



Le service d'authentification multi-facteur

TODO

Le service d'authentification U2F

Le service d'authentification à double facteur U2F est basé sur la possession d'un objet se connectant sur un port USB : le token U2F. Celui-ci, tel qu'acheté par le service IRTS, peut se présenter sous deux versions :

La Yubikey 4	 A black USB token with a yellow Yubikey logo and a 'fido U2F CERTIFIED' badge.
Le Yubikey Nano (pour un encombrement minimum)	 A small, gold-colored USB token with a 'fido U2F CERTIFIED' badge.

1. Le principe

CAS (Central Authentication Service) est un SSO (Signle Sign On) web permettant d'unifier l'authentification des utilisateurs du système d'information. Historiquement, il reposait uniquement sur les mots passe d'un annuaire LDAP. Depuis 2011, le service est assuré par un cluster de 4 serveurs assurant une haute disponibilité, un seul des quatre étant suffisant pour rendre le service.

La fragilité de l'authentification basée sur le seul mot de passe LDAP est reconnue depuis longtemps. Les risques de compromission sont principalement liés à l'ingénierie sociale, notamment le phishing consistant à envoyer massivement un message consistant à faire croire que la DSIN exige de connaître le mot de passe de l'utilisateur, sous peine de bloquer le compte dans un délai court, ce qui déclenche panique et comportements irrationnels. Mais aussi : "keyloggers" matériels ou logiciels, intrusion sur les serveurs, "sniffers" réseau, etc. Cette technique ne suffit plus.

En pratique, l'utilisateur peut s'authentifier selon 3 différents facteurs :

- ce qu'il sait : un mot de passe ;
- ce qu'il possède : un objet matériel ;
- ce qu'il est : biométrie.

Utiliser de manière complémentaire plusieurs facteurs est une technique nommée MFA : Multi Factor Authentication. Elle permet d'atténuer les risques de vol d'identifiants en compensant les inconvénients d'un facteur par les avantages d'un autre.

Le facteur supplémentaire proposé ici est basée sur une clé USB spéciale (ce n'est pas une clé ordinaire destinée à stocker un système de fichiers) : le standard FIDO U2F. Historiquement, le fabricant est Yubico, mais il existe maintenant des produits compatibles, moins chers. Le fait de posséder cette clé, attribuée d'une manière statique à un utilisateur, permet, en association avec le mot de passe, d'affirmer que le compte informatique en cours d'utilisation est celui de cette personne.

De plus, on gère un autre type d'authentification basée sur un objet matériel, cette fois-ci le téléphone portable : **OTP** (One Time Password). Il s'agit d'une application libre et gratuite, Free OTP, disponible pour Android et IOS, permettant de calculer le hash cryptographique d'une graine stockée dans le téléphone, celle-ci étant couplée au temps (nombre de minutes depuis *The Epoch*). Le téléphone et le service d'authentification calculent indépendamment cette valeur de hash, et les deux versions doivent correspondre. Ceci revient à utiliser un mot de passe qui change à chaque minute. Cette technique est plus contraignante que U2F, car il faut démarrer l'application sur son téléphone et saisir un code à 6 chiffres en plus du mot de passe, mais elle reste utilisable quel que soient le navigateur et le système d'exploitation de l'ordinateur sur lequel on effectue d'authentification.

Il n'est pour autant pas question d'abandonner les mots de passe, mais de les conserver d'une manière complémentaire, en gardant à l'esprit que cette clé peut être perdue ou volée, surtout si l'utilisateur la laisse branchée à demeure (déconseillé).

La sécurité d'U2F est basée sur la cryptographie asymétrique : une paire clé privée - clé publique est stockée dans la clé. La première ne sort jamais de la clé et sert à chiffrer un "challenge" (chaîne de hexadécimale aléatoire), tandis que la seconde est fournie au navigateur afin de procéder à la vérification. De la sorte, il est impossible de copier une clé U2F sur une autre.

Le standard FIDO U2F est supporté par Facebook et Google. Il est en production sur notre service UNCloud (NextCloud), avec son propre système d'enregistrement et d'authentification indépendant de CAS. Au moment d'écrire ces lignes, Firefox et Chrome sont les deux navigateurs qui supportent la technologie FIDO U2F, aussi bien sous Windows que Linux, contrairement à Internet Explorer et Edge.

2. Installation de la clé

2.1 Préparation

- Sous Firefox : le protocole U2F est nativement supporté mais inactif par défaut. Pour l'activer, tapez **about:config** (dans la barre d'URL) et positionner la clé de registre **security.webauth.u2f** à **true**
- Sous Chrome : normalement, aucune action n'est requise ; cependant, certaines versions nécessitent l'installation du plugin FIDO U2F.

Spécificités Clients Linux

Normalement, celle-ci est vue comme un clavier et aucune action particulière n'est à faire pour qu'elle fonctionne. Cependant, avec certaines clés et certaines versions d'Ubuntu, il est possible qu'une action soit nécessaire sur le système. Voir la page suivante :

<https://support.yubico.com/support/solutions/articles/15000006449-using-your-u2f-yubikey-with-linux>.

NB : contrairement à ce que dit cette page, inutile de redémarrer : il suffit de taper cette commande sous root : `udevadm control -reload-rules`

2.2 Enregistrement de la clé

Pour un fonctionnement avec CAS (le nouveau CAS V5 uniquement), il est nécessaire que la clé soit connue dans l'annuaire ldapauth. Pour cela, l'enregistrement est à effectuer avec le service MonCompte :

- Aller avec un navigateur sur <https://moncompte.univ-nantes.fr>
- S'authentifier
- Sécurité → clés U2F.
- Donner un nom à sa clé - il est possible de déclarer autant de clés que l'on désire. Puis cliquer sur le bouton "valider"
- Normalement, le voyant de la clé clignote. Appuyer sur le bouton.
- La clé est enregistrée.

Les correspondants informatiques peuvent vérifier dans Dyna l'enregistrement des clés, et les supprimer en cas de perte ou de compromission.

Il est important de supprimer dans Dyna les clés perdues ou compromises, la possession de cet objet, en combinaison avec le mot de passe, permettant l'usurpation d'identité informatique.

Il est recommandé, en même temps, de mettre en place l'authentification **OTP** qui servira en secours.

Dans Dyna, un correspondant informatique peut également imposer MFA (U2F ou OTP) à un compte considéré comme "particulièrement sensible".

3. Utilisation au quotidien

Une fois que le compte est déclaré comme utilisant U2F, l'usage de cette clé est obligatoire pour toute authentification CAS. Ceci est détecté dès que l'identifiant unique de l'utilisateur, saisi dans la mire d'authentification, correspond à un utilisateur U2F. Le voyant lumineux de la clé clignote tandis que le message s'affiche :



Appuyer sur le bouton sans oublier de saisir également le mot de passe : les deux sont requis. Normalement le clignotement cesse aussitôt que l'authentification est réalisée.

Pour les utilisateurs qui, comme moi, sont distraits et oublient à l'occasion leur clé U2F à la maison, si l'authentification **OTP** a été activée, il est possible de s'en servir en dépannage. Cliquer sur le lien "autre mode d'authentification", et saisir le code à 6 chiffres indiqué par l'application FreeOTP du téléphone portable.

Le service d'authentification OTP

TODO

From:
<https://wiki.univ-nantes.fr/> - Wiki

Permanent link:
<https://wiki.univ-nantes.fr/doku.php?id=personnels:securite:authmultifacteur&rev=1537447353>

Last update: **2018/09/20 14:42**

