VII. Notre solution technique 2FA

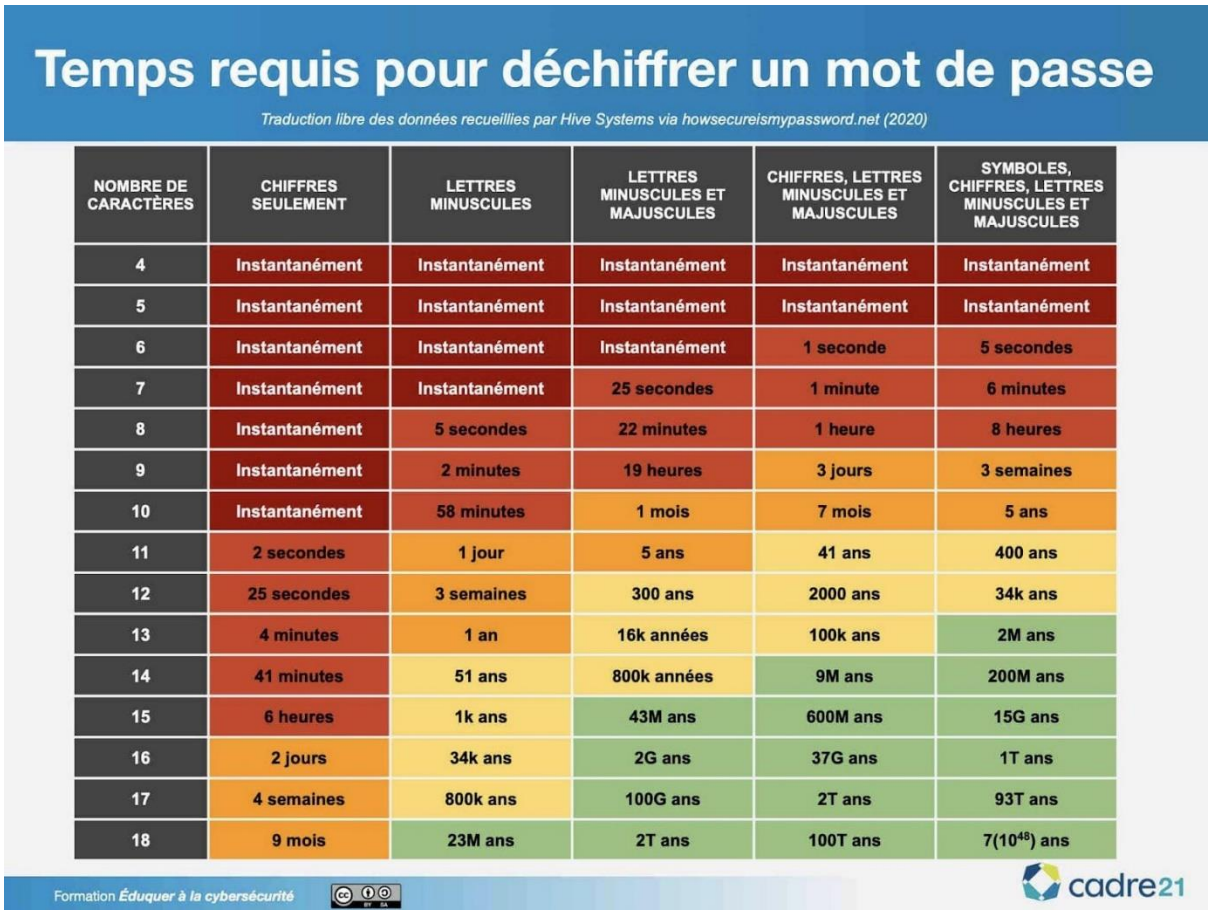
L'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) recommande de privilégier l'utilisation d'une authentification multi facteur, c'est-à-dire de mettre en œuvre plusieurs facteurs d'authentification appartenant à une des catégories parmi les facteurs de connaissance, de possession et inhérent.

Nous avons donc choisi de prendre deux facteurs : un facteur de connaissance et un facteur de possession.

Comme facteur de connaissance, nous avons fait le choix du mot de passe.

Nous demanderons aux collaborateurs de mettre au moins une majuscule et une minuscule, d'insérer au moins un chiffre, et un caractère spécial.

Ces contraintes seront explicitées aux professionnels, car comme vu dans le tableau ci-dessous, le temps de déchiffrage des mots de passe sans ces contraintes est instantané.



NOMBRE DE CARACTÈRES	CHIFFRES SEULEMENT	LETTRES MINUSCULES	LETTRES MINUSCULES ET MAJUSCULES	CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES	SYMBOLES, CHIFFRES, LETTRES MINUSCULES ET MAJUSCULES
4	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
5	Instantanément	Instantanément	Instantanément	Instantanément	Instantanément
6	Instantanément	Instantanément	Instantanément	1 seconde	5 secondes
7	Instantanément	Instantanément	25 secondes	1 minute	6 minutes
8	Instantanément	5 secondes	22 minutes	1 heure	8 heures
9	Instantanément	2 minutes	19 heures	3 jours	3 semaines
10	Instantanément	58 minutes	1 mois	7 mois	5 ans
11	2 secondes	1 jour	5 ans	41 ans	400 ans
12	25 secondes	3 semaines	300 ans	2000 ans	34k ans
13	4 minutes	1 an	16k années	100k ans	2M ans
14	41 minutes	51 ans	800k années	9M ans	200M ans
15	6 heures	1k ans	43M ans	600M ans	15G ans
16	2 jours	34k ans	2G ans	37G ans	1T ans
17	4 semaines	800k ans	100G ans	2T ans	93T ans
18	9 mois	23M ans	2T ans	100T ans	$7(10^{48})$ ans

Selon l'ANSSI:

De nombreux contrôles permettent de s’assurer que les mots de passe ainsi créés offrent une robustesse en accord avec le niveau de sécurité attendu par l’entreprise, comme :

- Mettre en place des mécanismes automatiques et systématiques permettant de vérifier que les mots de passe respectent bien les règles définies dans la politique de sécurité des mots de passe ;
- Comparer les mots de passe lors de leur création à une base de données répertoriant les mots de passe les plus utilisés ou bien ceux qui ont été compromis ;
- Repérer les mots de passe contenant des motifs (ou des répétitions de motifs) spécifiques (comme une suite de chiffre telle que « 12345 » ou comme la suite des premières lettres des claviers comme « azerty »);
- Repérer les mots de passe contenants des informations personnelles saisies lors de la création du compte, comme les noms et prénoms ou encore les dates de naissance;
- Lors d’un renouvellement du mot de passe, interdire la réutilisation d’un mot de passe parmi les X derniers mots de passe déjà utilisés.

Le facteur de possession que nous avons choisi est une authentification mobile.

L’authentification mobile est réalisée par l’envoi d’un SMS contenant un OTP. Un OTP est un mot de passe temporaire qui possède deux propriétés fondamentales : il expire rapidement et il ne peut pas être réutilisé.

Une fois l’OTP reçu, l’utilisateur le tape dans l’interface dédiée pour finaliser l'authentification.