



AUTORISATIONS HABILITATIONS ET ACCÈS



SOMMAIRE DU SÉMINAIRE

GÉNÉRALITÉS

Les définitions

COMMENT EN SOMMES-NOUS ARRIVÉS LÀ

La multiplicité des annuaires
De nouvelles manières de travailler

L'APPROCHE GLOBALE DE L'AHA

Les grands domaines de l'AHA
Les problèmes (concrets) à résoudre
Une question de volumes
Le schéma global AHA

L'ÉQUIPE PROJET ET SES COMPÉTENCES

L'organisation et les compétences
nécessaires
Comment trouver les bonnes informations

LES USAGES ET PROBLÈMES QUI NÉCESSITENT UNE APPROCHE AHA

La problématique du BYOD
Failles de sécurité, comportements
Le RGPD change l'approche « gestion
d'identités »

LES TECHNOLOGIES DE BASE QU'IL FAUT CONNAÎTRE : XML ET JSON

LES FONDEMENTS CRYPTOGRAPHIQUES

Le chiffrement, mathématiques et clés
Ne pas confondre clés et hash
Les principaux algorithmes
L'exemple du chiffrement symétrique DES
Panorama des algorithmes utilisés
Chiffrement quantique et homomorphe
Principe de la signature électronique
Fonctionnement d'une PKI
La technologie SSL/TLS
La mécanique ACME
La chaîne d'approbation des certificats
Le rôle clé des certificats racine
Let's Encrypt, oui mais...tout n'est pas parfait

UNE BONNE GESTION DES MOTS DE PASSE

La catastrophe sécuritaire des mots de passe
Le comportement contestable des usagers
Ce que pourrait être un mot de passe
Les mots de passe forts
Hashage pour garantir l'intégrité d'un mot
de passe

Les recommandations que l'on n'applique pas
L'usage des clés de sécurité
Les captchas

L'AUTHENTIFICATION MFA : DURCIR LE PROCESSUS

Réduire le rôle des mots de passe
Authentification multifacteur (forte)
Authentification à une phase
Authentification à deux phases 2FA
L'authentification MFA dans Windows 10
et OKTA

LES BASES DE LA GESTION DES IDENTITÉS

Ce que recouvre la gestion d'identités
La justification du projet gestion
des identités
Le principe du moindre privilège
OID : Object Identifier
UUID : Identité Universelle Unique
Les standards d'identités
Notre identité numérique ne doit
pas nous échapper
L'intrusion des GAFAM
dans notre sphère : BYOID
L'identité souveraine
L'identification unique et la Blockchain

LDAP

Les justifications d'un annuaire unique
Ce qu'est LDAP
Les contraintes d'un annuaire LDAP
L'arborescence LDAP
Désignation des objets
L'arbre DIT
Le modèle d'information
Active Directory : arbres et forêts

SINGLE SIGN-ON

Cookies, sessions et tokens
Pourquoi un SSO : Single Sign-On
Architecture centralisée et
provisionnement central
Architecture décentralisée
Authentification unique dans le Cloud
L'hébergement dans le Cloud d'Active
Directory
Le projet SSO : les étapes
Les précautions à prendre dans le
lancement d'un projet SSO
Les solutions SSO

WEBSO

Principe WebSSO
Le token standard JWT
OAuth 2.0
Les API conformes à OAuth
OpenID Connect
GNAP, la nouvelle génération
Le serveur Radius

FÉDÉRATION D'IDENTITÉS

Les objectifs de la fédération
Les acteurs
WS-Federation
SAML
La technologie Kerberos

IAM : LES INTÉGRÉS DE L'IDENTITÉ

Les liens entre gestion des identités et SSO
Les processus IAM : l'intégré de l'AHA
Les conditions d'une bonne approche IAM
Les indicateurs clés d'un projet IAM
IAM vs IRM
La gestion des identités clients : CIAM
IDaaS : IAM dans le Cloud
Les solutions Open Source de gestion
d'identité

LA BIOMÉTRIE

L'AUTHENTIFICATION DES MOBILES

Les pin d'accès aux mobiles : une
plaisanterie...
L'authentification spécifique des mobiles
L'authentification forte en pleine expansion

LA FIN DES MOTS DE PASSE

Les nouveaux venus de l'authentification
mobile
FIDO 2 (WebAuthn)
Mobile Connect : l'opérateur dans la boucle
Le cheminement vers l'authentification
invisible

L'APPORT DE LA BLOCKCHAIN

Ce que peut apporter la Blockchain
Blockchain et SMI : une perception
terrifiante

AVANT DE SE QUITTER, CE DONT IL FAUDRA SE SOUVENIR