

1. OBJECTIF DU DOCUMENT

Ce document décrit les principes et obligations de gestion du poste de travail standardisé au CHU de Nantes (CHUN).

Cette annexe doit permettre aux candidats de répondre aux différentes consultations émises par le CHU de Nantes en proposant une solution technique adaptée et optimisée à l'environnement cible.

Le respect de cette annexe technique ne présuppose pas de l'implémentation qui devra être validée par les équipes des services numériques.

2. GESTION DES POSTES CLIENTS ET EQUIPEMENTS NUMERIQUES

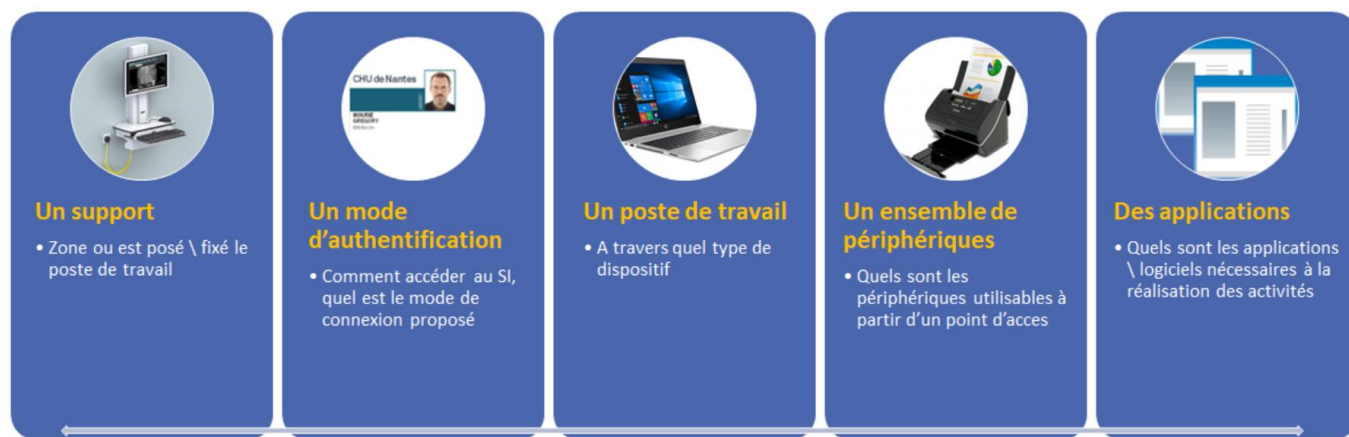
Ce support rassemble les différentes informations techniques et organisationnelles destinées à la définition, au maintien, à la mise à jour et à la modification du standard, basé sur un socle normalisé.

Il présente :

- **Le principe de catégorisation**
 - Les postes sont regroupés selon leur similitude d'usage
- **Les contraintes concernant l'authentification de l'utilisateur pour accéder au poste client**
 - L'ouverture d'une session Windows "standard" après insertion carte (le poste personnel) ou le déverrouillage d'une session Windows générique après insertion carte (le poste partagé)
- **Les contraintes pour connecter un équipement au réseau CHU**
 - Installation d'un master Windows CHUN (suite acquisition marché publique ou fourniture par éditeur) pour un accès complet (domaine Microsoft CHUN, réseau de confiance "trusted") ou système géré par le fournisseur avec un accès réseau restreint (pas de jonction au domaine, pas d'outils CHUN, réseau "untrusted" avec accès basés sur matrice de flux réseau)
- **Le principe de qualification**
 - Tout matériel ou logiciel intégré au parc doit faire l'objet d'une qualification interne

3. CATEGORISATION DES EQUIPEMENTS NUMERIQUES

Un environnement de travail standardisé CHU de Nantes est défini par la combinaison de cinq composants :



REDACTEUR(S)	VERIFICATEUR(S)	APPROBATEUR(S)	Date d'application
Eric MALEVALLE (Responsable - PILNH \Services Numériques\Infrastructures)	Pierrick MARTIN (Coordonnateur qualité - PILNH \Services Numériques)	<Ne pas modifier>	30/05/2023

3.1 Support

Différents supports sont proposés\disponibles en fonction de l'usage et de la localisation du poste de informatique ;



La réponse aux besoins de mobilités des soignants et médecins (visite de patients, administration de médicaments, soins ...) est satisfaite par la mise à disposition de postes informatiques sur chariots (chariot de visite, chariot médicament, chariot de soins ...), les postes localisés en salle de soins destinés à un usage d'affichage simple (peu ou pas d'interactions utilisateur) disposent généralement d'un support de type fixation murale etc...

3.2 Mode d'authentification

3.2.1 Principe

Le CHU de Nantes fournit à chacun de ses agents une carte d'établissement (la "**carte Gaia**") sur laquelle s'appuie la gestion des accès **logique** (poste de travail, applications ...) et **physique** (locaux, parking, restauration...).

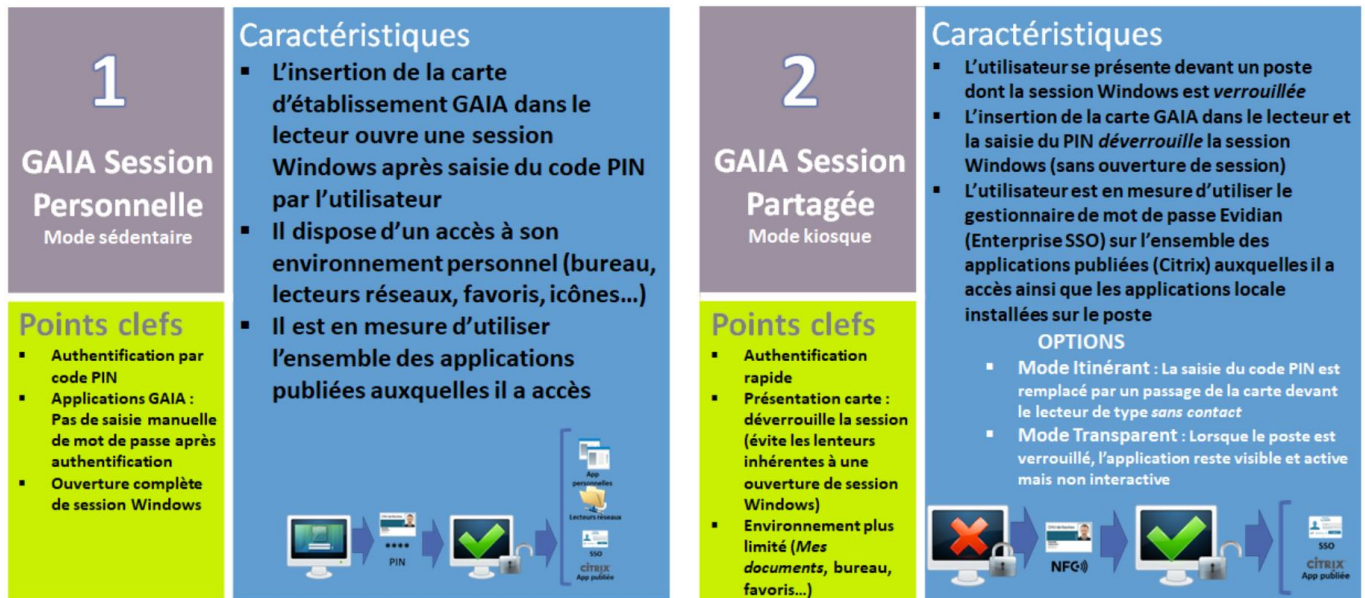
Pour accéder au poste et à son environnement système et applicatif, le CHU de Nantes utilise la solution Gaia (basée sur les produits Evidian Enterprise SSO et Authentication manager). Cette suite permet donc à l'utilisateur d'accéder à un environnement Windows et aux applications métier via l'utilisation d'une carte à puce propre au CHU de Nantes (carte d'établissement).

Après l'**authentification primaire** de l'utilisateur (code PIN), Entreprise SSO récupère dans le référentiel des données de SSO, les attributs de sécurité de l'utilisateur, tels que **les mots de passe** pour accéder à ses applications cibles. Ces attributs de sécurité sont **stockés de manière sécurisée** dans le référentiel des données de SSO puis rapatriés sur le poste de travail dans un cache de sécurité chiffré.

La solution de SSO va se substituer à l'utilisateur pour la saisie des credentials (identifiant et mot de passe) vers les applications référencées (grâce à un script d'identification des champs de saisie à configurer depuis les consoles Evidian).

La solution permet ainsi d'assurer la gestion des multiples mots de passe dès lors que l'utilisateur s'est authentifié au démarrage de sa session.

La solution Gaia installé sur un poste de travail peut être configuré en mode Session personnelle (Sédentaire) ou en mode session partagée (kiosk) :



En fonction du contexte d'utilisation de l'application (poste personnel ou partagé, application client lourd ou application publiée) l'authentification aux applications métiers est basée :

- Sur du SSO classique ActiveDirectory-Kerberos (Windows Integrated Authentication - WIA)
- Sur du SSO Evidian (client SSO) : un agent (Evidian User Access), exécuté sur le poste de travail, capture les fenêtres d'authentification et saisie les champs identifiant/mot de passe en se basant sur les définitions techniques du script e-SSO contenu dans le container de l'utilisateur.

3.2.2 Détail de fonctionnement du mode Gaia Session Partagée

Par défaut, le principe du mode Session partagée (aka "kiosk") est le suivant :

1. Au démarrage initial du poste, le système Evidian assure une ouverture de session Windows automatique sans avoir à saisir le mot de passe (autologon avec un compte Windows **générique**)
2. Avant l'apparition du bureau Windows, le système Evidian verrouille la session Windows, aucune action utilisateur n'est possible

Lorsqu'un utilisateur souhaite utiliser le poste :

1. Il insère sa carte d'établissement (carte "Gaia", à puce contact (historiquement IAS ECC, actuellement ID Prime) et sans contact RFID (MiFare classic)) dans le lecteur
2. Il saisit son code PIN pour déverrouiller la **session Windows générique**
3. En arrière-plan, l'agent Evidian se charge sous l'identité (login et mot de passe) du porteur de la carte
4. L'agent Evidian ferme toute les applications éventuellement ouverte par l'utilisateur précédent et réalise la connexion des lecteurs réseaux du porteur de la carte (fonction *FUSMap*)



Seul l'agent Evidian identifie le porteur de la carte, la session Windows est toujours celle du compte windows **générique**

L'agent Evidian connaît donc l'identité du porteur de la carte ; A partir de là, lorsqu'une fenêtre d'application connue par l'agent apparaît, celui-ci se substitue à l'utilisateur pour saisir son identifiant (login) et son mot de passe :

Exemple :

- Lorsque le client Citrix se lance, une fenêtre d'authentification apparaît, l'agent SSO capte cette fenêtre et rentre le login AD et le mot de passe de l'utilisateur à sa place ; Citrix est donc authentifié

avec le l'identité du porteur de la carte et lui affiche ses icônes de raccourcis d'applications sur le bureau

- Lorsque l'utilisateur lance une application installée sur le poste (client lourd) et que celle-ci est connu par le système Evidian, l'agent Evidian saisie a la place de l'utilisateur son identifiant et son mot de passe
- Lorsque l'utilisateur ouvre mail.chu-nantes.fr dans son navigateur, l'agent Evidian reconnaît cette adresse et saisie l'identifiant et le mot de passe de l'utilisateur dans les champs login et mot de passe

Ce mode peut être personnalisé en fonction de l'usage :

- **Mode Flash (sans contact)** : Un simple passage de la carte sur le lecteur (sans contact) déverrouille la session et lance le moteur Evidian grâce à la puce RFID de la carte
- **Mode Verrou transparent** : lors du verrouillage de la session (après retrait carte par exemple), le bureau reste visible mais le clavier et la souris sont inopérant (utile par exemple dans le cas d'un PC d'affichage)
- **FUSMap Exception** : Ce mode permet de ne pas fermer les applications ouvertes et de ne pas connecter les lecteurs réseaux du porteur de la carte mais de laisser ceux du compte générique
- **FUSMap Custom** : Ce mode permet d'exclure une application donnée de la liste des applications à fermer lors du changement d'utilisateur

Chaque cas d'usage étant différent, la mise en place d'une solution doit être discutée avec la cellule Infra\Poste Client

3.3 Poste de travail

Plusieurs "form factors" sont mis à disposition du personnel en fonction de l'usage qui sera fait du poste de travail. Le critère principal d'affectation est généralement lié aux besoins d'affichage (taille de diagonale) :

Segment	Sédentaire					Mobile		Ultramobile		Spécialisé		
Catégorie	Générique	Station	Compact			Générique	Ultra portable	Tablette	Smart phone CHU	Affichage dynamique	PDA	Vidéo projecteur
Modèle	Lenovo Think Centre	Lenovo Think Station	AllInOne	Tiny	PanelPC	Lenovo 15"	HP 13"	iPad	Surface	Android	22"	50"



Le poste de travail dispose d'un **système d'exploitation** conçu, maintenu et administré par la Direction des Services Numériques. Chaque poste de travail est qualifié en interne avant mise en production afin de vérifier sa compatibilité avec les autres éléments du SI.

Eléments clef :

- Différents formats en fonction de l'usage
- Le nombre de postes à un impact fort sur d'autres coûts (CAIH\SPIE\Trend...)
- L'hétérogénéité des matériels complexifie la gestion et augmente le nombre et/ou le temps de traitement des déploiements et des incidents

- Extension de la garantie constructeur (3 ou 5ans) par le titulaire du marché (jusqu'à 4ans supplémentaires)
- Chaque poste doit être qualifié et intégré aux différents systèmes par l'équipe INFRA\Poste Client
- Leur gestion est assurée par des outils dédiés (Windows avec SCCM, Apple et Android avec [WorkspaceOne](#))
- Les mises à jour systèmes sont automatiques et obligatoire
- Acquisition auprès de marchés nationaux (CAIH, UGAP, etc.) ou hors marché (période de pénurie, demandes spécifiques, dons...)

Le matériel acquis en dehors des processus DSN peut parfaitement être intégré au parc : Dès lors que le master CHU est installé sur le matériel, il peut être connecté au domaine CHU et bénéficier de tous les outils de gestion de configuration du CHU. Dans le cas contraire, il dispose simplement d'une connexion réseau en zone "untrusted" et le poste n'est pas géré par la DSN.

3.4 Périphériques

En fonction du type de postes et de leur usage, différents périphériques sont présents sur les postes, par défaut ou en option :



Chaque matériel doit être **référéncé** avant déploiement. Le référencement consiste à valider la capacité de la Direction des Services Numériques à acquérir, déployer, maintenir et remplacer le matériel. Le risque qu'un déploiement interfère sur d'autres composants du poste (système, logiciel, autre matériel...) doit être géré via le processus de qualification interne DSN en amont.

3.5 Applications

Chaque application ou outil installé sur un poste CHU doit être référencé et intégré. Certaines applications\logiciels\composants sont installés en standard lors de la descente d'une image système sur un poste. Cet ensemble d'applications sont regroupés dans le socle commun aka **Master CHU**.

En fonction du résultat de la qualification initiale, le logiciel peut être déployé de différentes manières :

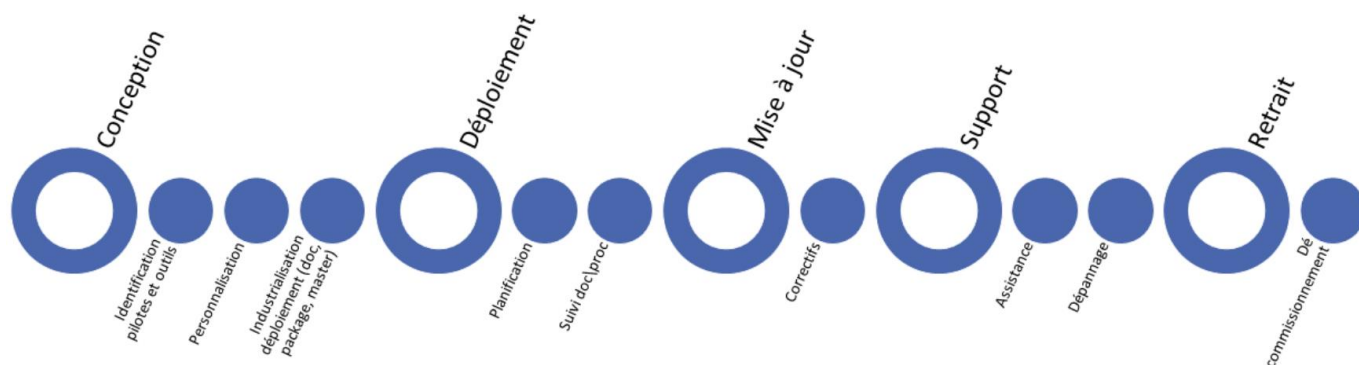
1. Publication d'application installée sur un serveur (Citrix) : L'application est installée et exécutée sur un serveur et est présentée à l'utilisateur par une technologie de déport d'affichage
2. Déploiement "Sans assistance" (MECM) : L'application est préalablement packagée pour permettre une installation silencieuse et sans assistance depuis l'outil SCCM \ MECM \ [ConfigMgr](#) de Microsoft. Elle est ensuite exécutée localement.
3. Installation manuelle : L'application est installée manuellement par un technicien en suivant une procédure. Le poste est immobilisé le temps de l'installation et de la configuration.

4. NORMES ET STANDARDS

4.1 Gestion du système d'exploitation (Windows 10)

La version de Windows 10 déployée au CHU au 01 février 2023 est la version 22H2 en version Enterprise et en mode Semi Annual Channel.

La gestion du cycle de vie du système d'exploitation suit généralement les étapes suivantes:

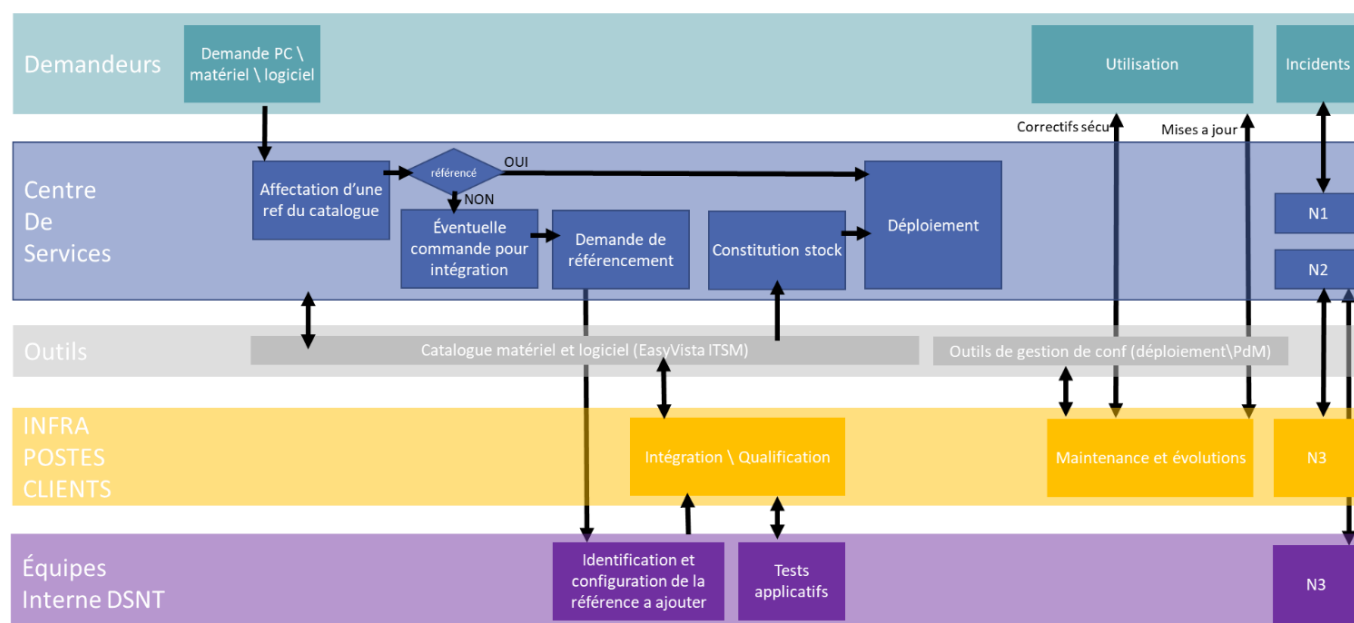


4.2 Principe de gestion des nouvelles références (nouveau logiciel ou nouveau matériel)

Toute application et matériel présent sur le parc informatique doit préalablement être identifié et documenté avant déploiement en production.

L'objectif est principalement de maîtriser l'hétérogénéité des matériels ou logiciels de marque/modèle différents pour un même usage. Cette homogénéité des références réduit la complexité de gestion (acquisition, constitution de stocks, qualification, déploiement, dépannage, maintenance, remplacement...).

L'ajout de nouveau matériel ou logiciel passe principalement par le processus macro présenté ci-dessous :



Le point de départ d'une nouvelle intégration passe généralement par une "demande de référencement" : Elle permet l'éventuel ajout d'un matériel ou logiciel en réponse à un besoin non couvert par les items existant au catalogue. Cette demande doit être formalisée depuis l'outil d'ITSM Easyvista:

The screenshot displays the 'Résultats de recherche' (Search Results) page of the ITSM Easyvista tool. At the top, there is a navigation bar with links: 'BESOIN D'AIDE ?', 'DÉCLARER UN INCIDENT', 'EFFECTUER UNE DEMANDE', 'Mes tickets', 'Mes tâches', and 'Mon compte'. Below this, the search bar shows 'JE RECHERCHE PAR MOTS-CLÉS' with the keyword 'référencement' entered. The results are categorized into three sections: 'J'ai besoin d'aide sur :', 'Déclarer un incident :', and 'Effectuer une demande sur :'. The 'Effectuer une demande sur :' section contains two items: 'Référencement d'un nouveau logiciel' and 'Référencement d'un nouveau matériel', each with a 'Détails' button and a 'Demander' button.

L'équipe Gestion des Demandes Unitaires (GDU) vérifie la cohérence de la demande et l'affecte pour analyse à l'équipe DSN la plus à même d'y répondre. Cette équipe, en lien avec "Infra\Postes Clients", réalise l'intégration et la qualification de la nouvelle application ou du nouveau matériel.

4.3 Ajout d'une nouvelle application

Pour l'ajout d'une nouvelle application au catalogue, les principales actions à réaliser sont les suivantes :
Identification du périmètre

- Nombres d'utilisateurs, fréquence d'usage, profiles, mode d'accès, dépendance avec le matériel, licences, mode d'authentification...
- Validation de l'intégration
- Vérifier que l'installation est possible dans le contexte CHU, l'adapter au besoin (changement de versions de composants, exclusion AV...)
- Choix du mode de déploiement
- Virtualisation avec [AppV](#), publication avec Citrix, déploiement avec MECM, installation manuelle sur procédures
- Validation \ recette
- Validation des tests applicatifs \ fonctionnels
- Intégration aux référentiels
- Documentation Wiki, création du CI [EasyVista](#), référencement dans MECM
- Validation phase transition
- Valider les éléments nécessaires au passage du Build au Run (support, maintenance, évolutions...)
- Mise en production
- Déploiement en production

4.3.1 Détail : Choix du mode de déploiement

La mise à disposition \ installation d'une application sera réalisée via les technologies suivantes :

Mode publication d'application (Citrix)

Mode installation traditionnelle (MSI, [InstallShield](#)...) sans assistance (unattended) via CHUStore

Mode manuel\interactif

Le tableau ci-dessous synthétise les principaux critères de choix :



Xen Desktop

MECM

Manuel

CRITERES FONCTIONNELS

L'application doit cibler des ordinateurs précis et non des utilisateurs	non	oui	oui
L'application doit être accessible par les utilisateurs ciblés (et uniquement ceux-ci) sur les postes partagés (type kiosk))	oui	non	non
L'application dépend d'un matériel	non	oui	oui
La documentation d'installation\paramétrage n'est pas fournie et des choix différents doivent être réalisés en fonction de l'utilisateur ou du poste cible	non	non	oui
L'application doit "suivre" l'utilisateur , quel que soit son poste (roaming de sessions)	oui	non	non
L'éditeur ne valide pas une utilisation Citrix	non	oui	oui
Mise à jour fréquente	oui	non	non
Le périmètre est très limité (peu d'utilisateurs et/ou de postes)	oui	non	oui

CRITERES TECHNIQUES

L'application est proche du système (installation de pilotes ou services)	oui	oui	oui
Forte contraintes réseaux (latence, débit...) ⇒ Utilisable en VPN ADSL?	oui	non	non
L'application n'est pas installable en mode silencieux sans assistance	oui	non	oui

4.4 Ajout d'un nouveau matériel

Pour l'ajout d'un nouveau matériel au catalogue, les principales actions à réaliser sont les suivantes :

Identification du périmètre

- Nombres d'utilisateurs, dépendance avec le logiciel...
- Validation de l'intégration
- Vérifier que l'installation est possible dans le contexte CHU, que le matériel n'impact pas d'autres éléments et qu'il est compatible avec les équipements ou les logiciels existants
- Validation \ recette
- Validation des tests applicatifs \ fonctionnels
- Intégration aux référentiels
- Documentation Wiki (installation, dépannage, maintenance, consommable éventuels), création du CI [EasyVista](#)
- Validation phase transition
- Valider les éléments nécessaires au passage du Build au Run (support, maintenance, évolutions...)
- Mise en production
- Déploiement en production

4.5 Connexion d'un équipement au réseau CHU (Fourniture par société externe)

4.5.1 Politique de sécurité

Un matériel est considéré comme "extérieur" dès lors qu'il ne dispose pas du socle et des composants validés et supportés par la DSN du CHU (ex pour un PC, le "Master CHU" windows10). Il n'est pas référencé dans l'ITSM, pas présent dans l'[Active Directory](#) et ne dispose pas de l'agent MECM\SCCM.

Dans le cas d'une nécessité de connexion d'un équipement extérieur au réseau interne du CHU, une justification doit être formalisée et approuvée par le RSSI. Les SN du CHU de Nantes se réservent la possibilité de proposer que l'acquisition projetée soit prise en charge dans le cadre d'un de ses marchés. Une demande ne pourra être approuvée sans respect des contraintes suivantes (source PSI SMSI SOA Doc PTS) :

A13 - Sécurité des communications

Gestion de la sécurité des réseaux

Les réseaux sont cloisonnés.

Les équipements informatiques (PC, MFP, équipements biomédicaux) sont déployés dans la version OS et patch officielle de la DSN, disposent d'un MASTER DSN avec le pack des outils (SCCM, intégration AD, AV à jour, PDM, GAIA, etc.) et sont intégrés au domaine AD et gérés de façon industrielle avec le reste du parc.

Les équipements qui ne peuvent pas respecter cette configuration sont isolés sur des VLAN filtrés derrière un pare-feu interne, il appartient au demandeur de fournir la liste des flux et des IP.

Toute exception à cette règle et toute modification du MASTER doit être explicitement validée par le RSSI.

Le VLAN des admins est isolé.

4.5.2 Types de réseaux disponible

Deux types de réseaux sont disponibles pour connecter un équipement au réseau CHU :

Deux types de réseaux sont disponibles pour connecter un équipement au réseau CHU:

Réseau Bureautique (Zone de confiance, réseau "TRUSTED")

Types d'accès:

- Accès aux ressources internes (intranet) sans restriction
- Accès aux ressources externes (internet) selon PSSI
- Connexion Ethernet\Filaire (intra.chu-nantes.fr) ou wlan\Sans-fil (Wi-Fi avec authentification 802.1x par certificats au CHUN-MEDICAL)
- Accès possible au réseau UNTRUSTED

Contraintes:

- **Si Windows, réinstallation obligatoire du poste avec le master CHU Windows 10**
- **Si matériel Android, installation obligatoire de l'agent WorkspaceOne**
- Présence des mises à jour de sécurité système Microsoft (KB) et composants tiers (Framework, navigateurs, utilitaires...) à M+1 max
- Présence d'un antivirus à jour

Réseau Isolé (Zone non fiable, réseau "UNTRUSTED")

Types d'accès:

- Accès aux ressources internes (intranet) **sur liste uniquement**
- Accès aux ressources externes (internet) **sur liste uniquement**

Contraintes:

- Système d'exploitation géré par l'intégrateur (acquisition, installation, configuration, maintenance)
- Tout les flux réseaux sont fermés sauf ceux explicitement listés dans la matrice de flux
- Aucun outil\logiciel\application CHU n'est présent sur le poste
- La DSN ne propose pas de support en dehors des accords négociés lors de la connexion de l'équipement
- **Pas de connexion Wifi**

Exigences pour l'intégrateur:

- Fourniture de la matrice de flux réseau (port\protocole\source\destination)
- Obligation de mise à jour régulière du système et des applications
- Formalisation de la méthode de prise de main
- Obligation de présence d'un antivirus avec mise à jour régulière

Modifier