Le service d'authentification multi-facteur

1. Principe

CAS (Central Authentication Service) est un SSO (Signle Sign On) web permettant d'unifier l'authentification des utilisateurs du système d'information.

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'ingénérie sociale, notamment le phishing consistant à envoyer massivement un message consistant à faire croire que la DSIN exige de connaitre 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 but de ce document est de présenter l'authentification à deux facteurs, dont le mot de passe classique PLUS une information supplémentaire de contrôle, l'OTP.

Le service d'authentification OTP

1. Principe

L'idée est ici d'utiliser comme deuxieme facteur d'authentification un objet dont l'utilisateur ne se sépare en général jamais : son téléphone portable.

Celui-ci possède un secret qui est initialisé une fois pour toutes, et qui n'est ensuite jamais communiqué par l'utilisateur, même d'une manière chiffrée. Ce secret s'appelle la graine OTP (One Time Password) ; il est stocké dans l'annuaire LDAP dans un attribut secret.

Cette technique peut prendre deux formes : TOTP et HOTP. Nous avons choisie la première, basée sur le temps, la seconde présentant la contrainte que le dispositif de calcul (le téléphone) soit unique pour un utilisateur donné, avec un risque de désynchronisation. L'information d'authentification, qui est concaténée au mot de passe traditionnel, est une empreinte cryptographique de la graine OTP et du temps : le nombre de minutes entre *the epoq* (le 01/01/1970, 0 heure) et l'instant présent. De la sorte, tout se passe comme si on disposait d'un mot de passe qui change à chaque minute, le suivant étant impossible à déduire du précédent. Il n'est pas indispensable que le téléphone soit connecté au

réseau au moment de l'authentification, mais il est par contre nécessaire qu'il soit rigoureusement à l'heure.

2. Installation

Il faut d'abord installer l'application FreeOTP (FreeOTP Authenticator de RedHat ou FreeOTP+ de Haowen Ning) sur son téléphone portable, sous Androïd ou iOS. Google Authenticator fonctionne également.

Les service MonCompte est chargé de l'enregistrement des graines OTP.

- Se connecter sur https://moncompte.univ-nantes.fr
- S'authentifier
- Aller dans le menu Sécurité → authentification double facteur OTP
- Scanner le QR-code avec l'application Free OTP
- Activer OTP

A partir de ce moment, l'authentification OTP sera obligatoire pour cet utilisateur.

Dans Dyna, un correspondant informatique peut voir si un compte est configuré pour l'OTP. Il peut également interdire que l'OTP soit désactivé.

3. Utilisation pratique

Lorsque l'utilisateur saisit son identifiant unique (login) sur la mire d'authentification CAS, celui-ci détecte grâce à l'annuaire ldapauth qu'il s'agit d'un compte pour lequel OTP a été configuré.

> Si OTP et U2F sont positionnés sur le même compte, le second, plus pratique à utiliser, sera pris en compte en priorité, avec possibilité de secours avec OTP, au cas où le token U2F aurait été oublié.

Indiquer les 6 chiffres affichés par l'application FreeOTP. L'utilisateur dispose d'une minute ; après cela, le code changera automatiquement.