Identités et fédération d'identités

"You'll never walk alone"

23 Juin 2023

claude@lemarson.com
https://www.lemarson.com

Sommaire

La fédération d'identités

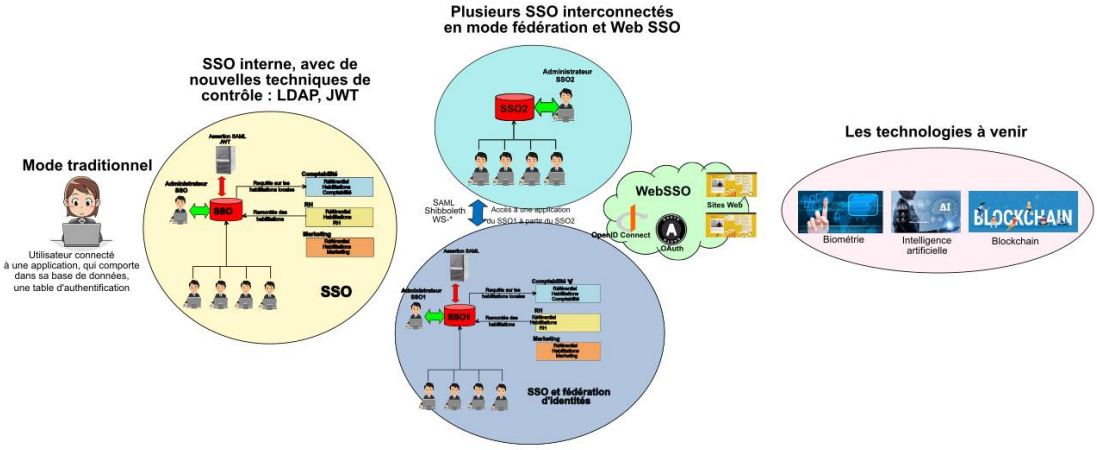
15,93 G$ en 2022 (Grand View Research) et CAGR de 12,6 % jusqu'en 2030 !!!

Le concept d'identité numérique

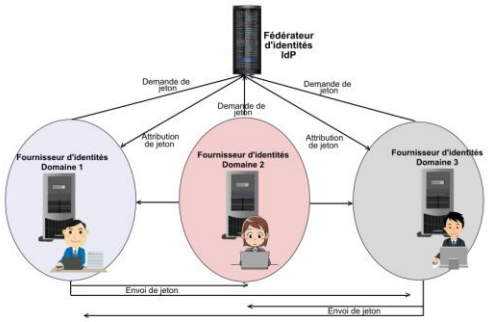
Fait partie du domaine AHA : Autorisations, Habilitations, Accès

- **Entité**
  - Personne physique ou morale (organisation, entreprise), une ressource (matériel informatique) ou un groupe d'entités individuelles.
  - Employé, partenaire, fournisseur susceptible de jouer un rôle dans l'entreprise.
  - Une entité peut posséder plusieurs identités numériques, en fonction de l'environnement.
  - Les « credentials » sont des informations qui peuvent être utilisées pour authentifier une entité.
- **Identité**
  - Ensemble des caractéristiques par lesquelles une entité est connue. Des attributs peuvent être définis comme le nom, état (suspendu, actif…), niveau de confidentialité, l'adresse, la notoriété ou être innés comme les empreintes digitales.
- **Identifiant**
  - Essentiel : va servir de pivot à tout le montage.
  - Information qui permet de distinguer sans ambiguïté une entité d'une autre dans un contexte donné. Peut être un attribut, ou un groupe d'attributs, mais doit rester unique (c'est tout le problème).
  - Une entité peut être représentée par plusieurs identifiants.
  - L'identifiant de référence est un identifiant qui ne change jamais dans un domaine donné
  - L'identifiant unique personnel (IUP) est un identifiant identique pour tous les domaines d'une même entité

La réalité dans et hors entreprise

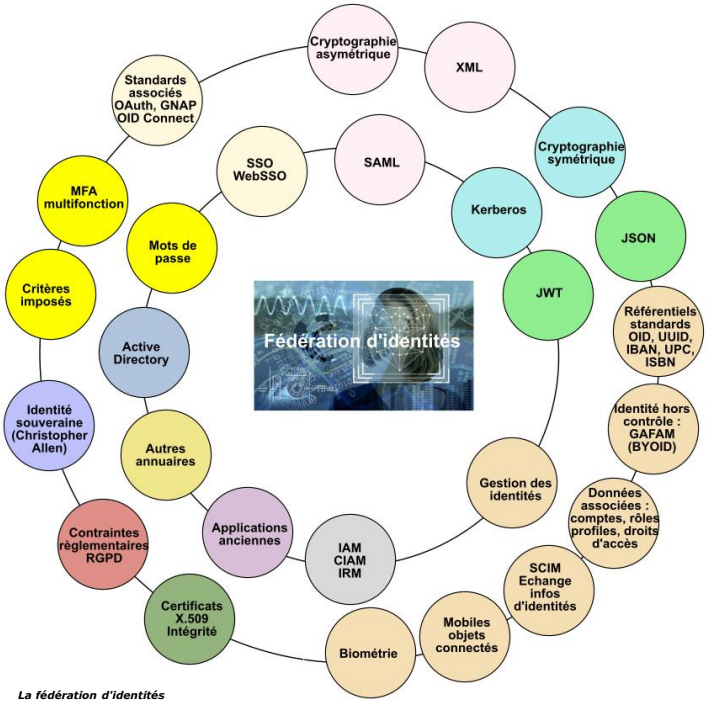


Le principe de la fédération



- La fédération est un mécanisme qui permet à une structure invitante (un système de sécurité, un prestataire indépendant…), de regrouper (inviter) des domaines de sécurité étrangers, de manière à ce que leurs usagers puissent accéder à ses ressources, sans avoir à s'identifier de nouveau.
- Ce moyen d'accès, fourni par un IdP ("Identity Provider") est un jeton, qui a une durée de vie limitée et des droits limités.
- Couche fédératrice placée au-dessus des solutions disparates en place : SSO, LDAP, AD, SAML…
- La fédération peut être interne ou externe.

Le schéma global de la fédération



Les standards d'identités : OID

Facilitent la fédération : les domaines parlent le même langage

- En mode OID (« Object Identifier »), un objet est défini par un nom et une séquence de chiffres séparés par un « . ». C'est une alternative aux mécanismes URI.
- Certaines classes ont fait l'objet d'une normalisation et sont réutilisables.
- Référence universelle qui garantit l'interopérabilité entre différents domaines.
- L'IANA a déjà standardisé un grand nombre d'objets et attributs et on peut obtenir auprès d'elle un OID d'entreprise : une branche de l'arborescence, dans laquelle on pourra décrire nos propres éléments.
- Diversité, on peut décrire toutes sortes d'informations : les pays (2.16.124 pour le Canada, 2.16.250 pour la France ou 2.16.840 pour les USA), des organismes nationaux, des algorithmes de chiffrement (2.16.840.1.101.3.4.1 pour AES mis en œuvre aux Etats-Unis), des algorithmes de hashage tels que SHA-1 (1.3.14.3.2.26), des messages d'alertes (2.49), etc.
- Diversité qui explique la complexité apparente du référentiel.

OID	Fonction
0.9.2342.19200300.100.1.1	uid Attribute Type
0.9.2342.19200300.100.1.3	mailAttribute Type
0.9.2342.19200300.100.1.7	photoAttribute Type
0.9.2342.19200300.100.1.9	host Attribute Type
0.9.2342.19200300.100.1.20	homePhone Attribute Type
0.9.2342.19200300.100.1.41	mobile Attribute Type
0.9.2342.19200300.100.1.60	jpeg Photo Attribute Type
0.9.2342.19200300.100.4.15	dNSDomain Object Class
1.2.840.113549.1.9.1	emailAddress Attribute Type
1.2.840.113549.1.9.7	challengePassword Attribute Type
1.2.840.113549.1.9.25.2	encryptedPrivateKeyInfo Attribute Type
1.3.6.1.1.1.1.22	macAddress Attribute Type
1.3.6.1.1.1.2.6	ipHost Object Class
1.3.6.1.4.1.42.2.27.4.2.4	javaObject Object Class
1.3.6.1.4.1.42.2.27.8.1.6	pwdMinLength Attribute Type
1.3.6.1.4.1.42.2.27.8.1.7	pwdExpireWarning Attribute Type
1.3.6.1.4.1.42.2.27.8.1.11	pwdMaxFailure Attribute Type
1.3.6.1.5.5.7.9.5	countryOfResidence Attribute Type
1.3.18.0.2.4.1135	printer-name Attribute Type
2.5.4.3	cn Attribute Type
2.5.4.10	o Attribute Type
2.5.4.11	ou Attribute Type
2.5.4.15	businessCategory Attribute Type
2.5.4.20	telephoneNumber Attribute Type

Les standards d'identités : UUID

Facilitent la fédération : les domaines parlent le même langage

- Les formats UUID ("Universally unique identifier") sont définis par la RFC 4122 de l'IETF.
- Il existe cinq formalismes distincts UUID, généré par les machines clientes et pas par une autorité centrale.
- Deux grandes familles : UUID aléatoires qui changent à chaque demande ou fixes.
- Le format 1 : UUID aléatoire basé sur des données de date et d'heure et sur l'adresse MAC de la machine qui le génère (12 caractères hexadécimaux).
- Si on génère plusieurs fois l'UUID format 1 à partir de la même machine, les 12 derniers caractères seront donc toujours les mêmes.

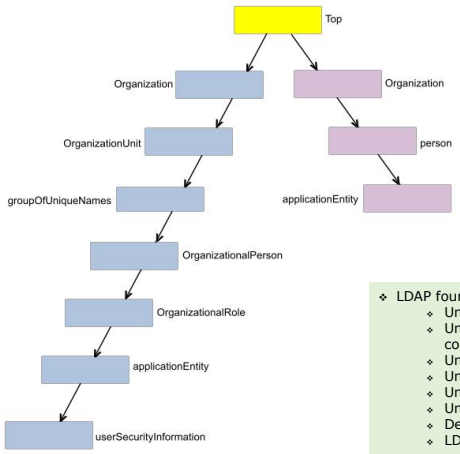
d261fc94-ed01-11ea-abd3-0242acXXXXXX
84d62f66-ed03-11ea-add3-0242acXXXXXX

- Il y a donc un risque de pouvoir retrouver l'adresse MAC, même sans autorisation…
- Le format 4 est le plus utilisé, généré de manière aléatoire.
- Il n'est plus question de date et de nom machine, mais de 128 bits totalement différents, à partir d'une même machine.

01594705-c83e-4b6d-84c0-3c577fadfa15
d414e52b-f429-41d5-b743-96536d7b0750

- La question est de savoir s'il est possible de générer des doublons par cette procédure.
- Le risque est très faible, avec un nombre de combinaisons différentes de 5,3 x 10^{36} : si l'on génère un milliard d'UUID type 4 à chaque seconde, nous aurons une chance sur deux de créer un doublon tous les 100 ans.
- **Les formats 3 et 5 permettent de générer des UUID permanents**.

L’arborescence LDAP

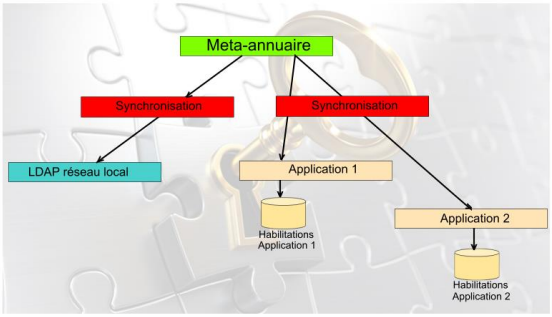


- Une arborescence LDAP décrit la structure hiérarchique des contributeurs au système d’information : individus, machines, applications ou toute autre ressource.
- Chaque contributeur est un objet, résultat de l’instanciation d’une classe d’objets homogène, les objets étant dotés d’attributs qui les décrivent et qui eux-mêmes respectent une typologie claire et non ambiguë.
- Certains attributs sont obligatoires et d’autres sont optionnels, choisis dans une liste standard, la même pour tous les annuaires compatibles LDAP.
- A noter que ces objets sont susceptibles d’hériter d’autres objets, selon une hiérarchie elle-aussi standardisée.

- LDAP fournit un ensemble d'outils :
  - Un protocole permettant d'accéder à l'information contenue dans l'annuaire.
  - Un modèle d'information définissant l'organisation et le type des données contenues dans l'annuaire.
  - Un modèle de nommage qui définit comment l'information est référencée.
  - Un modèle fonctionnel qui définit comment accéder à l'information.
  - Un modèle de sécurité qui définit comment les données sont protégées.
  - Un modèle de duplication qui définit comment la base est répartie entre serveurs.
  - Des APIs pour développer des applications clientes.
  - LDIF, (LDAP Data Interchange Format) un format d'échange de données.

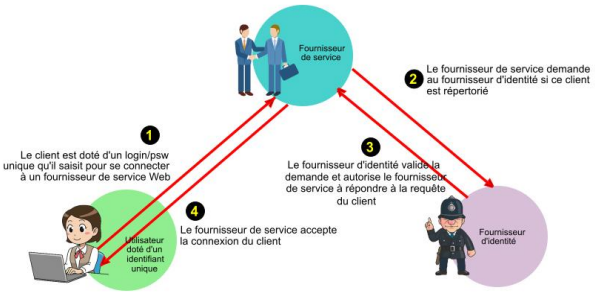
SSO : Single Sign On

- Le SSO regroupe en un point d’accès unique, toutes les informations d’habilitations concernant les usagers ou les moyens pour les obtenir :
  - Un méta-annuaire est mis en place, qui constitue le point d’entrée unique pour toutes les demandes d’habilitations.
  - L’annuaire est à la norme LDAP.
  - Habituellement, la gestion des connexions au réseau local est traitée par Active Directory et celle des applications dans des bases de données liées, maintenues en l’état, le problème étant soit de les faire remonter en temps réel, soit de les laisser « sur place » à charge pour le méta-annuaire de les retrouver quand il en aura besoin.
  - Il y a deux formes de méta-annuaires qui correspondent à ces deux stratégies : centralisé et décentralisé.
  - A chaque connexion, le méta-annuaire recherche si la ressource demandée est autorisée pour le couple login/password demandeur.
  - Si c’est le cas, il la rend disponible sans que l’usager soit obligé de saisir l’habilitation correspondant à la ressource.
- Toutes les synchronisations entre les habilitations locales et le méta-annuaire ne sont pas possibles : quand la base locale n’est pas accessible, par exemple :
  - La synchronisation n’est pas toujours exécutable en temps réel, tout dépend des protections liées.



WebSSO

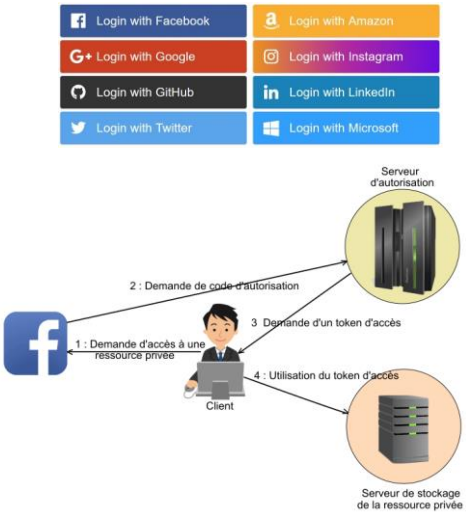
- Une forme particulière du SSO, appliquée à Internet.
- L'objectif est d'éviter que les usagers aient à se souvenir d'une multitude de login/password et n'aient à en retenir qu'un seul.
- Le WebSSO peut s'intégrer dans une architecture SSO d'entreprise, susceptible de traiter la partie externe à l'entreprise.
- De plus en plus de cahiers des charges font état de cette nécessité.
- Les mêmes acteurs que pour une fédération :
  - L'Identity Provider (IdP) ou fournisseur d'identités.
  - Le Service Provider (SP) ou fournisseur de service.
  - Le User Agent (UA) ou agent utilisateur.
- Mais cette fois, on est dans le Web.



Principe du SSO appliqué au Web

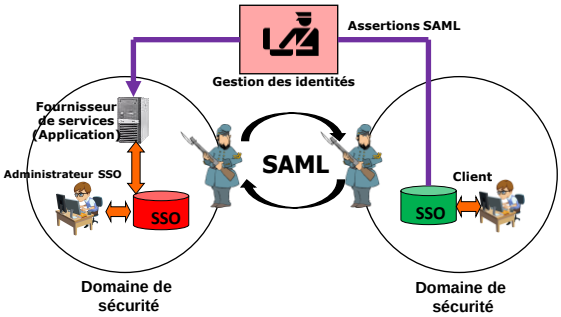
OAuth 2.0

- Oauth traite l'habilitation de droit d'usage, pas l'authentification.
- Il traite le problème de l'**accès par une application à une ressource** : image, « credentials », numéro de compte, etc, hébergée par un serveur de ressources, qui agit pour le compte du propriétaire de la dite ressource.
- OpenID Connect, est une surcouche d'OAuth 2.0, à qui il ajoute l'authentification. Selon les cas, on se contentera d'OAuth combiné avec un protocole au choix ou d'OpenID Connect, qui englobe OAuth. Dans le paysage d'AHA, ces deux protocoles sont désormais incontournables… et indissociables.
- Fondé sur 4 rôles :
  - Resource Owner : détenteur des données.
  - Resource Server : serveur qui héberge les ressources protégées, chargé de répondre aux demandes d'accès qu'il valide par le contrôle des jetons (Access Token).
  - Client : l'application qui demande l'accès aux ressources protégées, qui peut être une application PHP côté serveur ou JavaScript côté client ou mobile.
  - Authorization Server : le serveur qui délivre les jetons d'accès après que le propriétaire des ressources l'ait autorisé à le faire.
- Trois grandes phases :
  - Obtenir un jeton de requête.
  - Obtenir l'autorisation de l'utilisateur.
  - Échanger le jeton de requête contre un jeton d'accès.
- De grandes plates-formes l'utilisent : Twitter, Google +, Facebook.

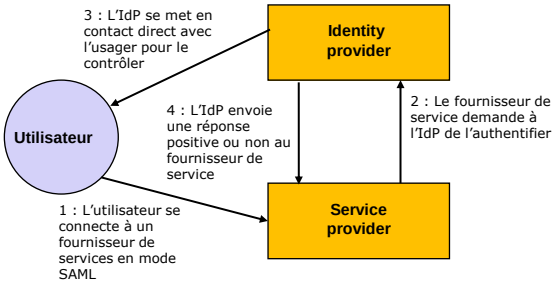


SAML

- Version courante 2.0
- Security Assertion Markup Language.
- Protocole d'échange d'authentifications et d'autorisations entre domaines de sécurité.
- SAML définit un format du message XML, une assertion et des profils.
- Normalisé par l'OASIS Security Services Technical Committee.
- SAML exploite plusieurs standards XML : Schema, Signature, Encryption (uniquement SAML 2.0).
- Deux usages distincts : SSO interne et fédération d'identités avec des partenaires.

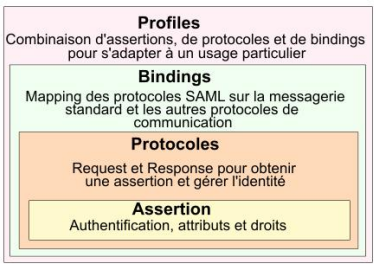


- SAML définit deux briques de base pour sécuriser les échanges :
  - Le **SP (Service Provider)**, fournisseur de service, protège l'accès aux applications. Il refuse tout accès sans authentification préalable.
  - L'**IdP (Identity Provider)**, fournisseur d'identité, s'occupe d'authentifier l'utilisateur ainsi que de récupérer des informations additionnelles associées à son identité.
  - Dans le cadre d'une fédération entre plusieurs domaines d'identifications, SAML définit une troisième brique appelée le **DS (Discovery Service**) qui permet à l'utilisateur de sélectionner manuellement son domaine dans une liste.



L'architecture SAML

- Une spécification SAML est constituée de 4 éléments :
  - Assertions
  - Protocoles
  - Bindings
  - Profiles
- Trois types d'assertions :
  - Assertion d'authentification
  - Assertion d'attributs
  - Assertions de décision d'autorisation



Exemple d'assertion SAML

```
<saml:Assertion
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      ID="XXXXX"
      Version="2.0"
      IssueInstant="XXXXX"
      <saml:Issuer>https://idp.example.org/SAML2</saml:Issuer"
      <ds:Signature
            xmlns:ds:="http://www.w3.org/2000/09/xmldsig#">
            ...
      </ds:Signature>
      <saml:Subject>
            <saml:NameID>
            Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">
            XXXXX
      </saml:Subject>
      <saml:SubjectConfirmation
            Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
            <saml:SubjectConfirmationData
                  InResponseTo="XXXXX"
                  Recipient="https://sp.example.com/SAML2/SSO/POST"
                  NotOnOrAfter"XXXXX"/>
       </saml:SubjectConfirmation
       </saml:Subject
       <saml:Conditions
            NotBefore="XXXXX"
            NotOnOrAfter="XXXXX"
            <saml:AudienceRestriction>
                  <saml:Audience>https://sp.example.com/SAML2</saml:Audience>
            </saml:AudienceRestriction
       </saml:Conditions
       <saml:AuthnStatement
            AuthnInstant="XXXXX"
            SessionIndex="XXXXX">
       <saml:AuthnContext>
            <saml:AuthnContextClassRef>
                  urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
            </saml:AuthnContextClassRef>
       </saml:AuthnContext
       </saml:AuthnStatement>
       <saml:AttributeStatement>
            <saml:Attribute
            xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
            x500:Encoding="LDAP"
            NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
            Name="urn.oid:1.3.6.1.4.1.5923.1.1.1.1"
            FriendlyName="eduPersonAffiliation">
            <saml:AttributeValue
                  xsi:type="xs:string">member</saml:AttributeValue>
            <saml:AttributeValue
                  xsi:type="xs:string">staff</saml:AttributeValue>
            </saml:Attribute
      </saml:AttributeStatement>
</saml:Assertion
```

ns pour namespaces (espaces de noms)
Où trouver la description des tags XML des grammaires assertion, XMLSchema et XMLSchema-instance

identifiant de l'assertion

Heure d'émission de l'assertion

identifiant dde l'IdP (fournisseur d'identité)

Signature électronique qui porte sur l'assertion

Le sujet décrit l'authentifié principal, caché ici derrière un identifiant transitoire pour des questions de sécurité

L'élément conditions précise les conditions pour lesquelles l'assertion sera considérée comme valide

L'élément AuthStatement décrit l'action d'authentification au niveau de l'IDP

L'assertion "XXXXX" a été émise à "XXXX" par le fournisseur d'identités https://idp.example.org/SAML2 concernant le sujet "XXXXX" spécifiquement pour le fournisseur de service https://sp.example.com/SAML2

L'élément AttributStatement décrit un ensemble d'attributs affectés à l'authentifié principal

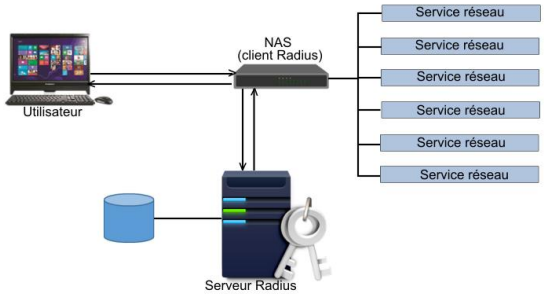
Expliquer le succès de SAML

- La neutralité de la plateforme
  - SAML offre un cadre de sécurité indépendant de la plate-forme technique qui l'utilise.
  - Valable pour la partie SP (application) et IdP.
- Une nouvelle expérience utilisateur
  - Une solution SSO basée sur un protocole standard qui affranchit de la gestion des mots de passe, pour donner accès aux applications, potentiellement chez de nombreux SP (dans le Cloud entre autre), évite à le stress et améliore l'efficacité des usagers.
- Une réduction de la complexité pour le Service Provider
  - Le SP se contente d'émettre une demande vers un IdP, soit hébergé par le client lui-même, soit par un tiers de confiance assurant la fédération d'identité. Le SP est donc déchargé de la fastidieuse phase d'authentification pour se limiter au service.
  - Le SP peut réutiliser l'authentification stockée dans un cookie autant de fois que nécessaire.
- La sécurité y gagne
  - Tout se passe par l'intermédiaire du navigateur au cours d'une même session sans que le SP ne fasse de requête entrante sur le réseau du client. Il n'est donc plus besoin d'ouvrir des ports sur les FW, seul le flux HTTP est impliqué et surveillé.

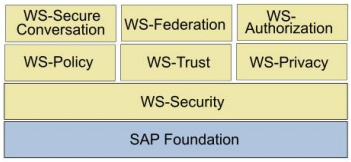
Des technologies anciennes mais présentes

Le serveur Radius

- Le protocole RADIUS (Remote Authentication Dial-In User Service).
- Orienté accès aux services réseaux : routeurs, concentrateurs VPN, switchs.
- Fonctionne en mode client/serveur pour les postes locaux et mobiles.
- Fondé sur un serveur, relié à une base d'identification (base de données, LDAP) et un client RADIUS, le NAS (Network Access Server), qui est l'intermédiaire entre le serveur et les clients



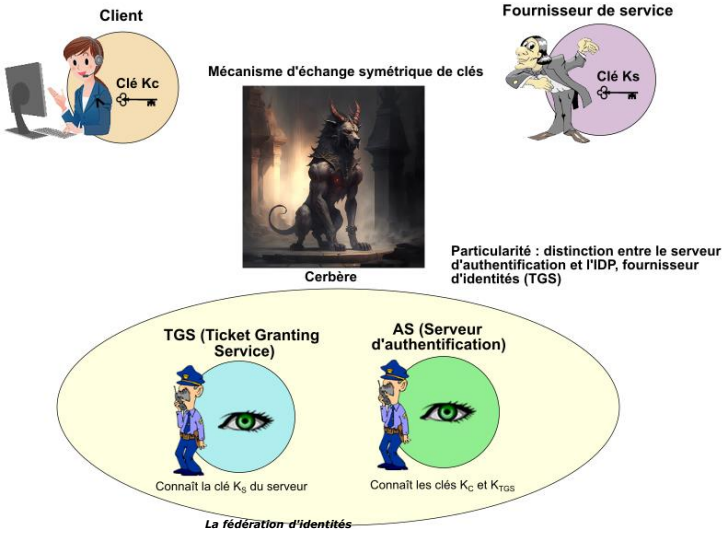
WS-Federation



- WS-Federation ou « Web Services Federation Language », ou « WS-Fed » est une spécification qui définit des mécanismes de fédération d'espaces de confiance hétérogènes.
  - Origine BEA (Oracle), BMC Software, CA, IBM, Layer 7 Technologies, Microsoft, Novell (Attachmate) et Verisign, ancienne mais encore présente.
  - WS-Federation est une extension de WS-Trust.
  - S'appuie sur les spécifications WS-Security, WS-Policy et WS-SecureConversation.
  - Concrètement, WS-Federation permet d'effectuer l'authentification mutuelle d'applications utilisant des approches de sécurité hétérogènes, comme par exemple les mécanismes d'authentification Kerberos et X.509.
  - WS-Federation agit comme une couche entre WS-Policy et WS-Trust pour indiquer comment les relations de confiance doivent être gérées.

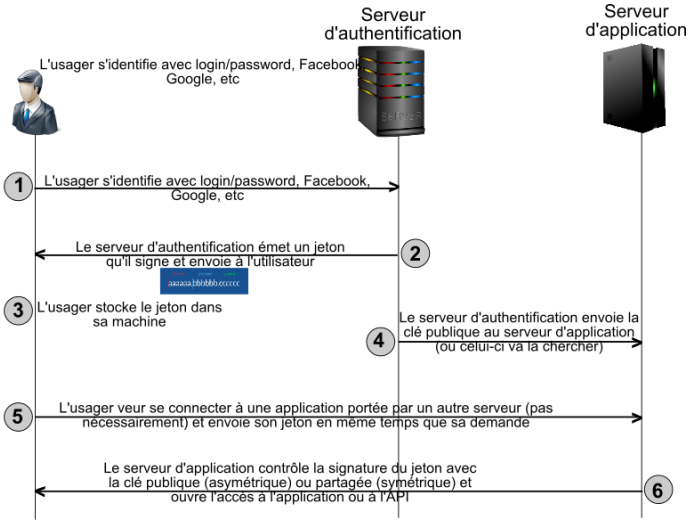
La technologie Kerberos

- Créé au MIT (du grec Cerbère, le gardien).
- Fondé sur des échanges de clés secrètes en mode symétrique : la même clé sert au chiffrement et au déchiffrement.
- Ce que l'on gagne en vitesse d'exécution, on le perd en robustesse et imperméabilité.



Montée en puissance de JWT

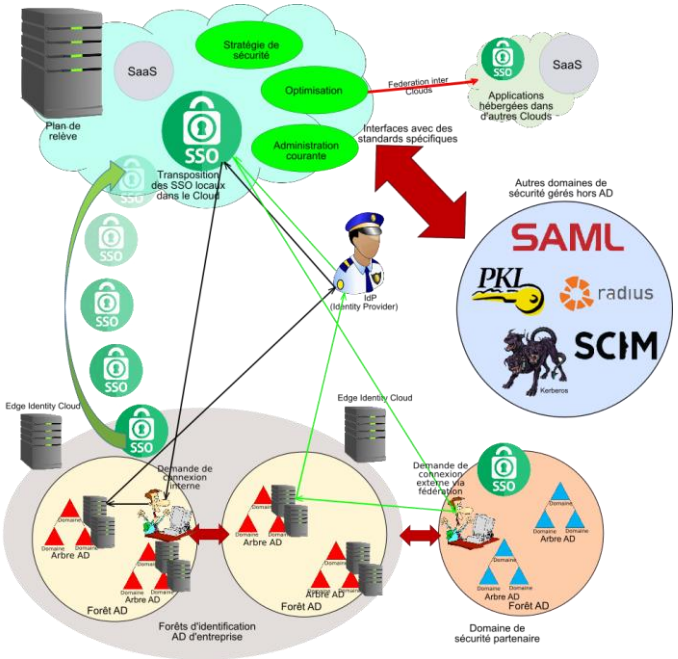
Une alternative à SAML

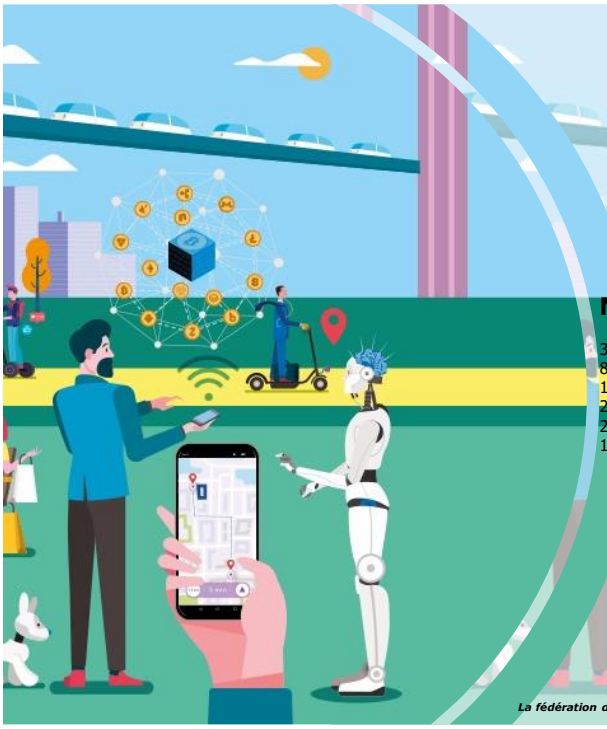


- JWT est une déclinaison JSON qui répond au besoin d'authentification d'un client Web, connecté à un site Internet ou à une application interne.
- La mécanique JWT est organisée en 3 phases : l'identification du client via identifiant / mot de passe, la génération d'un token par le serveur d'authentification et l'envoi pour chaque requête HTTP du contenu de ce token à l'application.
- Nombreux avantages par rapport aux autres solutions (SAML…), essentiellement pour sa simplicité de mise en œuvre et sa sécurité. C'est le candidat idéal pour développer une problématique d'authentification sans état :
  - Il encapsule toutes les données nécessaires.
  - Il comporte une date de péremption et un identifiant unique, valable le temps de la session.
  - On ne peut modifier son contenu et n'importe quelle application est « a priori » éligible pour contrôler l'authentification.
  - JWT est destiné aux développeurs dans les entreprises, mais de nombreux produits et protocoles sont fondés dessus

La fédération dans le Cloud : AD

- L'annuaire de fédération doit gérer des espaces de sécurité non AD. La plupart du temps le réseau local reste AD, mais une solution non Microsoft est parfois installée au-dessus, AD n'étant alors qu'un annuaire LDAP parmi d'autres.
- Trois cas de figure.
  - Le rôle de super-annuaire est confié à Microsoft qui s'est rendu compatible via AD avec de nombreuses solutions AHA spécifiques, dont certaines sont portées par le Cloud : AuthAnvil, CA Secure Cloud, Centrify, Dell One Identity Cloud Access Manager, IBM Tivoli, NetIQ Access Manager, Okta (Cloud), PingFederate, Radian, SecureAuth IdP, SailPoint Identity,VMWare Workspace One, etc.
  - Soit on choisit un autre fédérateur, un Tivoli ou un Radian par exemple.
  - Certaines de ces solutions sur le Cloud sont très séduisantes, en termes de fonctionnalités, de simplicité d'administration et d'ouverture aux standards. Mais on fera les mêmes remarques à leur sujet : risque de dépendance vis-à-vis d'un fournisseur unique, qui n'aura pas nécessairement la même « carrure » rassurante que Microsoft.
  - La troisième possibilité, suicidaire, voudrait que l'on développe soi-même la fédération, en prenant à notre charge les interfaces avec les ressources existantes.





Identités et fédération d'identités

23 Juin 2023

Nos prochains webinaires

30 Juin 2023 :	**Les grandes figures du TI... dont on parle moins**
8 Septembre 2023 :	**Les grandes utopies du TI : capitaliser sur nos erreurs**
15 Septembre 2023 :	**Backup et restauration des datacenters**
22 Septembre 2023 :	**Productivité, il n'y a pas qu'Office. Ah, bon...**
24 Novembre 2023 :	**Les transports du futur : verts et sans pilotes**
15 Décembre 2023 :	**L'hyperautomatisation : les temps modernes du TI**

claude@lemarson.com
https://www.lemarson.com