MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES

Liberté
Égalité
Fraternité

DIRECTION DES RESSOURCES HUMAINES

SOUS-DIRECTION DE L'ATTRACTIVITÉ ET DES RECRUTEMENTS

Bureau des concours et examens professionnels

Concours interne et troisième concours pour le recrutement dans le grade d'adjoint administratif principal de 2e classe de chancellerie au titre de l'année 2027

Épreuve écrite d'admissibilité

Vendredi 2 octobre 2026

Épreuve de spécialité

Section Numérique

Durée totale de l'épreuve : 2h - Coefficient : 3

Épreuve consistant en la rédaction d'un écrit professionnel fondé sur la base d'un dossier complétée par la réponse à un questionnaire à choix multiple, dans la section choisie au moment de l'inscription. Certaines questions ou documents pourront être proposés en anglais.

Le dossier documentaire comporte 10 pages (page de garde, sommaire, sujet et questions non compris)

Sommaire

Questions à choix multiples (8 points) 1
Écrit professionnel (12 points) 5
Document 1 : Le vote par Internet 6
Document 2 : Peut-on voter par internet pour les élections politiques ? 7
Document 3 : Vote par internet 9
Document 4 : S'authentifier 10
Document 5 : Authentication methods: choosing the right type 12

Questions à choix multiples (8 points)

Pour répondre, vous cocherez les cases correspondant à vos réponses sur la copie prévue à cet effet.

Pour chaque question, une ou plusieurs réponses sont possibles.

Barème :

- *bonne réponse = + 0,4 point*
- *mauvaise réponse / réponse incomplète = - 0,1 point*
- *absence de réponse = - 0,1 point*

Le total de points sur la partie QCM ne peut être inférieur à 0.

1/ Qu'est-ce que le cloud computing ?

a. Un logiciel antivirus
b. Un type de virus informatique
c. L'utilisation de serveurs distants pour stocker et gérer des données
d. Un type de disque dur

2/ Qu'est-ce qu'un KEEPASS ?

a. Un coffre-fort numérique
b. Un mot de passe générique
c. Une clé passe-partout
d. Une passphrase de déverrouillage

3/ À quoi sert un switch internet ?

a. À contourner un réseau
b. À accélérer la vitesse de transmission
c. À créer un partage de réseau Internet
d. À passer d'un site Internet à un autre site Internet

4/ Quel est le nom du protocole utilisé par la messagerie ?

a. BGP
b. FTP
c. SMTP
d. ICMP

5/ What does mean POE ?

a. Power Over Ethernet
b. Product of Efficiency
c. Perfect Over Ethernet
d. Power Off Ethernet

6/ Lequel ou lesquels des énoncés suivant est/sont correct(s) en ce qui concerne la politique en matière de mots de passe ?

a. Un mot de passe robuste est composé au minimum de 12 caractères
b. Le mot de passe doit contenir des majuscules, des minuscules, des chiffres et des caractères spéciaux
c. Il faut avoir des mots de passe différents pour chaque compte de connexion
d. Lors du renouvellement d'un mot de passe le système ne contrôle pas l'historique des mots de passe

7/ Quel est l'ordre croissant correct des capacités de stockage ?

a. Téraoctet – Kilooctet – Pétaoctet – Mégaoctet – Gigaoctet
b. Kilooctet – Gigaoctet – Mégaoctet – Téraoctet – Pétaoctet
c. Kilooctet – Mégaoctet – Gigaoctet – Téraoctet – Pétaoctet
d. Kilooctet – Mégaoctet – Gigaoctet – Pétaoctet – Téraoctet

8/ Qu'est-ce que le « boot menu » ?

a. Menu d'amorçage qui permet de modifier les options de démarrage du système
b. Menu de démarrage Windows
c. Menu d'un système de restauration de données
d. Menu qui permet au démarrage de sélectionner différents systèmes d'exploitation

9/ Qu'est-ce qu'un « chatbot » ?

a. Un logiciel de reconnaissance vocale
b. Un logiciel programmé pour simuler une conversation
c. Un logiciel de reconnaissance faciale
d. Un logiciel de traduction simultanée

10/ What is the main function of an Active Directory server ?

a. It authenticates and authorizes all users and computers in a Windows domain-type network
b. It actively stores users' folders and documents
c. It forwards data packets between computer networks, including internetworks
d. It actively directs data packets within a network

11/ Le Machine Learning ou apprentissage automatique est une sous-discipline :

a. de la science des données (Data Science)
b. de l'intelligence artificielle
c. du Deep Learning (apprentissage profond)
d. de la robotique

12/ Un numéro SDA :

a. est un service qui attribue un numéro unique à chaque poste téléphonique ou utilisateur dans l'entreprise : La Sélection Directe à l'Arrivée
b. permet de fournir des services automatisés distribués par une société
c. est un numéro d'identification pour administrer un système décentralisé
d. donne accès à une Distribution en alimentation secours

13/ Qu'est-ce qu'une attaque en déni de service (DDoS) ?

a. Une cyberattaque qui bloque l'accès à l'appareil ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès
b. Un envoi de multiples requêtes jusqu'à saturer un serveur et le rendre inaccessible
c. Un programme informatique malveillant dont l'objectif est de s'implanter sur un système informatique
d. Le fait de tenir en ligne de manière répétée et intentionnelle, publiquement ou dans des cercles restreints, des propos ou des comportements ayant pour but ou conséquence une dégradation des conditions de vie de la personne qui en est victime

14/ En moyenne, combien d'électricité consomme une requête sur ChatGPT par rapport à une recherche Google (source : l'Agence internationale de l'énergie (AIE)) ?

a. 10 x plus
b. 20 x plus
c. 5 x moins
d. 2 x plus

15/ Which are the proposition symbols for AI (Artificial intelligence) ?

a. True and false
b. True, false, and null
c. True
d. False

16/ Quelle proposition contient une commande qui permet de se connecter à un système Linux distant et d'obtenir une console (*shell*) :

a. curl 192.168.1.100 443
b. ssh 192.168.1.100
c. ping 192.168.1.100 -g 1400 -G 1500 -h 3
d. rdp 192.168.1.100 -p 3389

17/ Les fonctions réseau d'une box internet domestique sont :

a. routeur
b. serveur DHCP
c. pare-feu
d. contrôleur de domaine

18/ Pour quel protocole opter lorsqu'on veut privilégier l'intégrité de la transmission ?

a. SCP
b. FTP
c. UDP
d. TCP

19/ Quelles sont les fonctions d'un-e RSSI (Responsable de la Sécurité des Systèmes d'Information) ?

a. Assurer l'évolution cohérente du système d'information (SI) d'un ministère, d'une administration ou d'une zone du SI de l'État
b. Assurer un rôle de conseil, d'assistance, d'information, de formation et d'alerte sur tout ou une partie des systèmes informatiques et de télécommunication
c. Gérer l'exploitation courante des systèmes informatiques, surveiller les équipements, gérer les incidents
d. Superviser la conception de projets informatiques, guider son équipe, assurer la qualité du produit final

20/ What is the purpose of Infrastructure as Code?

a. To build and install servers automatically
b. To install some software programs automatically
c. To update systems automatically
d. To check systems' conformity

Écrit professionnel (12 points)

Pour répondre au sujet, le candidat ou la candidate devra s'appuyer sur les éléments du dossier et sur ses connaissances personnelles.

Une copie mal présentée, peu lisible ou peu soignée pourra faire perdre des points, tout comme la présence de fautes d'orthographe, de grammaire ou de syntaxe.

Vous êtes Camille Trucmuche, correspondant/correspondante des systèmes d'information (CSI) du Consulat Général de France en Syldavie. En vue des prochaines échéances électorales, il vous est demandé de présenter à la Consule générale adjointe d'une part les modalités du vote par Internet et les mesures de sécurité associées, ainsi que vos propositions concernant les méthodes d'authentification, et d'autre part une foire aux questions (FAQ) synthétisant les éléments essentiels.

Document 1 : Le vote par Internet

Source : https://intranet.diplomatie.gouv.fr/spip.php?article121125 Diplonet 29 janvier 2025

Le Vote Par Internet (VPI) est une modalité de vote ouverte aux seuls Français de l'étranger, leur permettant ainsi de voter sans se déplacer dans des bureaux de vote parfois très éloignés de leur lieu de résidence.

A ce jour, le vote par internet a été mis en œuvre à sept reprises pour les deux scrutins pour lequel cette modalité de vote est prévue : pour l'élection des députés représentant les Français établis hors de France en 2012 et 2022, pour les élections législatives partielles de 2013 et 2023, pour les élections législatives anticipées de 2024 et pour les élections des conseillers des Français de l'étranger de 2014 et 2021.

Cette modalité de vote est largement utilisée (près de 75% des votants pour les législatives en 2024, soit plus de 400.000 votants par internet). Elle doit être à nouveau mise en œuvre pour les prochaines élections des conseillers des Français de l'étranger (2026).

Document 2 : Peut-on voter par internet pour les élections politiques ?

Source : https://www.service-public.gouv.fr/particuliers/vosdroits/F11257 Service Public 20 mai 2026

Vérifié le 20 mai 2026 - Service Public / Direction de l'information légale et administrative (Premier ministre)

Les règles sont différentes selon que vous votez en France ou depuis l'étranger :

En France
Vous ne pouvez **pas voter par internet**.
Pour voter, vous devez vous rendre dans votre bureau de vote avec un justificatif d'identité, le jour du vote.
Mais si vous prévoyez d'être absent ce jour-là, vous pouvez faire une procuration de vote. Faire une procuration vous permet de charger un autre électeur de voter à votre place, dans votre bureau de vote, le jour du vote.
Pour connaître l'adresse de votre bureau de vote et vérifier vos procurations en cours, vous pouvez utiliser **ce téléservice** : Vérifier votre inscription électorale et votre bureau de vote

Depuis l'étranger
Pour voter par internet, vous devez respecter les **3 conditions suivantes** :

- Vivre à l'étranger
- Être inscrit sur une liste électorale consulaire. Vous pouvez vérifier votre inscription électorale à l'aide de ce téléservice
- Avoir indiqué, lors de votre inscription, une adresse mail (adresse électronique) et un numéro de téléphone. Ces données sont nécessaires pour vous communiquer un identifiant et un mot de passe

Vous pouvez voter par internet lors des **élections suivantes** :

Élection des conseillers des Français de l'étranger
Lors de l'élection des conseillers des Français de l'étranger, vous pouvez voter par internet du **22 mai 2026 à 12h** (heure de Paris) **au 27 mai 2026 à 12h** (heure de Paris).

Pour cela, il peut être nécessaire de mettre à jour vos coordonnées figurant dans le registre des Français de l'étranger avant une date limite.

À savoir : Lorsque les circonstances le justifient, le bureau de vote électronique peut retarder l'heure de clôture du vote par correspondance électronique.

Pour voter par internet, vous devez vous authentifier. Il est possible de le faire de **2 façons** :

- Avec un identifiant et un mot de passe
- Avec une identité numérique certifiée France Identité

À noter : Tant que votre vote par voie électronique n'a pas été enregistré, vous pouvez voter au bureau de vote le jour de l'élection ou voter par procuration

L'enregistrement du vote le rend définitif et empêche toute modification.

Élections législatives

Lors des élections législatives, vous pouvez voter par internet.

À savoir : Lorsque les circonstances le justifient, le bureau de vote électronique peut retarder l'heure de clôture du vote par correspondance électronique.

Pour voter par internet, vous devez vous authentifier. Il est possible de le faire de 2 façons :

- Avec un identifiant et un mot de passe
- Avec une identité numérique certifiée France Identité.

À noter : Tant que votre vote par voie électronique n'a pas été enregistré, vous pouvez voter au bureau de vote le jour de l'élection, voter par procuration ou par correspondance.

L'enregistrement du vote le rend définitif et empêche toute modification.

Document 3 : Vote par internet

Source : https://www.diplomatie.gouv.fr/fr/services-aux-francaises-et-aux-francais/vie-administrative-et-elections/elections-a-l-etranger/modalites-de-vote/vote-par-internet France Diplomatie 15 septembre 2025 Mis à jour le 05 juin 2026

Pour quels scrutins ?
Le vote par internet (vote électronique) est prévu pour désigner les représentants des Français à l'étranger lors des **élections législatives** et des **élections consulaires**. Cette modalité de vote n'est pas ouverte pour les autres élections (présidentielle, européennes, référendum).

Qui peut voter par internet ?
Pour voter par internet, vous devez être Français, résider à l'étranger et être inscrit sur une liste électorale consulaire. Vous devez également avoir renseigné une adresse électronique et un numéro de téléphone valides afin que l'administration puisse vous envoyer votre identifiant (par courriel) et votre mot de passe (par SMS). **Aucune autre formalité n'est requise.**
Il vous est conseillé de vérifier la mise à jour de vos informations personnelles, adresses mails et téléphones, sur www.service-public.fr ou en contactant votre consulat.

S'authentifier (cf. document 4)
En cas de question, les électeurs peuvent solliciter **l'assistance mise en place par le ministère de l'Europe et des Affaires étrangères via le formulaire de contact** accessible depuis la page de connexion au portail de vote. La réponse sera adressée par courriel.

Le vote par internet : sécurisé, chiffré, surveillé

Document 4 : S'authentifier

Source : https://www.diplomatie.gouv.fr/files/files/vote-par-internet-authentification-id-mdp-v2.pdf
https://www.diplomatie.gouv.fr/files/files/services/elections/vote-par-internet-authentification-fin.pdf
France Diplomatie 15 septembre 2025 Mis à jour le 05 juin 2026)

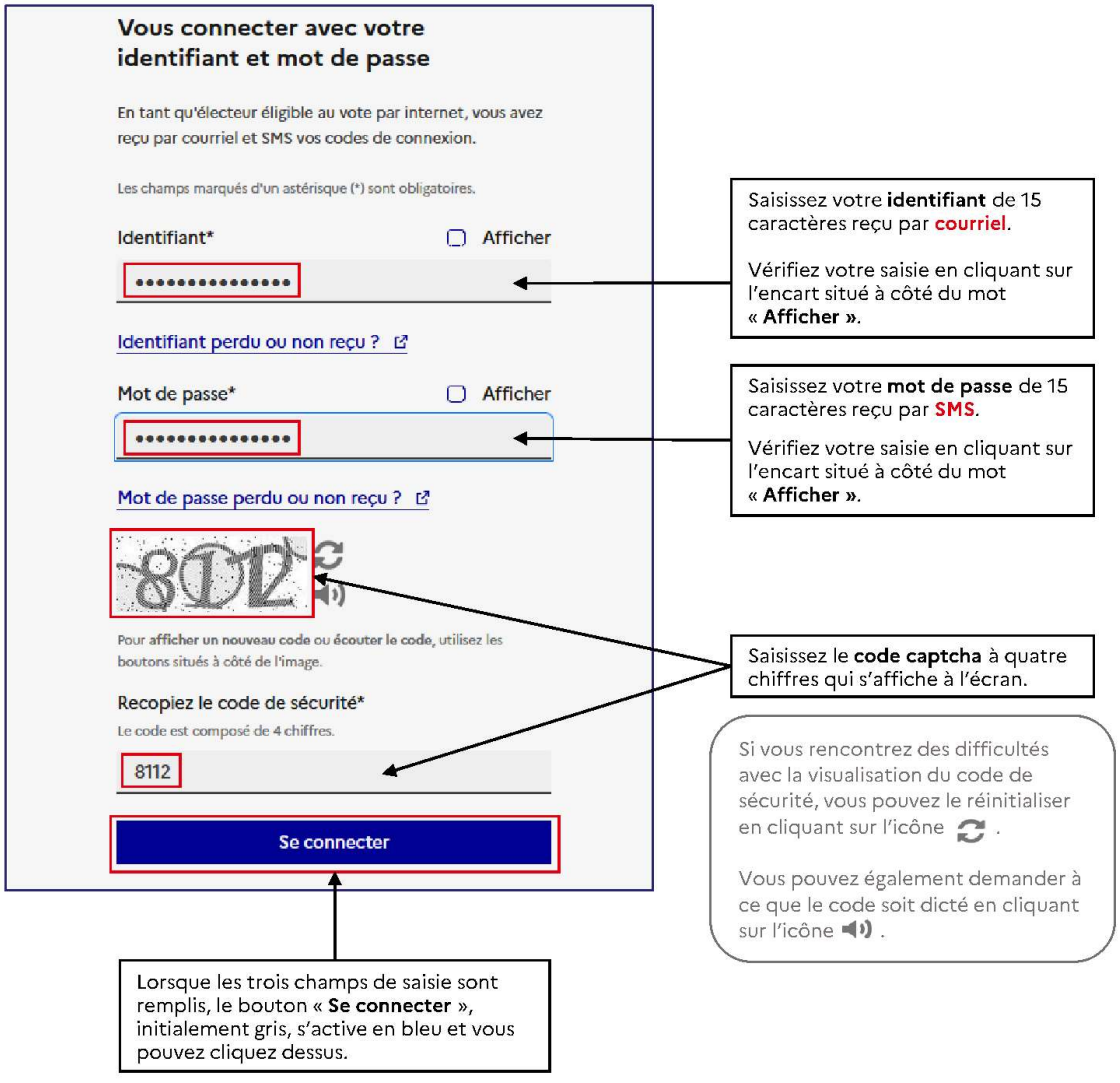
MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

VOTER PAR INTERNET

Avec un identifiant et un mot de pass

AUTHENTIFICATION

Si vous êtes inscrit sur le registre des Français établis hors de France et que avez renseigné un numéro de téléphone et un courriel **valides**, vous pouvez vous authentifier avec un identifiant et un mot de passe. **Votre identifiant vous est envoyé par courriel, votre mot de passe par SMS.**

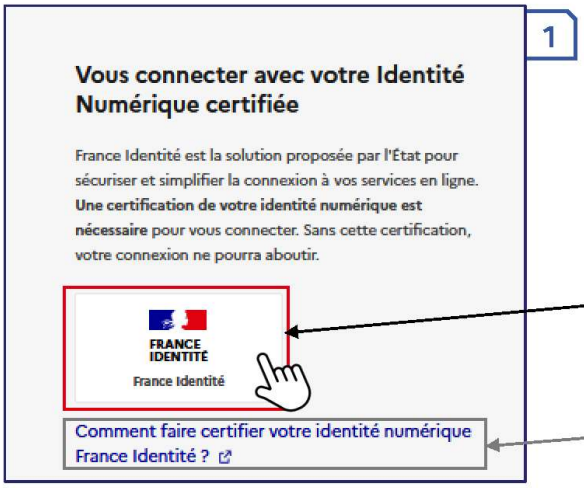


MINISTÈRE
DE L'EUROPE
ET DES AFFAIRES
ÉTRANGÈRES
Liberté
Égalité
Fraternité

VOTER PAR INTERNET

Avec l'Identité Numérique certifiée

AUTHENTIFICATION



Si vous possédez une **identité numérique certifiée** et disposez de l'application **France Identité mise à jour**, vous avez désormais la possibilité d'utiliser ce moyen pour voter par internet.

Attention : vous devez obligatoirement avoir un smartphone et être en possession de votre **carte nationale d'identité électronique** (CNIe) pour cette authentification.

1. Pour vous authentifier avec votre **Identité Numérique certifiée**, cliquez ici.

Pour vous informer sur les modalités de certification de votre identité numérique, **rendez-vous sur le site de France Identité, en cliquant sur le lien suivant.**

2

Connexion sur ordinateur

Sur un ordinateur :
Ouvrez l'application **France Identité** sur votre smartphone.

Ensuite, sur la page d'accueil, cliquez sur le logo suivant :

Puis scannez le code QR avec votre smartphone.

Connexion sur smartphone

Sur un smartphone :
Cliquez sur « **Ouvrir l'application France Identité** ».

Vous êtes automatiquement redirigé sur l'application.

Document 5 : Authentication methods: choosing the right type

Source : *https://www.ncsc.gov.uk/sites/default/files/2026-05/Authentication-methods-choosing-the-right-type.pdf National Cyber Security Center United Kingdom Reviewed 12 June 2025*

Authentication methods: choosing the right type

Recommended authentication models for organisations looking to move 'beyond passwords'.

This guidance helps organisations to select an appropriate method to authenticate their customers who are accessing online services. It's intended for retailers, hospitality providers and utility services, but can be used by any organisation that needs to authenticate customers when accessing online apps or websites. Adding any of the methods described here (that is, in addition to password authentication) will significantly increase the security of your customer accounts.

There are several authentication methods that provide security that goes 'beyond passwords'. This guidance summarises the benefits and limitations of each method, so you can choose the one that's most appropriate for your organisation - and your customers. It also provides links to more detailed NCSC guidance on each of the authentication methods.

Why go 'beyond passwords'?

Bill Gates predicted the death of the password nearly 20 years ago. Many assumed that alternative methods would replace them, but passwords remain the default method of authentication for a huge range of services, both at work and home. Password authentication is cheap, easy to implement, and understood by users. Password use continues to rise, mostly due to the adoption of online services and the massive growth in use of personal computers, smartphones and tablets.

Since the average user has so many online accounts, creating different passwords for all of them (and remembering them) is hard. Inevitably, users will devise their own strategies to cope with 'password overload'. This includes using predictable patterns to create passwords, or re-using the same password across different systems. Cyber criminals can exploit these well-known coping strategies, leaving your customers and your organisation vulnerable.

It also makes good business sense to introduce additional authentication methods. Some estimates suggest that as many as one-quarter of online purchases are abandoned due to forgotten passwords, as recovering passwords (or creating new accounts) can be a time-consuming process and will put off many potential customers.

How does additional authentication help?

Passwords can be stolen in a number of ways, but the most common way is when an organisation holding account details suffers a data breach. Criminals will use passwords stolen in the breach to try and access other accounts, a technique known as 'credential stuffing'. It works because many people use the same password for different accounts.

Cyber criminals may also use phishing techniques (either by email, text message or direct messages/chat) to try and access accounts, or simply try the really obvious passwords that millions of people still use.

Regardless of how they acquire passwords, unless you implement an additional method of authentication, cyber criminals can use stolen credentials to access users' accounts fraudulently. This

might give them access to sensitive personal data (including financial data such as credit card details), or allow them to impersonate someone to carry out harmful actions.

Adding a second additional method of authentication for customer accounts makes it much more difficult for a cyber criminal to do harm.

Chose the model that's right for you

This guidance looks at three authentication models:

- Multi-factor authentification (MFA)
- Federated Single Sign-On (SSO) services
- FIDO2

For each authentication method, you should consider both the security and usability of each one, and - most importantly - the profile of your customer base. For example, some customers may be reluctant to purchase additional devices in order to buy goods from your online store.

Although passwords have weaknesses, as a method of authentication it's both understood and accepted by most users.

Whichever model of additional authentication you implement, you'll need to provide additional support for your users, during account setup and beyond.

You should offer a range of methods to ensure you appeal to as many of your users as possible. And offering these options during account setup provides an opportunity to explain the benefits of extra authentication, and how it works.

Multi-factor authentication (MFA)

The most common authentication method that goes 'beyond passwords' is to implement multi-factor authentication (MFA), which is also known as two-step verification (2SV) or two-factor authentication (2FA). Accounts that have been set up with MFA require the user to provide a second factor, which is something that only the user can access. The second factor can be:

- PIN codes or a string of characters, often sent to the user via SMS or email
- a physical security token that the user must 'present' to their device (such as via USB or NFC)
- biometric details (such as a fingerprint scan, or facial recognition)
- approval through an app on a trusted device (such as those provided by Microsoft or Google)

Note:

The most appropriate second factor to use during MFA implementation will depend on what services your organisation offers, and your customer profile. For example, using a PIN code sent via SMS is the most widespread and well-understood second factor, but is not the most secure option. Providing your users with a choice of second factors will ensure you cover the widest customer base. For more information about implementing MFA - including detailed guidance on choosing authentication factors - refer to the NCSC's guidance on Multi-factor authentication for online services.

You should not mandate use of a second factor every time an MFA-protected service is used, as this would soon be irritating for users. It should only be required for high-impact activities, such as:

- changing passwords
- changing account details

A second factor should also be required whenever suspicious account activity is detected, such as a sign-in from an unfamiliar device, or from a different part of the world than is normal for that user.

Federated Single Sign-On (SSO) services

Federated SSO, based on protocols such as OpenID Connect (OIDC), allows a customer to use their sign-in for an existing account in one trusted service to sign-in to another new service. This is usually a well-known service provider among users, such as Apple, Facebook or Google). This may also be referred to as Social Login. The ability to "Sign in with…" (or similar) removes the burden of creating another set of account details when signing into a new website.

In addition, if a chosen federation provider has account security measures already in place, or adds stronger measures – such as common password banning, MFA or suspicious activity blocking – then the new service inherits these benefits for sign-in to their accounts. This means the new service is spared the cost and effort of duplicating development of these measures themselves.

But by the same token, if a cyber criminal accesses the account a customer has with a trusted federation provider, then they'll also have access to the connected accounts in the online services that use it for authentication. For this reason, you should consider the security posture of the provider – and the accounts they provide – and only select providers that demonstrate appropriate security.

You'll also need to consider the availability of your chosen federation provider(s). If a provider's authentication service experiences an outage, and it is a customer's only way of signing in to your online service, they will be unable to complete a new sign-in until the outage is resolved (as demonstrated in the 2021 Facebook outage).

Even if you offer a selection of federation providers, some users will not want to associate an existing account with your new service. For these users, you should offer an alternate authentication method.

FIDO2

FIDO2 is a set of standards that define cryptographic authentication using public key credentials and protocols to provide more secure alternatives to passwords for accessing online services. FIDO2 authenticators can include:

- a personal device such as a smartphone or laptop with a trusted platform module (TPM)
- a physical USB key

They can be used for passwordless logins, or as a second factor.

Most FIDO2 tokens are USB-based - such as Yubikeys. There is a variety of FIDO2 authentication tokens available to suit various needs and budgets. Most modern smartphone apps can support FIDO2 as they have biometrics built-in to authenticate the user to the device. FIDO2 grants authentication via a user action such as entering a PIN, or presenting a known biometric (for example, a registered fingerprint or facial scan).

In the majority of cases, the customer would be responsible for purchasing the token. A lost token means that a customer would be unable to authenticate to the service they're trying to access if they

didn't have a backup, so they should register a backup (which may mean buying another token). Since relatively few services accept FIDO2, customers may be reluctant to purchase one or more tokens (given that there are alternative cheaper and more widely-used forms of authentication).

A lost token will also need to be revoked, which requires the customer to log into every service with the backup token to remove the lost one.

Whilst major phone and computer vendors are enabling FIDO2 natively on their devices (enabling the automatic sharing of tokens across user devices on their platforms), there are still several barriers to adoption, including usability and upfront cost.