : Est-ce que la prestation reçoit quelques requêtes par secondes ou par an ?
- **Sécurité** : Est-ce que la prestation est publique ou sécurisée ?
- **Disponibilité** : Est-ce que la prestation doit être hautement disponible ou non ?

Même si le composant « front-office » peut agréger plusieurs prestations, ce n'est pas une bonne pratique de mélanger dans le même composant des prestations avec des attributs non-fonctionnels très différents.
Exemple : avoir dans le même composant des prestations publiques et des prestations sécurisées, ou des prestations avec des besoins de performance différents.

Le choix de regroupement de prestations dans le même composant « front-office » reste un choix du RSI (Responsable du Système d'information) - qui est le responsable du domaine fonctionnel -, et de l'architecte solution référent du domaine métier.

6.2.3 BACK-OFFICE METIER

Le « back-office » métier est le système d'information qui sert de support aux processus métier de la prestation. Une ou plusieurs applications permettent aux collaborateurs des services métier de recevoir des demandes et de les traiter.
Exemple : Une prestation pour des demandes d'autorisation de construire qui seront traitées dans un outil de case management pour analyse du dossier.

L'architecture de PSPL est basé sur la séparation entre la partie « front-office » et « back-office » de la prestation. Cela implique que la partie « front-office » puisse échanger des données avec le « back-office ».

Le mode asynchrone en utilisant le gestionnaire de demande (chapitre 6.3.4) est le mode privilégié pour cette communication. Dans les cas où l'information doit être traitée immédiatement, le mode synchrone est aussi possible.

Dans le mode asynchrone, la partie « front-office » génère une demande dans le gestionnaire de demandes qui la transmet au système d'information métier à travers le BUS d'entreprise. La demande est un fichier XML avec un format normatif (chapitre 6.4.1) qui permet la récupération de toutes les informations introduites dans le composant « front-office ». Si le « back-office » veut communiquer l'état d'avancement du processus métier qui supporte la prestation, il peut retourner une nouvelle étape de demande vers le gestionnaire de demandes avec le nouvel état d'avancement du processus.

Dans le mode synchrone, seulement les API basées sur des protocoles HTTP sont acceptés. Cela veut dire que les systèmes d'information « back-office » doivent fournir des API pour cette consommation d'information de la partie « front-office ».

6.3 SERVICES TRANSVERSAUX

L'objectif principal du PSPL est d'offrir une plateforme de développement de prestations de cyber administration tout en maintenant la flexibilité des services métiers dans leurs implémentations et en garantissant la cohérence visuelle et d'interaction avec les usagers du Portail.

Un autre objectif majeur est de fournir aux services métier un catalogue de services informatiques pour faciliter le développement des prestations et de rationaliser les efforts de développement en mutualisant des services transversaux.

Un service transversal est un service informatique qui est nécessaire pour offrir la prestation, mais qui n'est pas directement du domaine métier.
Exemple : L'authentification et l'autorisation, un espace sécurisé, gestion demandes unifiée, etc.

6.3.1 AUTHENTICATION ET AUTORISATION

Le service d'autorisation et authentification permet d'avoir un mécanisme unifié pour fournir aux prestations l'identité de l'usager connecté et le contexte de connexion utilisé.

Pour avoir accès au PSPL de façon sécurisée, les usagers doivent créer un compte dans le Portail. Le PSPL offre une prestation pour la création d'un compte. Cette prestation a un processus métier associé, avec une identification forte de l'usager vers une autorité habilitée. Après avoir créé un compte, l'usager reçoit un IUP

(Identifiant Unique Pérenne).

Quand l'usager accède au PSPL de façon sécurisée, il doit remplir son IUP/mot de passe et choisir un contexte de connexion. Le contexte de connexion représente le contexte d'interaction avec le PSPL.
Exemple : Usager en tant que particulier, usager en tant que collaborateur de la commune de Renens, usager en tant que collaborateur de l'entreprise X.

La session de sécurité et les droits obtenus sont toujours associés à un contexte de connexion. Donc, un usager en tant que particulier peut avoir moins de droits que le même usager en tant que collaborateur d'une commune. La session de sécurité est étanche, dans la mesure où l'usager connecté au portail ne peut pas changer de contexte de connexion. Il doit obligatoirement se déconnecter et se reconnecter avec un nouveau contexte.

Pour déclarer une prestation sécurisée, le service métier doit remplir son attribut dans le catalogue des prestations. La prestation sera disponible pour l'usager, avec une session de sécurité valide, et l'information de l'usager connecté sera transmise au composant « front-office » avec toutes les requêtes. L'information de l'usager connecté inclut l'IUP et le contexte de connexion associé.

6.3.2 ESPACE SECURISE

L'espace sécurisé est une prestation fournie par le PSPL qui fonctionne comme un « tableau de bord » pour donner à l'usager un point de contact unifié avec toutes ses interactions avec l'Etat. Cette prestation suit le même modèle des autres prestations, avec un composant « front-office » et un système « back-office » qui permet d'agréger toutes les informations d'un usager.

Les fonctionnalités disponibles dans cette prestation sont les suivantes :

- Une liste de prestations filtrée par type d'usager (Particulier, Entreprise, Commune, Partenaire, etc.)
- Une liste de prestations favorites
- Un suivi de demande de toutes les prestations auxquelles l'usager participe.
- Accès à des dossiers sectoriels (Dossier Fiscal, Dossier médical).
- Notifications associées aux processus administratifs.
- Liste des documents reçus de l'administration.
- Configuration de son espace sécurisé et des préférences. (adresse de contact)

Pour les services métiers qui implémentent leurs prestations, l'avantage est de pouvoir communiquer des informations pertinentes à l'usager sur son tableau de bord, sans à avoir à développer cette fonctionnalité eux-mêmes. Ils peuvent utiliser l'Espace Sécurisé pour communiquer :

- L'État d'avancement d'une demande.
- Notifier l'usager avec des informations pertinentes sur leurs prestations.
- Envoyer des informations sur des documents produits par l'administration à l'usager.

Toutes ces communications sont faites de manière asynchrone avec l'échange de fichiers structurés (XML) dans le BUS d'entreprise, entre le système d'information métier et le système d'information de la cyberadministration.

6.3.2.1 SUIVI DE DEMANDES

Cette fonctionnalité est possible pour l'usager dans l'espace sécurisé où il peut consulter la liste des demandes qu'il a faites à l'administration, avec leur statut d'avancement.

Pour offrir cette fonctionnalité, les prestations doivent interagir avec le gestionnaire de demandes (chapitre 6.3.4) depuis la création de la demande jusqu'à sa clôture, en passant par les différentes étapes de son avancement.

Exemple : Un service métier reçoit dans son système d'information « back-office » une demande de prestation. Cette demande est un fichier structuré, en format XML (chapitre 6.4.1) qui contient toutes les informations capturées dans le composant « front-office ». Si le service métier veut communiquer à l'usager un changement de statut de la demande, son système d'information doit produire un fichier structuré en XML avec le nouveau statut et le communiquer au gestionnaire de demandes à travers le BUS d'entreprise. L'usager aura alors l'information du nouveau statut dans son interface sécurisée de suivi de demandes.

6.3.2.2 SERVICE DE NOTIFICATIONS

Le mécanisme d'échange de fichiers structurés XML à travers le BUS d'entreprise, utilisé pour le suivi de demande, est aussi utilisé pour communiquer des notifications à l'usager dans son espace sécurisé. Ces notifications sont des messages unidirectionnels (sans réponse de la part de l'usager) avec l'objectif d'informer un usager ou un groupe d'usagers sur une information pertinente dans le cadre de leur relation avec l'administration.

Ces notifications doivent être utilisées lorsqu'il y a des informations sensibles qui ne doivent pas être transmises par e-mail. Pour chaque notification, l'usager reçoit un e-mail simple, sans information sensible, avec un lien vers le PSPL. Le suivi du lien oblige l'usager à se connecter au PSPL et à son espace sécurisé pour voir la notification. La lecture du message est associée à une quittance.

6.3.2.3 DISPONIBILISATION DE DOCUMENTS

Si le service métier veut transmettre des documents à l'usager dans le cadre d'une prestation, il peut utiliser un mécanisme d'échange de fichier XML avec toutes les informations du document qui doit être rendu disponible.

Ces informations présentent dans l'échange doivent contenir, entre autre, le titre du document, les attributs pertinents pour le métier (metadata) et le numéro de la demande.

6.3.3 COUPE CIRCUIT

Pour les interactions entre les composants « front-office » et les systèmes d'informations métier, nous privilégions la communication asynchrone à travers le BUS d'entreprise et l'échange de messages structurés. Ce type de communication permet de garantir une traçabilité des opérations et de faire face à des pics de charge sans mettre en cause la disponibilité des systèmes d'information métier.

Dans certains cas, la communication asynchrone n'est pas envisageable. Donc, les appels du composant « front-office » doivent être faits en mode synchrone vers les applications métier. Si le système d'information

métier n'a pas de haute disponibilité, il est possible que les appels échouent.

Dans le cas où les appels doivent être synchrones et les systèmes d'information métier ne sont pas hautement disponibles, nous recommandons l'utilisation d'un coupe circuit. Ce mécanisme n'est pas livré avec PrestaKit mais il est facilement intégrable et il permet de maintenir une interaction avec l'usager, même dans les cas où le système d'information métier n'est plus disponible, avec la configuration d'un « fallback » qui représente l'action à prendre au cas où l'appel synchrone échoue.

6.3.4 GESTION DES DEMANDES

Le gestionnaire de demandes est un service transversal fourni par le PSPL qui permet d'offrir certaines fonctionnalités communes aux prestations.

Quand une prestation métier entre dans le cadre d'un formulaire, qui doit être rempli et envoyé au métier pour traitement, plusieurs fonctions mutualisées sont mises à disposition par le gestionnaire de demandes.

- Génération d'un identifiant d'une demande
- Enregistrement des brouillons temporaires de la demande
- Traçabilité de la demande
- Communication asynchrone avec les systèmes d'information métier

Une prestation cyber qui veut envoyer une demande utilise le gestionnaire de demandes avec des appels synchrone sur une API REST, dont le client est embarqué dans PrestaKit. Le gestionnaire de demandes permettra de créer un identifiant, gérer un brouillon, et envoyer la demande au système d'information métier correspondant.

La génération de bouillons est une fonctionnalité utile pour les formulaires complexes, ou l'usager peut enregistrer son avancement sans envoyer la demande. Cet enregistrement permet de revenir au formulaire, et récupérer les données déjà saisies pour faciliter le remplissage de ses formulaires complexes. Le temps par défaut d'enregistrement de ce bouillon est de 3 jours, sauf si le projet a décidé de prolonger le temps pour des raisons métiers. Dans ce cas, ce paramètre devra être spécifié dans le catalogue des prestations.

Ce genre de fonctionnalité et commun a la plupart des prestations. Ceci permet d'éviter la duplication fonctionnelle dans toutes les prestations de ce type et offre à l'usager une vision unifiée de toutes ses demandes à l'administration.

Cette vision unifiée est aussi possible grâce au mécanisme d'actualisation du statut d'une demande. Quand le service métier veut informer l'usager qu'une demande a changé de statut, son système d'information métier produit un fichier structuré XML (chapitre 6.4.1) avec l'information pertinente, et l'envoie au gestionnaire de demande à travers le BUS d'entreprise. Cette information est communiquée à l'usager dans son espace sécurisé.

6.3.5 E-PAYMENT

Une explication du service de paiement électronique est en cours de rédaction et sera bientôt disponible.

6.3.6 CAPTCHA

Le service de CAPTCHA offre un mécanisme de séparation entre humains et machines pour éviter la soumission d'informations indésirables (SPAM) par des robots.

Ce service est disponible pour toutes les prestations publiques et son utilisation est intégrée dans PrestaKit.

6.3.7 SESSION INFO

Le service de Session Info permet à une prestation d'obtenir une collection d'attributs de l'usager connecté au portail. Ce service est utile pour les prestations sécurisées, mais il peut aussi être utilisé par les prestations publiques dans les cas où cette information est nécessaire pour du pré-remplissage de formulaires.

Ce service peut être appelé par la partie javascript du composant *front-office* mais aussi par la partie java. L'appel doit contenir le cookie de session de l'usager connecté, sinon, la réponse du service est 302 (redirection vers la page de login)

6.3.8 INFORMATION UTILISATEUR

Le service information utilisateur (composant CYREAD) permet à une application métier (back-office) d'obtenir la même collection d'attributs qu'avec session info, pour un contexte donné.

Il permet aussi d'obtenir les informations suivantes :

- IUP correspondant à un numéro AVS.
- NAVS correspondant à un IUP.
- Information sur une étape.
- Liste des courriels de comptes autorisés à accéder à une prestation donnée pour un espace sécurisé.
- Liste des courriels des responsables de prestation pour une prestation et un espace sécurisé.

6.3.9 DEPOT DE DOCUMENT

Le service de dépôt de document permet d'offrir la fonctionnalité de contrôle anti-virus aux prestations qui ont besoin de télécharger des documents dans les formulaires de prestations.

Ce service est intégré dans PrestaKit (Software Development Kit).

6.3.10 SERVICE DE CONFIGURATION

Le service de configuration est un service technique qui permet de fournir une collection de paramètres standards du PSPL. L'utilisation de ce service est transparente si le projet utilise le PrestaKit pour construire le composant « front-office » de la prestation. Ce service permet d'éviter un redéploiement de la prestation dans les cas où certains paramètres du PSPL changent.

Quelques exemples de paramètres présents dans le service de configuration sont :

- Un préfix des url d'accès générique pour toutes les prestations.

- Une URL du CAPTCHA pour l'utilisation des prestations publiques.

6.3.11 SERVICE D'ENREGISTREMENT

Le service d'enregistrement est un service d'infrastructure technique pour les prestations cyber. Sa fonction est d'offrir une vue dynamique sur la disponibilité des prestations. L'utilisation de ce service est transparente avec l'utilisation du PrestaKit qui a déjà toute la configuration nécessaire pour enregistrer les prestations.

Comme les prestations cyber FO sont des applications web indépendantes, elles peuvent être déployées sur des machines différentes dans le réseau. Elles peuvent aussi ne pas être disponibles en raison d'une erreur ou d'une maintenance d'exploitation.

Au lieu d'avoir une configuration statique de l'adresse IP de la prestation, ce service permet qu'au démarrage la prestation s'annonce avec son adresse de façon dynamique.

Quand une requête arrive pour la prestation, le gateway zuul, consulte le service d'enregistrement pour voir si la prestation est enregistrée et est disponible. Le cas échéant le proxy redirige la requête vers la prestation. Dans le cas contraire, il retourne un message d'erreur configurable indiquant que la prestation n'est pas disponible.

Le service d'enregistrement permet aussi une gestion élastique de la performance des prestations. Au cas où plusieurs instances de la prestation sont exécutées dans plusieurs machines et toutes enregistrées avec le même identifiant, le gateway zuul obtient une liste de toutes les instances et réalise un *load balancing* automatique.

6.3.12 PRESTAKIT

PrestaKit n'est pas un service, mais un outil transversal (*framework*) pour aider les développeurs de prestations dans leur démarche.

PrestaKit est composé de plusieurs librairies de software pour faciliter la construction de composants *front-office.*

Les librairies sont :

- PRESTATIONS-NG
  - Module Angular/Typescript pour les composants de UX de la prestation.
- PRESTATIONS-BE
  - Module Spring Boot/Java pour le composant *Back-End* du *front-office.*
- FOEHN
  - Module de style avec les polices, images, feuille de style, qui représente l'image visuelle de l'Etat de Vaud.
- SKELETON
  - Ce module utilise tous les autres pour fournir une prestation modèle « Hello World » que le développeur peut utiliser comme base pour implémenter la prestation.

L'information sur cette *framework*, accès au code source et la documentation développeur, et disponible sur le lien https://www.vd.ch/prestakit/

6.4 NORMES

6.4.1 FORMAT D'ECHANGE POUR LES DEMANDES

*Une **XSD** de référence pour l'échange d'état d'un processus métier associé à une demande est en cours de rédaction et sera bientôt disponible.*

6.5 STANDARD INTERFACE UTILISATEUR

Comme décrit dans le chapitre 4, un des objectifs stratégiques de la cyberadministration vaudoise est d'unifier les points d'accès. Cela veut dire que quand un usager interagit avec l'État de Vaud il a une interface unique et cohérente pour interagir avec l'ensemble des services métiers.

Pour unifier l'expérience utilisateur, il est nécessaire d'offrir une image cohérente à travers tous les services de l'État, et de garantir que l'usager n'a pas à connaitre la structure organisationnelle de l'État pour obtenir une prestation.

L'unification des points d'accès veut aussi dire que l'usager n'a pas à chercher ses prestations dans plusieurs portails sectoriels (portail santé, portail fiscalité, etc.), mais dans un seul (l'Etat de Vaud), avec un seul domaine https://www.vd.ch.

6.5.1 CHARTE GRAPHIQUE VD

La charte graphique VD est l'ensemble de ressources qui représentent l'image de l'État de Vaud dans le média WEB.

Toutes les ressources informatiques nécessaires pour construire une prestation (feuilles de styles, polices de caractères et images) sont disponibles dans un dépôt GIT accessible à l'adresse http://dsi-vd.github.io/foehn/.

6.5.2 PAGES MODELE D'UNE PRESTATION

Une prestation de cyberadministration peut tomber dans plusieurs catégories (information à l'usager, recherche d'information ou formulaire de demandes).

Actuellement la charte graphique fournit deux pages modèles pour couvrir ces cas d'utilisation. Il y a une page modèle pour les prestations basées sur des formulaires de capture et une page modèle pour tous les autres.

Page défaut

Cette page modèle peut être obtenue ici : http://dsi-vd.github.io/foehn/components/detail/espace-securise--default

La page consiste en quatre zones de contenu, et une seule colonne. Les quatre zones de contenu sont :

- Header

- Menu
- Titre + contenu
- Footer

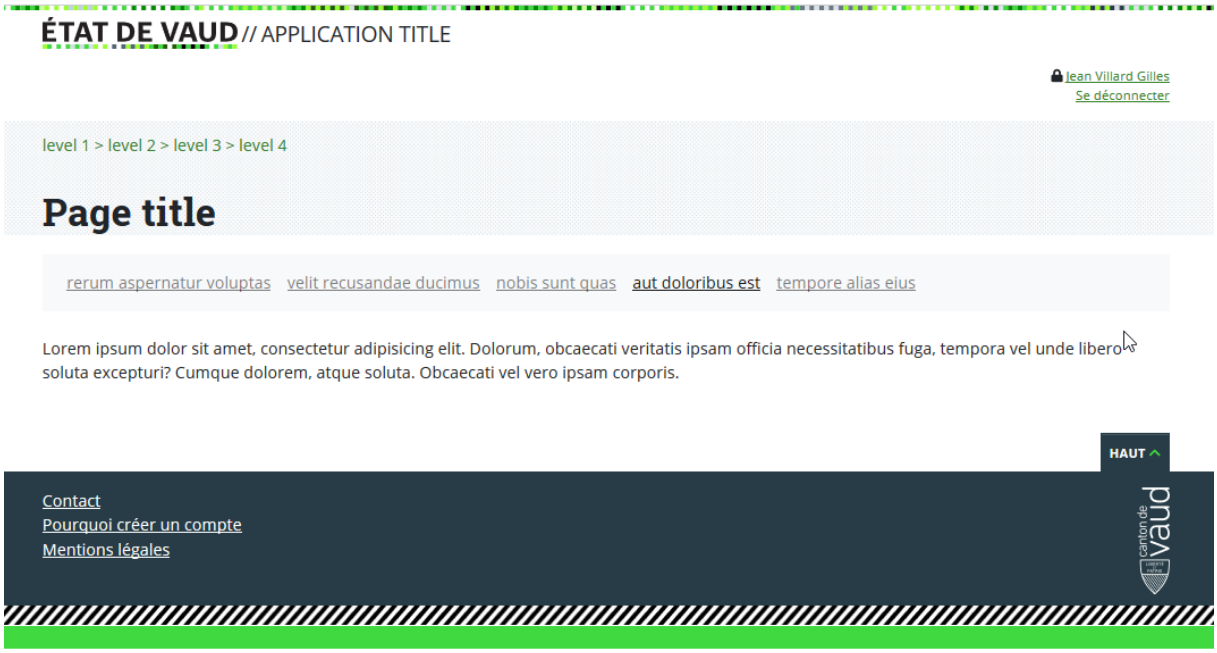


Figure 2 Page modèle défaut

La page modèle pour les prestations qui implémentent un formulaire de demande, sont similaires.

Page formulaire

Cette page modèle peut être obtenue ici : http://dsi-vd.github.io/foehn/components/preview/espace-securise--form

La page consiste en quatre zones de contenu, et une seule colonne. Les quatre zones de contenu sont :

- Header
- Titre prestations
- Titre étape + formulaire
- Footer

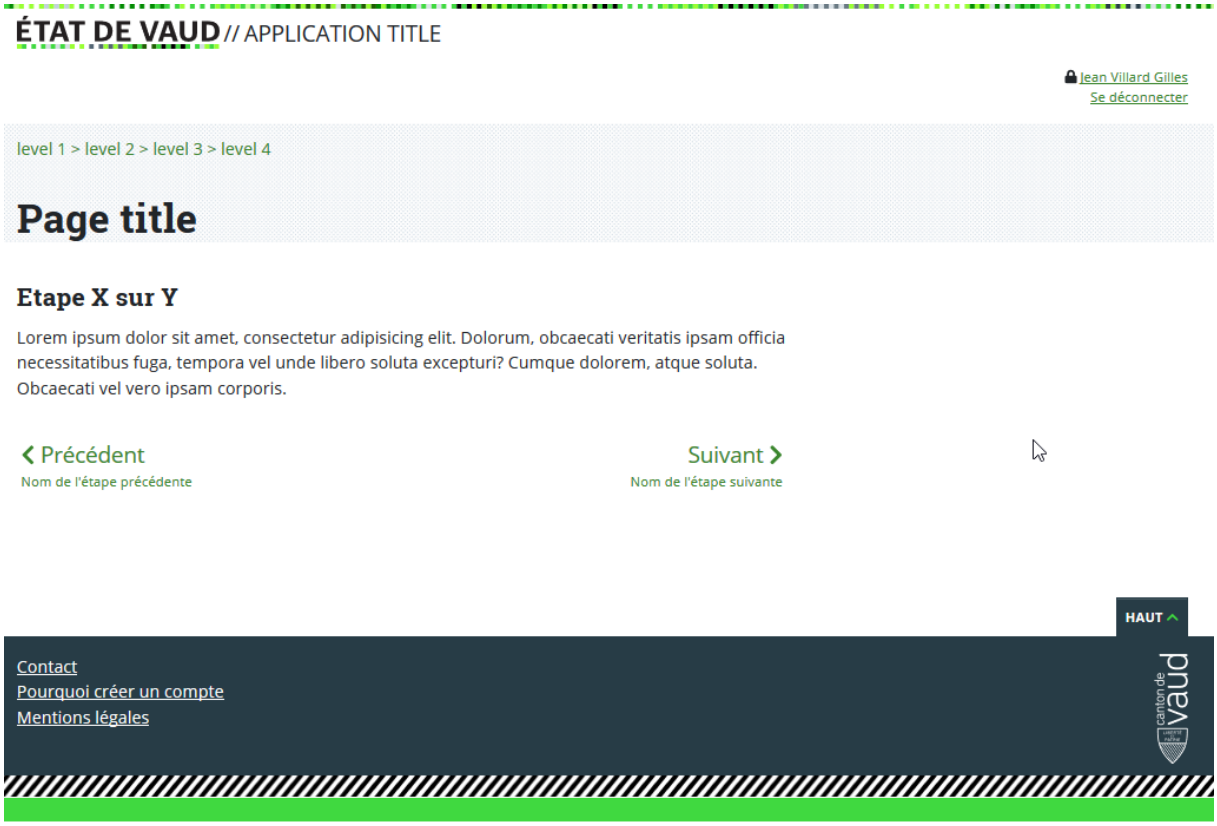


Figure 3 Page modèle formulaire

6.5.3 COMPOSANTS ET ERGONOMIE

Une liste de composants de navigation est disponible dans le projet d'exemple « skeleton » du PrestaKit.

6.5.4 ACCESSIBILITE

Les règles d'accessibilité que les pages des prestations doivent maintenir sont basées sur la norme ARIA. Les pages modèles pour les formulaires de saisie respectent déjà cette norme, mais si l'implémentation ajoute des extensions au modèle elles devront aussi être accessibles.

6.5.5 PAGE WEB ADAPTATIVE

Les pages d'une prestation doivent être adaptatives pour permettre une navigation facile sur desktop et mobile.

PrestaKit implémente déjà la mécanique « responsive » dans les pages modèles, mais si la prestation introduit d'autres éléments ou composants, elles doivent aussi être « responsives ».

6.6 STANDARDS DE SECURITE

Au niveau de la sécurité des systèmes d'information métier, la principale exigence est l'interdiction d'exposer

des applications métiers sur internet. Les applications métiers sont celles qui possèdent les données des usagers pour le traitement de leurs demandes.

L'avantage de la séparation entre un composant « front –office » et les applications métier est le découplage entre l'accès à la prestation et le traitement.

Comme les composants « front-office » sont hébergés dans une zone réseau différente des applications métier, et ne possèdent pas de données métier, le risque de sécurité est plus faible dans le cas où le composants « front-office » est compromis par des cyber-attaques.

Tous les appels des composants « front-office » vers les applications métier sont faits par des appels webservice sur des API REST. Ce sont des appels machine-machine, protégés par un compte technique de service.

Aucune requête provenant d'internet (et indirectement de l'usager) n'a la permission d'accès aux applications métiers et à la zone d'hébergement des données.

Les directives de sécurité sont les suivantes :

- Interdiction d'exposer les applications métier back-office sur Internet.
- Maintenir les applications back-office dans une zone sécurisée d'hébergement pour protéger les données utilisateurs d'accès non valides.
- La séparation des front-office / back-office qui représentent la séparation prestation cyber / application métier.
- La séparation réseau entre la solution portail qui sera hébergé en DMZ et les applications métiers qui resteront en zone sécurisée H.
- La séparation entre les requêtes internet, qui arrivent sur les prestations FO en DMZ et les requêtes machines<->machines entre la DMZ et la zone H.
- La possibilité que les appels machine<->machine entre la DMZ et la zone H soient fait en synchrone ou asynchrone, avec une préférence pour l'asynchrone.
- L'existence de deux niveaux de sécurité des prestations:
    - Accès public: La prestation est accessible directement sans authentification.
    - Authentification forte: La prestation est accessible après authentification avec IUP, obtenu par le processus de création de compte, et un autre élément d'authentification forte (SMS, carte matrix).
- Il est nécessaire d'avoir une validation d'entrée de données dans la partie serveur du « front-office »
- Les prestations devront catégoriser leurs données en termes de données personnelles et sensibles.
- Le processus de matérialisation des prestations devra contenir des tâches de validation des contraintes de sécurité.
- Dans la propagation du contexte de sécurité du composant FO vers le BO lors d'une demande, il faut assurer:
    - Que seules les données concernant l'usager sont extraites de l'application métier BO
    - Que l'interface SOA est alignée avec la fonctionnalité métier et non technique (exemple: pas d'interface qui permette d'exécuter des query génériques SQL)
    - Que la requête ne peut pas être modifiée afin de changer de contexte (suggestion: introduire un hash de la requête)
- Dans le téléchargement de fichiers, quelques contraintes sont ajoutées, comme par exemple:
    - Limitation du type de fichiers.
    - Obligation de quarantaine, avec anti-virus, antimalware, et sandboxing.
    - Interdiction de scripts et macros dans les fichiers.

- Limitation de taille.

6.6.1 COMPTES DE SERVICES DE PRESTATIONS

Chaque composant « front-office » doit posséder un compte technique pour avoir accès à des services métiers ou des services transversaux. Ce compte technique est utilisé pour les accès API entre les composants « front-office » et les systèmes d'informations métier.

Les API disponibles sont accessibles à partir d'un reverse proxy cyber qui contrôle les accès à partir du provisionnement des API dans le proxy.

6.6.2 ROLES DE PRESTATIONS

Chaque prestation cyber est individuellement adressable, avec un seul URL. Si la prestation est sécurisée, cette information devra faire partie du catalogue des prestations. Quand la prestation dans le catalogue est publiée le rôle d'accès est automatiquement provisionné dans IAM à partir de son identifiant.

6.6.3 INFORMATION DE SESSION

Information de la session d'un utilisateur connecté au portail est obtenue à partir d'un service REST qui s'appelle « Session Info» (chapitre 6.3.7). Ce service permet à la prestation d'obtenir une collection d'informations sur l'usager connecté.

L'information disponible peut être consultée ici (authentification requise). L'appel de ce service est disponible dans PrestaKit.

6.7 STANDARDS DE DEPLOIEMENT

Pour le déploiement d'une prestation cyber, le projet doit avoir les prérequis suivants:

- Le projet doit avoir une personne avec le rôle d'intégrateur. Ce rôle a la responsabilité de provisionner les environnements et de garantir le fonctionnement de la prestation en intégration.
- Dans le cas où la prestation est développée par un fournisseur externe, l'intégrateur devra fournir un accès VPN au fournisseur, pour lui donner accès au réseau ACV et aux outils de la DSI (Bitbucket, Nexus, etc.).

6.7.1 SOURCES

Les sources de la prestation devront être hébergées dans le système de contrôle de version à la DSI, actuellement Bitbucket. Le projet doit avoir un *repository* pour le composant *front-office* de la prestation séparé du composant *back-office*.

6.7.2 LIVRABLE DOCKER

Les composants *front-office* de la prestation devront être packagés dans une image Docker. C'est de la responsabilité du projet de construire le Dockerfile correspondant et de le maintenir dans le système de contrôle de version.

6.7.3 ENVIRONNEMENTS

Une prestation cyber aura au minimum un composant *back-office* et un composant *front-office*.

Le projet doit fournir au minimum les environnements INT, VAL et PROD pour le composant *back-office*, au cas où ils n'existent pas déjà.

Pour le composant *front-office,* le projet n'a pas besoin de provisionner les environnements parce que le Portail permet de mutualiser l'infrastructure en DMZ grâce aux conteneurs Docker.

6.7.4 DEFINITION URL D'ACCES

L'URL de la prestation en production sera défini par son identifiant dans le catalogue des prestations. Toutes les prestations sont exposées dans le portail selon le schéma suivant :

- Prestations Publiques : https://prestations.vd.ch/pub/<identifiant>
- Prestations Sécurisées : https://prestations.vd.ch/<identifiant>

7 PRESTAKIT

La documentation de PrestaKit est disponible sur https://www.vd.ch/prestakit/