L'authentification

L’authentification est une procédure, par laquelle un système informatique certifie l’identité d’une personne ou d’un ordinateur. Le but de cette procédure étant **d’autoriser** la personne à accéder à certaines ressources sécurisées. Il va comparer les informations des utilisateurs autorisés stockées dans une base de données (en local ou sur un serveur d’authentification) à celles fournies. L’accès sera autorisé seulement si les informations sont identiques. C’est l’administrateur du système d’information qui octroie les droits et paramètre l’accès. L’utilisateur possédant un compte d’accès (identifiant + mot de passe) n’aura accès qu’aux ressources dont il est autorisé à voir.

L'authentification par mot de passe

En sécurité informatique, **une authentification simple** est une procédure d'authentification qui ne requiert qu’un seul facteur d'authentification comme un mot de passe.

Malgré l'existence de dispositif matériels d'authentification, l'authentification par mot de passe reste la technique la plus répandue dans les systèmes informatiques. Sa prolifération a même donné lieu à la création d'un marché pour des produits de gestion des différents mots de passe dont un utilisateur peut être détenteur, et qu'il n'arrive plus à mémoriser seul. Cette technique sépare l’identifiant : le nom d’utilisateur fourni de manière déclarative ; et l’authentifiant : un mot de passe secret.

Les bonnes pratiques consistent à utiliser des mots de passes différents et pour tous ses comptes. De cette manière, en cas de compromission d'un mot de passe, les autres comptes ne seront pas compromis.

Pour permettre alors la gestion de ces multiples mots de passe, tâche pas très aisée, l’utilisateur peut utiliser un gestionnaire de mots de passe intégré à son OS comme le **trousseau** ICloud des OS Apple ou bien des logiciels qui permettent de se constituer une base de données de mots de passe chiffrée par un unique mot de passe maître dont la sécurité a pu être vérifiée. Cela permet alors de ne retenir qu’un seul mot de passe pour accéder à tous les autres. Les mots de passe peuvent alors être très longs, très complexes et surtout tous différents car c’est votre gestionnaire de mots de passe qui va les retenir à votre place.

Il existe plusieurs solutions de gestionnaire de mots de passe comme la solution Keepass, dont la sécurité a été évaluée par l’Agence nationale de sécurité des systèmes d’information (ANSSI).

Les recommandations de l’ANSII sur les mots de passe : https://www.cert.ssi.gouv.fr/information/CERTA-2005-INF-001/

Les conseils de la CNIL pour choisir un bon mot de passe : https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe

La fédération d'identité

La gestion des identités, qui doit être un moyen efficace, gérable, auditable et sécurisé de fournir aux utilisateurs ou processus l'accès aux ressources de l'entreprise implique une charge d'administration et de support considérable pour chaque identité gérée. La fédération tente de limiter cette charge et d'améliorer la convivialité pour les utilisateurs en limitant le nombre de gestionnaires pour une identité donnée. Moins une identité spécifique compte de gestionnaires, plus le système tout entier sera efficace ; plus le nombre de systèmes auxquels les utilisateurs peuvent accéder sans s'authentifier de nouveau est élevé, plus la convivialité est grande pour eux.

La fédération agit comme un **mécanisme périphérique** qui se situe en bordure du réseau et partage les informations d'identité avec d'autres mécanismes de fédération avec lesquels il existe une **relation de confiance**. La technologie de fédération s'appuie sur la confiance accordée aux pratiques d'authentification, d'administration et de confirmation d'identité d'une entité membre, pour certifier que les utilisateurs ou services d'applications peuvent accéder à une ressource externe, et vice versa.

Les objectifs de la fédération sont de **d'améliorer la convivialité pour les utilisateurs (un seul compte pour accéder à de multiples services)** et minimiser les coûts et la charge de gestion des identités. Les besoins d'échanges numériques à l'intérieur et entre organisations, a entraîné une **multiplication des "îlots d'identités"**, c'est-à-dire des fournisseurs d'applications externes qui gèrent les identités dans des plates-formes distinctes des systèmes de gestion des identités des entreprises. De nombreuses entreprises considèrent cette pratique risquée et souhaitent gérer ses risques via une relation de confiance avec un partenaire ou un tiers.

La fédération d'identités offre un moyen d'atteindre cet objectif en se basant sur des **standards**, permettant à un **fournisseur d'identités de transmettre des informations** sur une identité gérée à un **fournisseur de ressources** ou prestataire de services (également appelé partie utilisatrice). Chaque entité de la communauté de confiance ainsi créée effectue le suivi des identités des individus particulièrement importants (par exemple, les employés et les contacts proches), et les individus authentifiés par leurs propres entités peuvent accéder aux ressources des autres entités sans devoir s'authentifier plusieurs fois.

Les organisations doivent alors gérer le risque dans la relation de confiance entre le fournisseur d'identités et le consommateur d'identités.

Une composante importante de la fédération d'identité est le **Single Sign-on (SSO)**, un mécanisme qui permet aux utilisateurs de ne s'authentifier qu'une fois pour accéder à plusieurs systèmes ou applications. La fédération d'identité et le SSO sont parfois, et par erreur, appréhendés comme un seul et même système. La fédération d'identité s'appuie fortement sur les technologies SSO pour authentifier les utilisateurs à travers les divers domaines couverts.

Principe de fonctionnement :

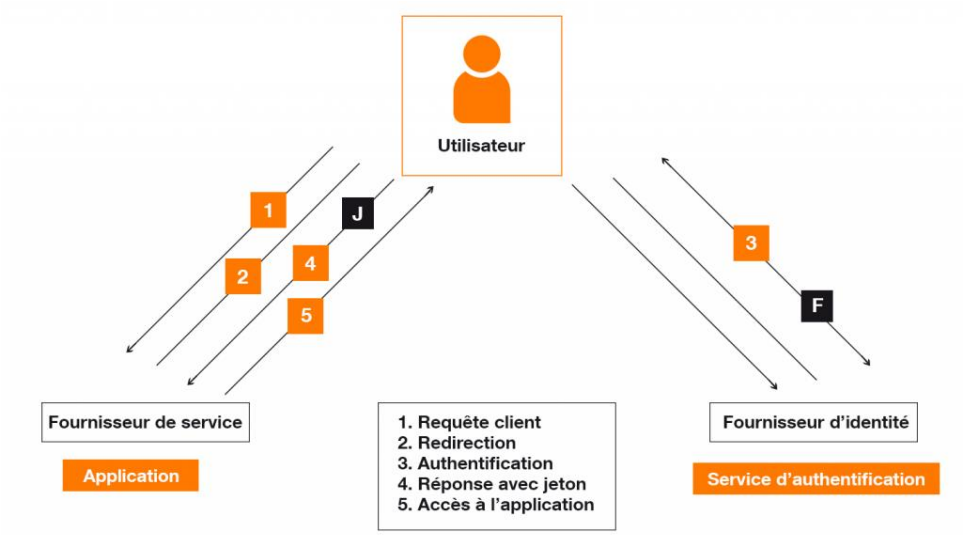
Dans un schéma en fédération d'identités, il y a trois acteurs :

- **L'utilisateur** : il s'agît de la personne qui interagit via son navigateur web. Il a une unique identité numérique associée à plusieurs attributs et souhaite accéder à une application protégée.
- Le **fournisseur d'identité** : il est l'élément central de l'architecture. Il est chargé d'authentifier les utilisateurs. Il vérifie les facteurs d'authentification de l'utilisateur et fournit la preuve de son identité. Il est aussi en charge des autorisations d'accès aux attributs. On parle également **d'Identity Provider – IdP.**
- Le **fournisseur de service** : il s'assure de l'identité de l'utilisateur et peut avoir besoin des attributs de l'utilisateur. On parle également **de Service Provider – SP**.

Les flux :

Ces différents acteurs interagissent entre eux pour, in fine, autoriser l'accès à l'utilisateur. Requête client, réponse avec jeton… Voici les étapes clés :

1. **Requête client** : l'utilisateur demande l'accès à un service protégé par une authentification
2. **Redirection** : le fournisseur de service redirige l'utilisateur vers le fournisseur d'identité pour qu'il puisse s'authentifier ;
3. **Authentification** : l'utilisateur s'authentifie (il justifie de son identité) à l'aide des facteurs d'authentification compatibles avec la méthode en place (login/mot de passe, clé, OTP …) ;
4. **Réponse avec jeton** : le fournisseur d'identité redirige l'utilisateur vers le fournisseur de service accompagné du jeton attestant de son identité ;
5. **Accès à l'application** : le fournisseur de service évalue le jeton et autorise l'accès de l'utilisateur.



Sources :

- https://www.egilia.com/fr/articles/20976-la-federation-identites-single-sign-on-le-serpent-mer-la-decennie.html
- https://cyberdefense.orange.com/fr/blog/la-federation-didentite/

Exemple de mise en œuvre de la fédération d'identités :

Shibboleth :

C'est une solution de fédération d'identités développée par le consortium Internet2, qui regroupe 207 universités et centres de recherches. Cette fédération vise à regrouper des universités,

commissions scolaires et autres organismes publics qui auraient comme rôle de définir et normaliser les attributs d'authentification et aussi de s'assurer que les membres respectent des standards rigoureux en matière d'authentification.

La délégation de l'authentification réutilise les techniques de **Single Sign-On web** (redirection, cookies…). Lors de l'accès initial à une ressource numérique, l'utilisateur est redirigé vers le service de découverte de la fédération, d'où il sélectionne son établissement d'origine ; il est ensuite renvoyé vers son fournisseur d'identités. Le prérequis pour le fournisseur d'identités est de disposer d'un service d'authentification global tel que **Central Authentication Service (CAS)** (pas forcément d'un SSO).

Les solutions proposées les géants du Web :

Google, Microsoft, Facebook, Tweeter propose également ces mécanismes de fédération d'identités pour :

- Permettre aux particuliers de s'authentifier sur des sites partenaires avec leur compte Google, Microsoft, Facebook ou Tweeter,
- Pour l'accès des professionnels à leurs services dans le Cloud.

Exemple : Google utilise la norme de la fédération d'identité **SAML** (Security Assertion Markup Language) pour permettre l'échange en toute sécurité de données d'authentification utilisateur entre les applications de ses services Cloud. Cette authentification unique (SSO) permet aux utilisateurs de se connecter à toutes les applications cloud de leur entreprise à l'aide des identifiants de leur compte Google géré. Google propose ainsi une authentification unique pré-intégrée pour plus de 200 applications cloud courantes.

Pour en savoir plus : https://support.google.com/a/topic/7417510

Une initiative française **: FranceConnect**

FranceConnect est un dispositif permettant de garantir l'identité d'un utilisateur pour l'accès à des services publics en s'appuyant sur des comptes existants pour lesquels son identité a déjà été vérifiée. Ce dispositif est un bien commun mis à la disposition de toutes les autorités administratives. Il est mis en œuvre par la **DINSIC**, un service du premier ministre. Certains acteurs du secteur privé peuvent aussi en bénéficier s'ils contribuent à l'action publique(banques et assurances par exemple).

Cette authentification permet actuellement l'accès à la plusieurs services publics : impôts, cartes grises, retraite, etc.

La poste permet à toute personne qui le souhaite, de se créer une identité numérique reconnue par France Connect

Site de l'identité numérique de La poste : https://lidentitenumerique.laposte.fr/

Site de FranceConnect : https://franceconnect.gouv.fr/

L'authentification avec un objet physique

Le principe de l'**authentification forte** est d'utiliser plusieurs facteurs de nature distincte afin de rendre la tâche plus compliquée à un éventuel attaquant. Les facteurs d'authentification sont classiquement présentés comme suit :

- Ce que l'entité connaît (un mot de passe, un code NIP, une phrase secrète, etc.).

- Ce que l'entité détient (une carte magnétique, RFID, une clé USB, un PDA, une carte à puce, un smartphone, etc.). Soit un élément physique appelé jeton d'authentification, authentifieur ou token.

L'authentification biométrique

L'authentification biométrique fait appel aux caractéristiques biologiques uniques d'un individu pour vérifier son identité et garantir son accès sécurisé à un système électronique.

Les technologies biométriques en jeu s'appuient sur la façon dont chaque individu peut être identifié de manière unique grâce à une ou plusieurs caractéristiques biologiques, telles que l'empreinte digitale, la morphologie de la main ou du lobe de l'oreille, la physionomie de la rétine et de l'iris, les ondes vocales, la dynamique de la frappe au clavier, l'ADN ou les signatures.

L'authentification biométrique est l'application de ces preuves d'identité dans le cadre d'un processus de validation d'un utilisateur souhaitant accéder à un système.

Les technologies biométriques sont utilisées pour sécuriser un large éventail de communications électroniques, qu'il s'agisse d'une entreprise, d'un site de commerce électronique ou d'une banque en ligne, ou simplement pour se connecter à un ordinateur ou à un smartphone.

Les systèmes d'authentification biométrique comparent les données biométriques fournies aux données authentiques confirmées d'une base de données. Si les deux échantillons concordent, l'authentification est confirmée et l'accès accordé. Ce processus s'intègre parfois à un système d'authentification multi facteur. Ainsi, l'utilisateur d'un smartphone peut se connecter à l'aide de son code secret (PIN) et y ajouter un scan de l'iris.