

ADDENDUM

CADRE DE COHERENCE TECHNIQUE DU SYSTEME D'INFORMATION

ASSISTANCE PUBLIQUE HOPITAUX DE PARIS

NORMES ET STANDARDS D'ARCHITECTURE TECHNIQUE
CCT 2024 REVISION 1 / ADDENDUM 2025 REVISION 1
DSN / SAU / CELLULE ARCHITECTURE TECHNIQUE

SUIVI DES VERSIONS

VERSION	DATE	AUTEUR	OBJET DE LA MODIFICATION
2025_R1	08/04/2025	<u>DSN/SAU/ARCHITECTURE</u> DAVID PORTE <u>CONTRIBUTIONS DES EQUIPES</u> DSN/CSI	CREATION DU DOCUMENT MODIFICATION DE REGLES <ul style="list-style-type: none">• @AE / §A.VI.3.1 / AUTHENTIFICATION DES UTILISATEURS AP-HP• @AE / §A.II.4.1 / CHOIX DES SYSTEMES D'EXPLOITATION AJOUT DE REGLES <ul style="list-style-type: none">• @AE / §B.V / SERVEUR DE PUBLICATION

SOMMAIRE

SUIVI DES VERSIONS	2
SOMMAIRE	3
OBJET DU DOCUMENT	4
A. CONTEXTE	4
B. ENTREE EN VIGUEUR	4
LISTE DES MODIFICATIONS APPORTEES	5
I. MISE A JOUR DE LA REGLE SUR LE CHOIX DES SYSTEMES D'EXPLOITATION	5
II. PRECISION ET AJUSTEMENTS SUR LA PRIORITE DES PROTOCOLES DANS LES REGLES D'AUTHENTIFICATION DES UTILISATEURS AP-HP	5
III. AJOUT D'UNE REGLE DE CLARIFICATION SUR LA PORTEE DE PUBLICATION D'UNE APPLICATION DEPUIS LE SERVEUR DE PUBLICATION 'CITRIX XENAPP'	6

OBJET DU DOCUMENT

A. CONTEXTE

Le présent addendum s'inscrit dans le cadre du Cadre de Cohérence Technique (CCT) du SI de l'AP-HP. Il en constitue une mise à jour partielle, destinée à corriger ou enrichir certaines règles définies dans la version :

- APHP_DSN_SAU_Cadre_de_Coherence_Technique_CCT_2024_R1 -

B. ENTREE EN VIGUEUR

Cet addendum entre en vigueur à compter de sa date de publication et **fait foi en tant que référence officielle** pour les règles qu'il précise ou remplace.

LISTE DES MODIFICATIONS APPORTEES

I. MISE A JOUR DE LA REGLE SUR LE CHOIX DES SYSTEMES D'EXPLOITATION

a) POSITIONNEMENT DE LA REGLE DANS LE CCT

@ ARCHITECTURE D'EXECUTION / §A.II.4.1 / Choix des systèmes d'exploitation

b) ANCIENNE REGLE

O La **seule distribution Linux autorisée** est **RedHat Entreprise**.

c) NOUVELLE REGLE

O La **seule distribution Linux autorisée** est la **distribution Rocky Linux**.

II. PRECISION ET AJUSTEMENTS SUR LA PRIORITE DES PROTOCOLES DANS LES REGLES D'AUTHENTIFICATION DES UTILISATEURS AP-HP

a) POSITIONNEMENT DE LA REGLE DANS LE CCT

@ ARCHITECTURE D'EXECUTION / §A.VI.3.1 / Authentification des utilisateurs AP-HP

b) ANCIENNES REGLES

O L'authentification des utilisateurs AP-HP lors d'une connexion à une application doit se baser sur la solution Active Directory

O La délégation de l'authentification à Active Directory doit se faire :
⇒ Soit par un bind LDAPS
⇒ Soit par l'utilisation, par ordre priorité, d'un web service mis à disposition par l'AP-HP

- Accessible en REST API
- Accessible en SOAP

O Une application non hébergée dans les datacenters de l'AP-HP doit authentifier les utilisateurs AP-HP en utilisant la solution de Web SSO mise en œuvre dans le SI de l'AP-HP (solution basée sur SAMLv2)

I La saisie du login et du mot de passe d'un utilisateur AP-HP, correspondant à ses identifiants internes, dans une application non hébergées dans les datacenters est interdite.

O Toute nouvelle application mise en œuvre dans le SI de l'AP-HP doit être compatible avec la solution de Single Sign On (SSO) mise en œuvre à l'AP-HP : la solution Bull Evidian.

c) NOUVELLES REGLES

- O** **L'authentification des utilisateurs AP-HP** doivent utiliser en priorité les protocoles suivants :
 - ⇒ **Protocole OIDC (OpenID Connect)**
 - ⇒ **Protocole SAMLv2.**

En l'absence de compatibilité avec ces protocoles, la délégation de l'authentification direct vers l'Active Directory peut être envisagée à titre exceptionnel, et exclusivement via un bind LDAPS. Ce cas d'usage spécifiques doit être dûment justifiés et validés par le pôle SSI de la DSN.

- O** Une **application non hébergée dans les datacenters de l'AP-HP** (par exemple, **une application SaaS hébergée chez un prestataire** ou dans un **cloud public**) doit exclusivement authentifier les utilisateurs AP-HP en utilisant la solution centralisé d'authentification mettant en œuvre les protocoles OIDC ou SAMLv2

- I** L'utilisation du login et du mot de passe d'un utilisateur AP-HP, correspondant à ses identifiants internes, dans une application non hébergée dans les datacenters est interdite.

- O** **Toute nouvelle application mise en œuvre** dans le SI de l'AP-HP **doit être obligatoirement compatible** avec une authentification SSO via les **protocoles OIDC ou SAMLv2.**

III. AJOUT D'UNE REGLE DE CLARIFICATION SUR LA PORTEE DE PUBLICATION D'UNE APPLICATION DEPUIS LE SERVEUR DE PUBLICATION 'CITRIX XENAPP'

a) POSITIONNEMENT DE LA REGLE DANS LE CCT

@ ARCHITECTURE D'EXECUTION / §B.V / Serveur de publication

b) NOUVELLE REGLE DE CLARIFICATION DE PORTEE

- I** Il est **interdit de publier** (via Citrix, RDP, ...) **une solution applicative exclusivement accessible à partir d'un navigateur.**