MODÈLE GÉNÉRIQUE ANNEXE SÉCURITÉ CCTP

Versions.

Date	Rev	Rédacteurs	Note
18/01/2017	v1.0	PT	Rédaction du document à partir du référentiel de l'APHM réalisé par Philippe Tourron RSSI
01/02/2017	v1.0	JCT	Mise en forme Version 1 du livrable

Description du livrable
Le cahier des clauses techniques particulières (**CCTP**) est une pièce contractuelle essentielle qui nécessite une rédaction appropriée. Élaboré par des techniciens, il doit définir une **expression du besoin qui soit conforme à la réglementation et au besoin de sécurité des Systèmes d'Informations de santé**.

Producteurs
Philippe Tourron (RSSI - AP-MH) William Grolier (RSSI- CHU NICE)

SOMMAIRE

1 INTRODUCTION

Les solutions informatiques déployées au sein du Système d'Information de l'ÉTABLISSEMENT doivent satisfaire les exigences de sécurité informatique définies dans la politique cadre de sécurité de l'ÉTABLISSEMENT.

Les solutions informatiques doivent, d'autre part, respecter au plus près les préconisations en matière de sécurité de l'ASIP, l'ANSSI et du Ministère de la santé (PMSSI qui pourra être fournie sur demande).

Les exigences de sécurité sont obligatoires leur non-respect est éliminatoire et elles sont notées O comme Obligatoire (en début d'exigence) dans ce document.

Les recommandations sont des orientations techniques fortement souhaitées en matière de sécurité pour apporter une cohérence avec les bonnes pratiques et recommandations du secteur santé. Elles sont décrites par cette annexe au titulaire et sont à prendre en compte dans le cadre de sa réponse, elles sont notées R comme Recommandé et le niveau de réponse à ces recommandations sera pris en compte dans l'évaluation technique de l'offre (le chef de projet doit adapter les parties surlignées jaune avant communication).

Le titulaire précisera si sa solution prend en compte ces recommandations. Dans la négative, les solutions palliatives qu'il propose ou le plan produit intégrant ces recommandations seront présentées.

2 EXIGENCES GÉNÉRALES SUR LES LOGICIELS

	Règle de sécurité	Description de la prise en charge	Évaluation
O	Le titulaire s'engage à acquérir et à concéder à l'ÉTABLISSEMENT l'ensemble des licences d'utilisation nécessaires au bon fonctionnement du dispositif connecté, sauf conditions spécifiques. Ceci concerne l'ensemble des logiciels et couches logiques utilisées (OS, progiciels, BDD, télémaintenance…).		
O	Le titulaire s'engage à n'installer et n'activer que les seuls logiciels nécessaires au bon fonctionnement du dispositif.		
O	Le titulaire s'engage à fournir une liste exhaustive des logiciels installés, documentée, contenant les informations détaillant chaque logiciel ainsi que les interactions entre eux.		
O	Pour les logiciels libres, la conformité du logiciel est de la responsabilité du titulaire seul.		
O	Pour les logiciels gratuits, la conformité du logiciel est de la responsabilité du titulaire seul : ils devront aussi respecter les exigences de sécurité.		

	Règle de sécurité	Description de la prise en charge	Évaluation
O	Pour les logiciels de type SaaS (Software as a Service : logiciel hébergé), la conformité du logiciel est de la responsabilité du titulaire seul.		
O	Les personnels du titulaire devront respecter la charte d'accès et d'utilisation du Système d'Information de l'ÉTABLISSEMENT (REF-xxx) lors de toute intervention à l'installation ou en maintenance. Le titulaire s'engage à en informer ses personnels.		
O	Toute opération réalisée par le titulaire et ses personnels lors de l'installation devra respecter les mêmes règles que celles décrites dans le chapitre Maintenance et Télémaintenance durant son exécution.		
R	Les logiciels types Auto-logon ne sont pas souhaités hors cas particulier.		
R	Lorsque des données nominatives sont gérées par l'application, le titulaire décrira s'il fournit une procédure ou un outil d'anonymisation pour pouvoir être appliqué à tout autre environnement que celui de production		
R	Il est souhaitable que les applications ou services nécessitant un fonctionnement permanent y compris lors des démarrages de l'ordinateur hôte, soient hébergés sur des machines ayant un système d'exploitation de type serveur.		
R	Aucune version de système d'exploitation non maintenue par l'éditeur en termes de mise à jour de sécurité ne devrait être installée sauf cas particulier nécessitant une protection supplémentaire à décrire.		
R	Si la solution proposée doit être hébergée sur un serveur de l'ÉTABLISSEMENT, il est recommandé qu'elle soit compatible aux prérequis fournis par la DSI.		

3 IDENTITÉS

L'ÉTABLISSEMENT a pris le parti d'établir le service d'annuaire de la société Microsoft (AD : Active Directory) en référentiel garant de l'unicité des comptes utilisateurs.

	Règle de sécurité	Description de la prise en charge	Évaluation
R	L'exploitation de cet annuaire comme source d'identité logicielle est fortement souhaitée et peut revêtir deux formes : ● Déport de la gestion d'identité de l'application au sein de l'AD ● Mise à disposition d'un point d'entrée (web service, connecteur…) permettant à l'ÉTABLISSEMENT de synchroniser le référentiel d'identités de l'application avec son référentiel d'identité et d'authentification (IAM).		
R	Cas de systèmes (biomédicaux par exemple) installés sur un poste de travail ÉTABLISSEMENT avec besoin de comptes locaux ou de systèmes autonomes pour gérer les comptes au sein du logiciel : il est recommandé d'installer le logiciel sur un répertoire partagé fourni par la DSI dont la sécurité d'accès est prise en charge par un groupe Windows et l'AD.		

4 AUTHENTIFICATION ET SINGLE SIGN ON

L'ÉTABLISSEMENT n'envisage l'authentification unique (Single Sign On) qu'au travers de l'identité de domaine portée par les protocoles communément utilisés en environnement Windows ainsi :

	Règle de sécurité	Description de la prise en charge	Évaluation
O	Les mots de passe des comptes nécessaires à l'administration de la solution doivent pouvoir être modifiés par l'ÉTABLISSEMENT.		
R	S'agissant des applications WEB, l'usage des protocoles NTLM ou Kerberos est attendu en vue de perpétuer implicitement et de manière sécurisée l'identité de l'utilisateur connecté au serveur web.		

	Règle de sécurité	Description de la prise en charge	Évaluation
	Concernant les applications usant d'un client lourd : ● Lorsque le référentiel d'identités de l'application est déporté dans l'AD, l'authentification auprès d'un serveur AD du ticket de session associé au processus applicatif est fortement préconisée. Si l'application n'offre pas – en l'état – la possibilité de récupérer l'identité Windows, un plan d'intégration le permettant est souhaité. A minima, l'authentification de l'utilisateur par mot de passe reposera sur LDAP. ● Lorsque le référentiel d'identités est propre à l'application et seulement synchronisé à l'AD, la simple récupération de l'identité du propriétaire du processus applicatif pourra être tolérée dans l'attente d'une intégration de LDAP à l'application. Ce mode transitoire aux bonnes pratiques est justifié lors du recours à une authentification forte (CPS ou équivalent) à l'ouverture de session Windows.		
R	Dans le cas d'architecture N-Tiers, l'origine de la connexion fera partie du processus d'authentification. Ainsi lorsque l'application permet la propagation des identités utilisateurs jusqu'aux données, l'utilisateur ne saurait se connecter directement au SGBD. La chaine d'accès devra donc être garantie pour chaque strate applicative.		
R	Pour les applications web exposées sur internet et qui intègreraient une authentification et/ou une gestion des comptes : Les pages réservées à l'authentification et à la création de comptes devront intégrer un dispositif de prémunition contre l'usage de robots.		
O	Pour les applications web exposées sur internet et qui intègreraient une authentification et/ou une gestion des ● comptes :		

	Règle de sécurité	Description de la prise en charge	Évaluation
	Les mécanismes d'authentification devront être adaptés à la criticité des données, une authentification forte est exigée pour l'accès à des données de santé par carte CPS ou équivalent (sauf disposition contraire du CCTP qui conduirait l'ÉTABLISSEMENT à prendre en charge une authentification forte en préalable à l'accès à l'application objet du marché).		

5 GESTION DES HABILITATIONS

	Règle de sécurité	Description de la prise en charge	Évaluation
R	La gestion des habilitations doit reposer sur le moteur d'habilitation de l'ÉTABLISSEMENT, (Hospital Security). Ce moteur fournit pour chaque utilisateur un ensemble d'information dont notamment le profil à utiliser dans l'application (fonctionnalités autorisées) et son périmètre d'habilitation (liste des Unités Fonctionnelles pour lesquelles il peut accéder aux informations). L'accès à Hospital Security peut se faire de diverses façons : Appel de web service Provisionning par EAI Dans la mesure où seule la notion de profil (telle que mentionnée ci-dessus, indépendante donc de l'affectation sur des Unité d'affectation de la personne) serait nécessaire, l'utilisation de groupe AD est envisageable. Intégration spécifique, auquel cas l'éditeur devra fournir les éléments pour un accès direct et documenté à son système d'habilitation ne présentant pas de risque pour le fonctionnement du produit (web service, tables de base de données, procédures stockées …)		

6 TRAÇABILITÉ

Les exigences fonctionnelles de traçabilité du CCTP peuvent être supérieures à celle citées ici d'une manière générale pour la sécurité.

L'ETABLISSEMENT met en œuvre la centralisation de ses traces applicatives et systèmes au sein d'un dispositif unique afin d'en garantir l'intégrité, la conservation et la bonne exploitation ;

	Règle de sécurité	Description de la prise en charge	Évaluation
R	la solution proposée devrait exposer de manière sécurisée ses éléments de traçabilité.		

Contenu de la trace :

	Règle de sécurité	Description de la prise en charge	Évaluation
O	En premier lieu les accès utilisateurs (et administrateurs) seront tracés en réussite et en échec.		
R	S'agissant des modifications de valeurs sensibles au sein du dispositif, il est souhaité que les traces correspondantes comportent la valeur en amont et en aval de l'événement. La suppression d'une donnée du point de vue applicatif ne saurait engendrer la perte de l'historique des accès et modifications associées.		
R	Lorsque la gestion des autorisations applicatives – même partiellement – est du ressors de l'application, il est souhaitable que tout événement relatif à l'édition d'un profil ou d'un utilisateur soit tracé.		
R	Dans le cas d'architectures N-Tiers ou lors de l'usage de comptes applicatifs, les traces devront comporter l'utilisateur d'origine et l'ordinateur source de la connexion. Si cela s'avérait impossible, la mise en corrélation des traces des différentes strates applicatives par le biais des identifiants de session devra permettre de déterminer avec certitude la continuité de l'accès.		
O	Dans tous les cas la capacité (ou non) à tracer toutes les actions (y compris la consultation de données) devra être décrite.		

	Règle de sécurité	Description de la prise en charge	Évaluation
O	Les traces produites devront être accessible par l'outil de centralisation des traces de l'ETABLISSEMENT dans un format et un mode d'accès rendus possibles et décrits par le titulaire (ATNA : format IHE, syslog, requête dans une base de données à fournir, fichier à décrire).		

7 PROTECTION DES SYSTÈMES

	Règle de sécurité	Description de la prise en charge	Évaluation
R	Le titulaire s'engage à mettre en œuvre les dispositifs et paramétrages nécessaires pour prémunir ses systèmes contre les attaques virales et intrusives. En cas de nécessité il pourra déployer ses propres utilitaires et politiques de mise à jour ; néanmoins il serait appréciable qu'il consente à inscrire ses dispositifs dans la démarche sécurité de l'ETABLISSEMENT en installant l'antivirus de l'ETABLISSEMENT et en inscrivant ses systèmes dans les règles de gestion des correctifs de sécurité en vigueur pour le reste du SI. De fait, en cas d'intrusion ou de contamination, le titulaire est responsable de la vulnérabilité de ses systèmes vis à vis des correctifs et définitions virales publics.		

8 CRYPTOGRAPHIE

	Règle de sécurité	Description de la prise en charge	Évaluation
O	Dans le cas d'applications web publiées sur internet, l'usage de SSL est impératif. Le titulaire pourra recourir à des certificats fournis par l'ÉTABLISSEMENT.		
O	De manière générale, l'utilisation de la		
	cryptographie par les applications doit être conforme aux standards du marché, et au Référentiel Général de Sécurité (RGS).		
O	Les données utiles à l'authentification doivent être chiffrées lors de leur communication et de leur stockage.		

9 MAINTENANCE ET TÉLÉMAINTENANCE

Lorsqu'une télémaintenance est prévue par le titulaire, des règles strictes doivent être prises en compte :

	Règle de sécurité	Description de la prise en charge	Evaluation
O	La connexion de télémaintenance doit se faire à travers la passerelle Internet sécurisée mise à disposition par l'ETABLISSEMENT (VPN IPSEC ou VPN SSL). La demande de ce VPN devra suivre la procédure de l'ETABLISSEMENT (PRO-xxx).		
O	Au niveau des postes de travail standard de l'ETABLISSEMENT, aucun outil de prise à contrôle à distance ne peut être installé dans le cadre d'une application. Le seul outil de prise à contrôle à distance autorisé est celui servant à l'administration système gérée par la DSI de l'ETABLISSEMENT.		
O	Il est de la responsabilité du titulaire d'assurer la sécurité de sa plateforme d'intervention à distance (données et logiciels)		
O	L'ETABLISSEMENT se réserve le droit de faire (ou de faire faire) des contrôles de sécurité de façon périodique ou événementielle chez le titulaire afin de s'assurer que le niveau de sécurité requis est conforme aux exigences suivantes		
O	le titulaire doit avoir une politique anti-virus et de mise à jour des correctifs de sécurité appliquée sur les postes de télémaintenance.		
R	les postes de télémaintenance devraient être isolés physiquement du réseau local du titulaire.		
O	les données à caractère personnel ou technique de l'ETABLISSEMENT		
	(configuration des équipements) exploitées par les équipes de support chez le titulaire ne doivent pas être divulguées (une protection adaptée doit être réalisée).		
O	L'intervention est encadrée par un règlement, un contrat ou une convention entre l'ETABLISSEMENT et le titulaire, définissant les engagements de chacun, les modalités pratiques, …		

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Le titulaire s'engage sur la sécurité de la prestation, son représentant légal devra signer l'engagement titulaire de maintenance fourni par la DSI (MOD-xxx) rappelant la confidentialité des données et l'engageant à informer ses personnel que tous les accès et actions seront tracés.		
O	Il est de la responsabilité du titulaire de restreindre les accès physiques et logiques de ses postes aux seules personnes autorisées (par sensibilisation et mise à disposition de moyens de sécurité adéquats).		
O	Il est de la responsabilité du titulaire de connaitre en toutes circonstances l'identité de toute personne qui se connecte ou s'est connecté sur la plateforme de télémaintenance et d'en assurer la traçabilité (cette traçabilité pourra être communiquée sur demande de l'ETABLISSEMENT).		
O	Il est de la responsabilité du titulaire de veiller à ce que toutes les informations résiduelles inutiles à l'issue d'une intervention soient supprimées.		
R	Il est souhaitable que le titulaire réalise un suivi permanent des incidents et vulnérabilités liés aux dispositifs connectés et mette à disposition les correctifs et préventifs nécessaires.		
R	Le titulaire pourra détailler exhaustivement les modalités de la maintenance (besoin en RH, temps de réparation…).		
O	Le titulaire s'engage à effectuer des tests de robustesse et de non-régression à chaque évolution du matériel ou du logiciel. Les impacts d'une défaillance qui serait néanmoins constatée seraient de la responsabilité du titulaire, la correction et la prise en charge des impacts à sa charge.		
R	Le titulaire garantit la mise à niveau de ses logiciels et plateformes en cas d'obsolescence du système d'exploitation ou de tout logiciel, étranger au fournisseur et à l'ETABLISSEMENT, indispensable au bon fonctionnement du système, ou fournir à titre gracieux les moyens pour maintenir un niveau de sécurité suffisant.		
O	Le titulaire doit fournir un rapport détaillé de l'intervention effectuée, un modèle pourra être fourni (MOD-xxx).		

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Le titulaire accepte d'utiliser un bastion d'administration pour accéder aux systèmes qu'il devra maintenir (de fait l'accès direct aux serveurs et applications sera interdit). Selon les besoins d'intervention l'accès aux systèmes à maintenir sera ouvert et fermé par la DSI à la demande (du mainteneur ou de la personne habilitée selon le protocole défini dans les conditions de la maintenance). Tout autre mode de fonctionnement devra être validé avec la DSI.		
R	Le titulaire pourra établir un PAS (Plan Assurance Sécurité) afin de faire connaitre les dispositions de sécurité qu'il met en place pour sa prestation. Le PAS traite : ● Des critères de sécurités utilisés dans la désignation des personnes chargées des interventions. ● De la désignation des sites d'exécution de la prestation, protection et accès physiques des locaux utilisés. ● Des règles de protections des informations du Système d'Information associées à la prestation de télémaintenance. ● De l'architecture générale de la plateforme d'intervention (cloisonnement technique etc.). ● Des accès logiques à la plateforme, identification et authentification, mise en veille, déconnexion automatique, gestion des droits, traçabilité… ● Des dispositions prises pour assurer la continuité de l'activité après un sinistre ou un incident majeur. ● De l'assurance et des contrôles de la sécurité des services de l'intervention fournis.		

10 SPECIFICATIONS WI-FI (802.11G OU 802.11B)

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Le chiffrement et l'intégrité des informations circulant sur le réseau doivent être assurés par la mise en place sur les équipements concernés du mécanisme WPA2 (version de la norme IEEE 802.11i certifiée par la Wifi Alliance).		

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Pour l'authentification l'association de WPA2 (« WPA2 – Entreprise ») avec un serveur d'authentification 802.1X (Radius) par le biais du protocole EAP est demandée. Pour éviter la gestion redondante des comptes, le serveur devra s'appuyer sur l'annuaire LDAP centralisé		

11 PROTECTION DES DONNÉES MÉDICALES

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Le titulaire et son personnel, le personnel de l'ETABLISSEMENT sont soumis à un engagement de confidentialité conformément aux préconisations de la CNIL et au Code de la Santé Publique. Ces articles s'adressent notamment auxtitulaires extérieurs.		

Article L1110-4 du Code de la Santé Publique

….Excepté dans les cas de dérogation expressément prévus par la loi, ce secret (secret médical) couvre l'ensemble des informations concernant la personne venues à la connaissance du professionnel de santé, de tout membre du personnel de ces établissements ou organismes et de toute autre personne en relation, de par ses activités, avec ces établissements ou organismes. Il s'impose à tout professionnel de santé ainsi qu'à tous les professionnels intervenant dans le système de santé.

	Règle de sécurité	Description de la prise en charge	Evaluation
O	En conséquence, notamment, les jeux de données fournies par l'ETABLISSEMENT sont strictement confidentiels et sont liés au secret professionnel.		
R	Un outil de codage des données est souhaité. Cet outil doit permettre de banaliser les informations de la base de données ou bien des fichiers de données pour préserver le secret médical.		
R	En outre, cet outil doit préserver l'anonymat des personnes si cela est le cas dans les données de tests.		

12 CAS PARTICULIERS SELON LE PÉRIMÈTRE

Cas de moyens mobiles :

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Tout dispositif mobile doit être chiffré (en conformité avec le Référentiel Général de Sécurité : RGS) et les clefs de chiffrement doivent être remises à l'ETABLISSEMENT.		

Cas de service hébergé en dehors du Système d'information de la DSI (pour tout ou partie de l'objet du marché) :

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Si le centre de maintenance ou d'hébergement est en dehors du territoire national cela devra être précisé pour analyser les contraintes réglementaires associées au type de système à protéger selon la politique de sécurité de l'état et du ministère de rattachement.		
O	Si des données de santés sont hébergées chez le titulaire ou un de ses sous-traitants celui-ci doit être agréé hébergeur de données de santé par l'ASIP (ou toute commission compétente désignée par la réglementation).		
O	Si des données nominatives à caractère personnel font l'objet de traitement par le système, une déclaration CNIL sera nécessaire et le titulaire devra démontrer le niveau de protection adapté à la criticité de ces données ? Cette démonstration fera l'objet d'un livrable de son offre.		

Cas de services installés dans le SI de l'ETABLISSEMENT mais administrés en autonomie par le titulaire

- Concernant l'accès au service hébergé par des utilisateurs de l'ETABLISSEMENT :

	Règle de sécurité	Description de la prise en charge	Evaluation
R	Un accès identifié, authentifié et habilité selon les conditions décrites dans les paragraphes précédents (Identité, Authentification, Gestion des habilitations) pour un logiciel installé dans le SI de l'ETABLISSEMENT est fortement souhaité, en cas d'impossibilité technique, un identifiant sera communiqué aux utilisateurs ou un mode de gestion permettra à un utilisateur identifié comme administrateur des comptes utilisateurs de gérer les utilisateurs.		
O	Une authentification d'accès devra permettre aux utilisateurs d'accéder aux services avec un niveau de sécurité adapté aux données à protéger, les utilisateurs pourront changer leur authentifiant (mot de passe ou moyen d'authentification), la confidentialité des mots de passe doit être garantie par l'hébergeur lors de son stockage (chiffré) et de sa saisie. Pour l'accès aux données de santé l'authentification devra être conforme aux exigences d'authentification forte de la CNIL (carte CPS ou équivalent).		
O	Les mots de passe ne doivent pas être stockés en clair dans le logiciel ou la base de données.		
O	Le titulaire remettra un compte et authentifiant pour audit au RSSI de l'ETABLISSEMENT et acceptera que l'ETABLISSEMENT réalise ou commandite des audits externes pour vérifier la conformité aux exigences de sécurité.		

Concernant la continuité du service hébergé :

	Règle de sécurité	Description de la prise en charge	Evaluation
R	Le service ne doit pas être indisponible plus de x heures (selon les besoins décrit dans le CCTP, cette recommandation peut alors devenir une exigence Obligatoire)		
R	Une copie exploitable des données (fichier informatique avec champs délimités et décrits) sera transmise ou accessible tous les x jours (mode de mise à disposition à décrire par le fournisseur ou imposé par le CCTP)		

Concernant La réversibilité du service hébergé :

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) sera transmise à l'ETABLISSEMENT 3 mois avant la fin de ce contrat pour permettre la réalisation de tests de migration (mode de mise à disposition à décrire par le fournisseur ou imposé dans le CCTP)		
O	Une copie exploitable des données (base de données ou fichier informatique avec champs délimités et décrits) sera transmise à l'ETABLISSEMENT en fin ce contrat (mode de mise à disposition à décrire par le fournisseur ou imposé dans le CCTP)		

Concernant La garantie de Confidentialité des données hébergées :

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Le titulaire s'engage à garantir un accès aux données aux seules personnes habilitées selon les besoins de l'ETABLISSEMENT		
O	Les intervenants seront identifiés et devront signer un engagement de confidentialité individuel (MOD-xxx). Les accès et actions réalisées pourront être tracés.		
O	Le titulaire s'engage à détruire les données en fin de contrat après les avoir restituées à l'ETABLISSEMENT sous une forme exploitable.		

Si la solution est installée dans infrastructure informatique de l'ETABLISSEMENT mais administrée intégralement par le titulaire :

	Règle de sécurité	Description de la prise en charge	Evaluation
O	Le titulaire doit s'engager à maintenir les composants à niveau en termes de sécurité et garantir une administration sécurisée intégrant a minima un antivirus mis à jour et un système d'exploitation ainsi que tous les composants mis à jour des correctifs de sécurité publiés par les éditeurs selon des modalités de qualification à décrire.		

	Règle de sécurité	Description de la prise en charge	Evaluation
O	L'accès depuis l'extérieur de l'ETABLISSEMENT pour l'exploitation et la maintenance devra se faire dans les conditions décrites au paragraphe Maintenance et Télémaintenance.		
O	Les échanges avec l'extérieur de l'ETABLISSEMENT devront être sécurisés : utilisation de protocoles sécurisés et filtrage et contrôle par les équipements de sécurité de l'ETABLISSEMENT (l'ETABLISSEMENT se réserve le droit de tracer tout accès et action sur les systèmes installés dans son infrastructure.		

13 GLOSSAIRE DES TERMES EMPLOYÉS

AD (Active Directory) : Service d'annuaire de la société Microsoft
Application Web : Architecture applicative reposant sur la mise à disposition par HTTP de contenus HTML dynamiques
HTTP (Hypertext Transfer Protocol) : protocole de communication client/serveur reposant sur le principe de requête/réponse vis-à-vis de ressources identifiées par une adresse réticulaire
IAM (Identity and Authorization Manager) : Service de gestion et de synchronisation des identités et autorisations entre les différents composants du système d'information
Kerberos : Protocole d'authentification reposant sur un chiffrement symétrique
LDAP (Lightweight Directory Access Protocol) : protocole standard de communication avec un service d'annuaire
NTLM : Protocole d'authentification reposant sur un mécanisme de challenge
PKI (Public Key Infrastructure) : Dispositif de gestion des clefs publiques. Permet l'édition des bi-clefs nécessaires au cryptage asymétrique.
SGBD : Dispositif de dépôt et d'indexation de données permettant l'adressage de grands volumes
SOAP : Protocole applicatif mis en œuvre dans le cadre de web services reposant sur l'échange de flux XML par le biais d'un serveur HTTP.
Web Service : Service applicatif exposé sous forme d'API selon le protocole SOAP.
XML (Extended Markup Language) : « langage de balisage extensible[1] » en français) est un métalangage informatique de balisage générique.